IN THE EUROPEAN COURT OF HUMAN RIGHTS **Application No. 46259/16**

B E T W E E N:

(1) PRIVACY INTERNATIONAL

(2) GREENNET LIMITED

(3) CHAOS COMPUTER CLUB E.V.

(4) MEDIA JUMPSTART INC.

(5) RISEUP NETWORKS INC.

(6) KOREAN PROGRESSIVE NETWORK JINBONET

Applicants

-v-

THE UNITED KINGDOM

Respondent

APPLICANTS' SUPPLEMENTARY BUNDLE ACCOMPANYING APPLICANTS' OBSERVATIONS AND REPLY TO OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

Intelligence Services Commissioner

Report of the Intelligence Services Commissioner for 2014

The Rt Hon Sir Mark Waller

Presented to Parliament pursuant to section 60(4) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 25 June 2015

Laid before the Scottish Parliament by the Scottish Ministers 25 June 2015

HC 225
SG/2015/74



© Crown copyright 2015

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at [insert contact details]

Print ISBN 9781474121118
Web ISBN 9781474121125

ID 04061503 06/15

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of
Her Majesty's Stationery Office

CONTENTS

FOREWORD 2

1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER 7

2. METHOD OF MY REVIEW IN RELATION TO WARRANTS AND AUTHORISATIONS 9

3. STATISTICS 11

4. ASSESSMENT OF MY INSPECTION VISITS 12

   i. Intrusive Surveillance 12

   ii. Directed Surveillance Authorisation (DSA) 15

   iii. Intelligence Services Act (ISA) - Property interference warrants 17

   iv. Covert Human Intelligence Source (CHIS) 20

   v. Intelligence Services Act (ISA) Section 7 authorisations 23

   vi. Consolidated Guidance 27

   vii. Bulk Personal Data 32

5. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS 39

6. ERRORS 40

7. BRIEF SUMMARY OF ASSESSMENTS 46

8. CONCLUSIONS 56

APPENDIXES 57

   1. The Statutory Functions of the Intelligence Services 58

   2. The Regulation of Investigatory Powers Act 2000 (RIPA) 59

   3. Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA) 60

   4. Warrants and Authorisations under the Intelligence Services Act 1994 (ISA) 64

   5. The European Convention on Human Rights (ECHR) 66

   6. Necessity and Proportionality 67

   7. Bulk Personal Datasets Direction 68

   8. Consolidated Guidance Direction 69

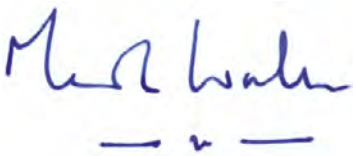
The Rt Hon Sir Mark Waller
Intelligence Services Commissioner
2 Marsham Street
London
SW1P 4DF

The Rt. Hon. David Cameron MP
10 Downing Street
London
SW1A 2AA

I enclose my fourth Annual Report covering the discharge of my functions as Intelligence Services Commissioner between 1 January 2014 and 31 December 2014.

It is for you to decide, after consultation with me, how much of the report should be excluded from publication, on the grounds that any such publication would be contrary to the public interest, or prejudicial to national security, to the prevention or detection of serious crime, to the economic well being of the United Kingdom, or to the discharge of the functions of those public authorities subject to my review.

I have continued to write my report in two parts, the Confidential Annex containing further details including techniques and operational matters which in my view should not be published. I hope you find this convenient.



The Rt Hon Sir Mark Waller

INTELLIGENCE SERVICES COMMISSIONER



FOREWORD

Under section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA) the Prime Minister appoints an Intelligence Services Commissioner who must hold or have held high judicial office within the meaning of the Constitutional Reform Act 2005. I held office as a Lord Justice of Appeal from 1996 until I retired in May 2010. I was appointed by the Prime Minister to the post of the Intelligence Services Commissioner on 1 January 2011. After my initial appointment, I accepted the Prime Minister's request to serve as Intelligence Services Commissioner for an additional three years from 1 January 2014.

The UK continues to be a target for groups and gangs, from home and abroad, who would threaten our national security and economic well being. In August 2014, the Joint Terrorism Analysis Centre (JTAC) raised the United Kingdom (UK) threat level from "substantial" to "severe", meaning that an international terror attack on UK soil is highly likely.

In the last 10 years, we have seen a step change in the nature of the threats we face with the tragic events in Paris and Copenhagen early in 2015 being recent examples of how terrorist tactics have evolved and diversified since 9/11 and 7/7.

The police, intelligence and security agencies and the Ministry of Defence (MOD) play a vital role protecting our country and meeting these challenges. They have been given wide ranging powers and capabilities by Parliament (further detail on the intelligence and security agencies and MOD's functions can be found in the appendix to this report) to disrupt the threats to the UK and our interests including powers to intrude upon the privacy of individuals.

What I oversee

As Intelligence Services Commissioner, I am responsible for auditing the authorisations required by the UK intelligence agencies and their officers enabling them to use lawfully the intrusive powers available to them under RIPA part II and the Intelligence Services Act 1994 (ISA). I also fulfil the same function in relation to the MOD's use of equivalent authorisations. In summary I oversee the granting of warrants and authorisations by Ministers where those are necessary, and internal authorisations where those are necessary.

I also oversee the use by the agencies of bulk personal datasets and compliance by the agencies and MOD with the Consolidated Guidance.[1] See Chapters 4.vi and 4.vii of this report for more detail about how I oversee these activities.

1 Consolidated Guidance to Intelligence officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating

I take it as a priority that any intrusion into privacy must be fully justified by the necessity to gain intelligence or carry out the activities in the interests of the UK and I do this by ensuring all activity undertaken by the agencies:

- is necessary for the purpose of protecting national security, the prevention or detection of crime or the economic well-being of the UK;
- falls under one of the statutory functions of the intelligence services;
- is proportionate including that:

  a) a less intrusive means could not have been used

  b) intrusion into privacy is limited so far as possible

  c) in particular any collateral intrusion into privacy is identified and kept to a minimum

  d) any intrusion is justified by the necessity to gain the intelligence or protect the UK.

- is/was authorised by a relevant senior official or Secretary of State.

Structure of oversight relating to warrants and authorisations

RIPA formally established the oversight mechanisms which Parliament intended for the intelligence services.

The oversight I provide is part of a much broader oversight structure which includes:

Secretaries of State
Each agency falls under the authority of a Secretary of State who is accountable to Parliament for what agencies do or fail to do. Their personal authorisation is required for more intrusive activities of the agencies.

Parliamentary oversight
The Intelligence and Security Committee of Parliament (ISC) (a cross party committee which draws its membership from both Houses) primarily examine MI5, MI6 and GCHQ's expenditure, administration and policy. The Committee reports to Parliament annually, and carries out other inquiries on which they produce reports.

Independent judicial oversight
The Interception of Communications Commissioner and the Intelligence Services Commissioner are appointed by the Prime Minister and are required to be the holder or past holder of high judicial office, ensuring independent, unbiased judgement. The Interception of Communications Commissioner is concerned with interception and communications data and now produces two reports a year, the most recent dated 12th March 2015. I as Intelligence Services Commissioner oversee other matters, as summarised on page (7) below.

It is the Secretary of State who is responsible for taking the relevant decision in the most intrusive areas and who is also accountable to Parliament. I, as Commissioner, have the function of review. The way I carry out my review is set out in Chapter 2. The essential features which I emphasise at this stage are:

1. I carry out two formal inspections a year at each of the agencies and MOD and at the warrantry units at the Foreign Office, the Home Office and the Northern Ireland Office;

2. I get a complete list of all warrants and authorisations current during the period including relevant internal approvals; the lists identify the subjects of the warrants and authorisations;

3. I select certain warrants, authorisations and internal approvals both randomly and by reference to subject matter so that the full paperwork that lies behind those warrants and authorisations can be assembled for my scrutiny;

4. The agencies, the MOD and the warrantry units also bring some warrants or authorisations to my attention which they think I should see and again the full paperwork will be made available;

5. At the agencies and MOD I personally read the warrants and authorisations and the paperwork that lies behind including submissions and supporting documentation; at the Foreign Office, the Home Office and the Northern Ireland Office I spend further time reading the paperwork mostly relating to different warrants and authorisations;

6. At the agencies and MOD I then hold formal interview sessions with those responsible for the documentation and carrying out the activities authorised; at the Foreign Office, the Home Office and the Northern Ireland Office I interview and question those responsible for advising ministers and considering the warrants and authorisations.

7. Once a year I meet each of the ministers – the Foreign Secretary, the Home Secretary, the Northern Ireland Secretary and the Defence Secretary.

A duty of cooperation is imposed on every member of an agency, every departmental official and every member of the armed forces to disclose or provide to me all such documents and information as I may require. I have never had anything but cooperation in this regard.

I emphasise that I do this activity personally and I undertake my duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves, without political favour or personal bias.

Review of 2014

Apart from my inspections other matters which occurred in 2014 were as follows.

In January the Prime Minister asked me to report on compliance with the Consolidated Guidance so that the ISC might be properly informed of my views. That Report was produced in February 2014 and provided to the ISC.

In March, I was ordered to give evidence at the Home Affairs Select Committee's Inquiry into Counter-Terrorism. I had taken the view that the appropriate Parliamentary Committee with whom I should discuss my oversight was the ISC. The Home Affairs Committee took a different view and ordered me to attend and thus I did so.

I also appeared before the ISC in October in relation to their Privacy and Security Inquiry.

I was pleased to have had the opportunity to co-host the International Intelligence Review Agency Conference with the ISC in July. The conference focused on the complex balance between protecting an individual's right to privacy and ensuring our collective right to security.

The Home Secretary opened the conference and representatives of the oversight bodies from fifteen different countries attended. Privacy safeguards continue to be my priority so I was particularly interested to exchange views and ideas with my counterparts in other democratic countries. The conference provided an expert forum for legislators and senior office holders working in the field of intelligence oversight to:

- identify current international challenges and drivers;
- consider emerging concerns that impact domestically and internationally;
- exchange ideas and compare models of accountability, including lessons learned and good practice;
- support countries in developing of intelligence oversight mechanisms drawing on the experience of countries with existing structures; and broaden dialogue and expand the expert network towards further international collaboration.

Finally, I was pleased to welcome the Prime Minister's decision to put my oversight of the Consolidated Guidance and bulk personal datasets onto a statutory footing. All of my oversight is now on a statutory footing and I have no extra- statutory responsibilities.

In particular I welcome that the agencies' use of bulk personal datasets and my independent oversight has been avowed. I have had non-statutory oversight since my appointment that oversight having been accepted by my predecessor just

before his appointment ended. In his announcement of 12 March 2015 the Prime Minister said:

"The Intelligence Services Commissioner, the Rt Hon Sir Mark Waller, currently provides non-statutory oversight of the Security and Intelligence Agencies' use of bulk bulk personal datasets. Sir Mark has previously recommended that this be put on a statutory footing."

I reported on this aspect in the confidential annex to my Annual Reports. In my Annual Report for 2013 I reported in my confidential annex for example on the agencies' acquisition, retention, storage and deletion of bulk personal datasets as well as access to and use of such data. In doing so I considered the related privacy issues and safeguards, particularly the possibility of data being misused and how this is prevented. I consider this to be a key part of my oversight as it is critical that access to bulk personal data is properly controlled and the risk that some individuals may misuse their powers to access private data is carefully guarded against. I report on this further in chapter 4.vii of this report.

Structure of my report

I am committed to being as open and transparent with the public as I possibly can be within the constraints of my office and of the subject matter I deal with. To this end as part of my continued drive for greater openness I have restructured my report and dealt with issues thematically including, for example, sections on Intrusive Surveillance, Directed Surveillance, Covert Human Intelligence Sources and Intelligence Services Act section 7 authorisations. There is also a section on my recently publically avowed Bulk Personal Data oversight. These sections highlight privacy considerations and provide my overall assessment during 2014 including some of the recommendations I have made to help ensure continued compliance.

My office also re-launched my website last October which now contains more detail about my functions, the legislative framework under which I operate and how I carry out my inspections.

1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER

My statutory functions are set out in full on my website, but in summary my primary role as Intelligence Services Commissioner is to ensure the UK intelligence agencies and parts of the Ministry of Defence lawfully and appropriately use the intrusive powers available to them including:

Figure 1: Oversight of warrants and authorisations issued by Secretaries of State

Function	Legislation
Oversight of the Secretary of State's powers to issue, renew and cancel warrants authorising entry on to or interference with property (eg the planting or installing of a listening device) or with wireless telegraphy	Section 5 and 6 of the Intelligence Services Act 1994
Oversight of the Secretary of State's powers to issue, renew and cancel authorisations for acts done outside the United Kingdom	Section 7 of the Intelligence Services Act 1994
Oversight of the Secretary of State's powers to grant authorisations for intrusive surveillance(e.g. monitoring through a listening device)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II
Oversight of the Secretary of State's powers to grant authorisations to investigate electronic data protected by encryption	Regulation of Investigatory Powers Act 2000 (RIPA) Part III

Figure 2: Oversight of internal authorisations issued by a Designated Officer	
Function	**Legislation**
Oversight of powers to grant authorisations for directed surveillance (DSA)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II
Oversight of powers to grant authorisations for the conduct and use of covert human intelligence (CHIS)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II

In the last year, under section 59A of the Regulation of Investigatory Powers Act 2000 (as amended by section 5 of the Justice and Security Act 2013), the Prime Minister published two directions which put on a statutory footing my oversight of:

- the acquisition, use, retention, disclosure, storage and deletion of bulk bulk personal datasets including the misuse of data and how this is prevented
- compliance with the Consolidated Guidance

Both directions can be found in the appendix to my report.

My other statutory functions include:

- Assisting the Investigatory Powers Tribunal when required;
- Reporting to the Prime Minister annually on the discharge of my duties;
- Overseeing the adequacy of the Part III safeguards of RIPA arrangements;
- Advising the Home Office on the propriety of extending the TPIM regime;
- Overseeing any other aspects of the functions of the intelligence services, HM Forces or the MOD when directed by the Prime Minister.

2. METHOD OF MY REVIEW IN RELATION TO WARRANTS AND AUTHORISATIONS

It is my duty, as far as I am able, to satisfy myself that the agencies have acted within the law and that the test of necessity and proportionality has been correctly applied.

I do this through my formal four stage inspection regime (a summary of my method can be seen on the right) where I audit warrants and authorisations.

I examine the systems in use to assure myself that the organisations I oversee have robust and rigorous internal checks and assurances in place. I also attend training courses given to both new and existing intelligence officers in order to gain a better understanding of the culture and ethos of the organisation.

During my formal inspections, I examine a statistically significant sample of:

- warrants issued by Secretaries of State authorising intrusive surveillance and interference with property and;
- other authorisations issued by designated officials (such as for covert human intelligence sources and directed surveillance)

In 2014 I was provided with a complete list of all 2032 warrants and authorisations and selected 343 so that I could read and scrutinise the supporting submissions and paperwork behind the same. Because some operations continue for substantial periods of time, I will have seen other warrants and authorisations on the list and the paperwork behind them during previous inspections.

Figure 3: Stages of oversight

Selection

I select from a list of all warrants and authorisations provided by the agencies which are current or were cancelled during the six months prior to my inspection. The list includes a brief description of what each is about.

Pre-Reading

All selected cases with supporting documentation are available. I scrutinise and review the necessity and proportionality of the operation paying particular attention to whether any intrusion into privacy has been justified. I am supported by my Head of Secretariat who ensures that the proper administrative procedures have been followed.

Formal Inspection Visit

During my inspections, I am briefed on current operations and I follow up on any points arising from my pre read or errors reported to me. I question intelligence officers and senior personnel to ensure they can justify their activity

Under the Bonnet Inspection

In these follow up inspections, which are designed to go beyond the paperwork and see the ways in which any assurances have been implemented, I question staff across a range of grades about how they will apply, or have applied, the tests of necessity and proportionality in the planning stages and when carrying out the activities specified in any warrant or authorisation.

Who I met

During 2014 I undertook formal oversight inspections of each of the authorities that apply for and authorise warrants that I oversee. They are:

The Security Service (MI5)
The Secret Intelligence Service (SIS)
Government Communications Headquarters (GCHQ)
The Ministry of Defence (MOD)

In addition I inspected the departments processing warrants (warrantry units) for each Secretary of State where I scrutinise the way submissions have been analysed and the advice given to, and the approach of, the Secretaries of State. They are:

The Home Office
The Foreign Office
The Northern Ireland Office (NIO)

I also meet the respective Secretaries of State who sign off warrants at each department. They are:

The Home Secretary
The Foreign Secretary
The Defence Secretary
The Northern Ireland Secretary

Details of the visits made to the agencies, MOD and to the Foreign Office, Home Office and Northern Ireland Office are contained later in my report with a summary of my conclusions on the same.

3. STATISTICS

I believe that publishing the total number of RIPA and ISA authorisations is helpful to public confidence and gives an idea of the number of authorisations that I could potentially sample during my inspection visits. However, it is my view that disclosing details beyond this could be detrimental to national security, and for this reason a further breakdown is provided only in my confidential annex.

I select warrants for scrutiny from a full list of all 2032 current warrants and authorisations provided by the agencies. This list includes brief descriptions of what each is about so in effect I see **all** of warrants and authorisations but select some for closer examination including in particular the submissions and other underlying documentation. In 2014 I selected 343 warrants and authorisations with their supporting documentation for closer scrutiny. Others or more accurately their predecessors, particularly those for long running operations, will have been seen during previous inspections.

Warrants and authorisations have a finite duration, expiring after 3, 6 or 12 months. As a result, the 2032 warrants and authorisations approved in 2014 should not be interpreted as adding to a cumulative total of warrants and authorisations over preceding years. I have set out these figures below for comparison.

Figure 4: Statistics by Year

Year	2011	2012	2013	2014
Approved	2142	2838	1887	2032
Scrutinised	_____	242	318	343
Percentage	_____	8.5%	16.8%	16.7%

Although it is vitally important that I scrutinises a representative sample of warrants and their underlying documentation I am of the view that understanding the systems and processes in place in the agencies is also important. Inspection of the warrants and their supporting documentation is not the extent of my oversight in this area. As well as the four stages of my inspection regime I also attend training courses given to both new and existing intelligence officers so that I can gain a better understanding of the culture and ethos of the organisation. On top of this I check the systems in place within the organisation to assure myself that they have in place robust and rigorous internal checks and assurances.

It is all of this taken together which allows me to undertake my oversight of the warrantry and authorisations.

4. ASSESSMENT OF MY INSPECTION VISITS

i. Intrusive Surveillance

Intrusive surveillance is covert surveillance related to anything taking place on residential premises or in a private vehicle, and involving an individual being present on the premises or in the vehicle, or deploying of a surveillance device. The definition of surveillance as intrusive relates to the location of the surveillance, since the surveillance in residential premises or vehicles is likely to involve a greater intrusion into privacy. Part II of RIPA and the associated code of practice provide the legal framework for authorising surveillance activity which is compatible with Article 8 of the European Convention on Human Rights (ECHR) (see appendix).

Privacy

Intrusive surveillance involves the greatest invasion of privacy and as such consideration must be given as to how to avoid unnecessary intrusion into privacy and specifically the privacy of any family members or friends of the individual under surveillance. The agencies must make a strong case to explain why the information to be obtained cannot be gathered by less intrusive means and that the necessity of obtaining the information outweighs the intrusion into privacy.

My overall assessment

In the submissions I have examined proper cases for necessity have been made and proper consideration has been given to limiting unnecessary intrusion into privacy and minimising collateral intrusion. The invasion authorised has also been justified by the necessity. **There are however some points to be made.**

- Timing of applications for warrants

According to the relevant codes of practice, application for DSA and CHIS renewals must be made **shortly** before the authority in force is due to end. However, warrants signed by a Secretary of State only require that the renewal is made **before** the warrant expires. This does not prevent the agency from applying for a renewal some months before the expiry date so that when the Secretary of State gives consideration to the renewal, the case for necessity and proportionality is in danger of being out of date. The possibility of a busy period coming up (such as the Olympic Games) or difficulties of availability (such as can be caused by a General Election) understandably lead agencies to put applications in train early but I have **recommended** that applications for renewal should be made only shortly before the warrant expires.

- Breadth of language

Intrusive surveillance can only take place in support of one of the functions of the intelligence services in relation to the activity specified in the warrant signed by the Secretary of State. In Northern Ireland I was concerned with the breadth of language used to define the subjects on two urgent warrants, one of which included an intrusive surveillance authorisation. However after challenging the Northern Ireland Office (NIO) I was reassured that they were keeping a very close eye on the use of the warrants and that the Secretary of State expected to be notified of any use. I was satisfied that the urgency of the warrants was necessary and that the correct procedures had been applied but **recommended** that the renewal submission, which had to take place within two working days, should reflect the limitations being applied by NIO to the use of the warrant.

I also noticed this in a few warrants seen at MI5 and stated that **care should be taken** with the language to identify who the subject of the warrant could be.

- Confidential Information and Collateral Intrusion

In the cases I reviewed I noted that careful consideration was given to the possibility that any confidential information might be obtained and consideration was given to any collateral intrusion and how to limit this. I **recommended** that the submission should spell out what is in place to limit collateral intrusion and that the submission should make clear that anything that is not of intelligence interest should be deleted as soon as practicable.

- Gardens

Paragraph 2.16 of the surveillance code of practice states that a front garden or driveway readily visible to the public would not be regarded as residential property for the purpose of RIPA. I **recommended** that this should be interpreted with caution and read in conjunction with RIPA s26(5) which states that devices which constantly provide information as if the device were actually present on the premise would be intrusive surveillance.

Conclusion

Intrusive surveillance is the most intrusive technique because it takes place inside family homes and cars. I keep this in mind when I am reviewing applications and when they come up for renewal I expect to see evidence of intelligence obtained to help justify the continued operation. I am satisfied that:

- The agencies take great care to seek other less intrusive means before undertaking this level of intrusion and often consult their lawyers to ensure the legality of their submission;

- The warrantry units at the Foreign Office, Home Office and Northern Ireland Office can and will question the agencies concerning the use and applicability of the suggested activity and they will not forward anything to the Secretary of State until they are satisfied. These units are an effective additional safeguard.

Finally I am satisfied that a Secretary of State will refuse any warrant if they are not convinced of the necessity and proportionality; they are aware that they are ultimately accountable for the operation.

ii. Directed Surveillance Authorisation (DSA)

Directed Surveillance is surveillance which obtains private information in a covert but not intrusive manner. Part II of RIPA and the associated code of practice provide the legal framework for authorising surveillance activity which is compatible with Article 8 of the ECHR (please see the appendix to this report).

Privacy

Directed surveillance is less intrusive but proper consideration must still be given to the necessity and proportionality of the activity. Specific consideration must be given to ensuring that the necessity of obtaining the information outweighs the intrusion of privacy.

My overall assessment

From the submissions I have examined the applications to undertake directed surveillance have made out a proper case of necessity and considered properly whether any intrusion into privacy is justified and the extent justified. **There are however certain points to be made.**

- Duration and Combination

During 2014 I became concerned that there is more room for error when directed surveillance is required in combination with a property warrant. Legislation allows the Secretary of State to sign a combined property and intrusive surveillance warrant but when a DSA is required in combination with a property warrant the property warrant is signed by the Secretary of State but the DSA must be authorised separately by the agency. Additionally property warrants and DSAs have different duration periods which means that the warrants and authorisations have different renewal/cancellation deadlines.

It is easy to see how errors can be made and indeed were made when for example through an oversight a DSA authorisation was not obtained. I have **recommended** that if the legislation were to be amended there should be room for flexibility in issuing combined warrants and around the duration of warrants so that they can be combined and synchronised.

- Modification to DSAs

Directed Surveillance may be authorised against a particular terrorist operation because RIPA requires that it is "for the purpose of a specific investigation or a specific operation". The authorisations should thus make it clear what the expected outcome is for these thematic style surveillance operations and identify the targets, preferably by name.

MI5 appear to be diligent in modifying the authorisation to add or delete named individuals taking into account necessity and proportionality as and when they become involved in the investigation. However, from the paperwork provided to

me it is sometimes difficult to keep track of amendments in more complex and long running authorisations. MI5 has committed to looking at ways to improve the provision of inspection material such as moving to online systems rather than paperwork which will assist in the scrutiny process.

- Open Source Information

The increased use of the internet and social media among target groups has led to greater interest in open source internet data by the agencies. The law, including Article 8 of the ECHR, applies equally to online activity as to activity in the physical world and the agencies are obliged to comply with the law in relation to the collection of open source internet data just as much as to the collection of any other type of intelligence. The agencies recognise that the collection of open source internet data may be capable of amounting to directed surveillance if the statutory criteria are met and they are working to formulate clearer guidance on when the collection of open source internet data might amount to directed surveillance. I have asked to be provided with any such guidance.

iii. Intelligence Services Act (ISA) – Property Interference Warrants

The Secretary of State under section 5 of ISA may issue warrants authorising MI5, SIS or GCHQ to enter into, go onto, or interfere with, property, or to interfere with wireless telegraphy. Property includes physical property and intellectual property. They are often referred to as property warrants. A property warrant may be used for remote interference with a computer in order to obtain information from that computer. It could also be used to authorise entry into or interference with a domestic residence for the purpose of concealing a listening device. In such cases they are used in conjunction with an intrusive surveillance warrant.

Privacy

These can be highly intrusive techniques and as such separate consideration must be given to limit any unnecessary intrusion into privacy and specifically the privacy of any family members or friends. A strong case must be made to explain why the information cannot be obtained through less intrusive means and that the necessity of obtaining the information outweighs the invasion of privacy.

My overall assessment

In the submissions for section 5 warrants which I have examined proper cases of necessity have been made and proper consideration has been given to avoiding unnecessary intrusion into privacy and limiting collateral intrusion. Such intrusion has also been justified by the necessity. **Once again however, there are points to be made.**

- Duration of Warrants

The legislation is ambiguous when it comes to dates from which warrant renewals run: it is possible to read ISA so that renewal of a property warrant begins on the day that the Secretary of State signs the renewal. For example if a warrant is issued on 16 March, its first day is 16 March and six months later it expires on 15 September i.e. 6 months less a day. If it is renewed at signing, on 7 September, its next period begins on the day of renewal [7 September] and runs for six months expiring on 6 March.

However, the code of practice for surveillance and property interference paragraph 7.40 states that renewal begins with the day it would have ceased to have effect but for the renewal. On this interpretation a warrant issued on 16 March and renewed on 7 September runs for 6 months from the date of the expiry 15 September to expire on 15 March.

According to the RIPA explanatory notes, RIPA *s43(9)* "clarifies the time from which a grant or renewal of an intrusive surveillance authorisation takes effect. It synchronises the duration of intrusive authorisations with those given for property

interference." This seems to support the code of practice understanding [see *s43(9)(b)]* but it remains unclear.

No harm is done if the first interpretation is being followed because renewal if anything is taking place early. But this lack of clarity is unhelpful so I have **recommended** that if the legislation were to be amended there should be greater clarity in the date from which warrants or authorisations run particularly following renewals.

- Thematic Property Warrants

I have expressed concerns about the use of what might be termed "thematic" property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers "to a particular act" or to "acts" undertaken in the course of an operation. However, section 5 is narrower referring to "property so specified".

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and
- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals.

The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment.

I accept the agencies' interpretation is very arguable. I also see in practical terms the national security requirement.

The critical thing however is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality. Thus I have made it clear:

- a Secretary of State can only sign the warrant if they are able properly to assess whether it is necessary and proportionate to authorise the activity
- the necessity and proportionality consideration must not be delegated

- property warrants under the present legislation should be as narrow as possible; and
- exceptional circumstances where time constraints would put national security at risk will be more likely to justify "thematic" warrants.

This has led to one of the agencies withdrawing a thematic property warrant in order to better define the specified property. We remain in discussion to find a way to do so but I am anxious to ensure that they are not missing intelligence opportunities which might endanger national security.

I made **five recommendations** at each of the intelligence agencies and warrantry units in relation to what might be termed thematic property warrants:

1. For any warrants which might be considered to be thematic to be highlighted in the list provided for my selection;

2. The terms of a warrant and the submission must always be such as to enable the Secretary of State to assess the necessity and proportionality;

3. The assessment of proportionality and necessity should not be delegated;

4. Property warrants should be as narrow as possible but circumstances where time constraints and national security dictate may allow a more broadly drawn "thematic" warrant; and

5. As the agencies and the Secretaries of State have made clear to me is the case, thematic or broadly drawn warrants should not be asked for simply for administrative convenience.

I have **recommended** in general, and not just for thematic warrants, that the submission attached to the warrant should set out all the limitations applied to the use of the warrant and particularly should identify what action is being taken to minimise intrusion into privacy.

- Renewing Property Warrants

Although the legislation does not require it, when renewing a property warrant I have in the past said that the warrant renewal instrument should state that the Secretary of State still considers the activity to be necessary and proportionate. It is important that it is clear that the Secretary of State has applied their mind to necessity and proportionality when a warrant is renewed. Unfortunately however on occasion a shortened format renewal wording is still being used. This is something that I have said should be addressed.

iv. Covert Human Intelligence Source (CHIS)

A CHIS is essentially a person who is a member of, or acting on behalf of, one of the intelligence services or MoD and who is authorised to obtain information from people who do not know that this information will reach the intelligence agencies or armed services. A CHIS may be a member of the public or an undercover officer. Part II of RIPA and the associated code of practice provide the legal framework for authorising the use and conduct of a CHIS which is compatible with Article 8 of the ECHR (please see the appendix to this report).

The agencies maintain an unshakeable commitment of confidentiality regarding the identity of CHIS which remains indefinitely. Revealing the role a CHIS has played could result in reprisals by a state or an organisation which could threaten the life of the CHIS or their family. In conducting my oversight and in scrutinising the authorisations this is an important consideration.

My overall assessment of CHIS use and conduct

From the cases I have examined the applications for the use and conduct of CHIS have properly considered the necessity and proportionality and in particular considered possible invasion of privacy and the justification for this. **There are however, points to be made.**

- Duration of authorisations

During 2014 I noticed that some CHIS applications had been made for three months and some for twelve months. The code of practice suggests that an application for the use and conduct of a CHIS must be made for a twelve month period even if it is known at the outset that activity will only take place for a matter of days. I have suggested that under these circumstances, where it is arguable that it is neither necessary nor proportionate to issue for the full twelve month period, the agencies might consider issuing for a shorter period. However the convention at present is, and the code of practice would seem to support this, that warrants or authorisations be issued for the full period allowed and cancelled when no longer needed. It is argued that this allows a greater degree of certainty and simplicity in "policing" warrants and authorisations of a particular kind if they have the same lifespan. With this in mind I have **recommended** that authorisations should be for the full period but applications must be cancelled in good time as soon as it is known that they are no longer required.

- Undercover Operatives

The authorisation process for police undercover CHIS was amended on 1 January 2014 so that:

- authorised undercover operations must be notified to the Surveillance Commissioners as must their subsequent cancellation.

- a prior approval process by a Surveillance Commissioner is required for undercover operations employed by law enforcement agencies for longer than 12 months.

This did not extend to the intelligence services' or armed forces undercover officers' who have not had the same criticisms as the police (so have not been included in the various reviews or amended legislation). However, I have kept an eye on emerging recommendations. MI5 in particular has reviewed their policy and guidance and have improved their record keeping.

- MOD

It is not accepted by HMG that RIPA Part II applies to all relevant activity outside the UK but the MOD applies the principles and it is that application which I oversee. In the MOD CHIS authorisations are obtained and RIPA safeguards applied as if it did. In some applications for CHIS the paperwork focused on the privacy of the CHIS. I **recommended** that consideration must also be given to the privacy of the subject of investigation and any subsequent collateral intrusion. Having carefully questioned the MOD about this I am satisfied that full and proper consideration is being given to privacy so it just needs to be reflected in the paperwork.

- SIS

SIS is primarily a humint (human intelligence) organisation. They operate overseas under a section 7 class authorisation for agent running (CHIS). I have **recommended** that this is an area where SIS could improve their paperwork recording in one document all the relevant considerations relating to authorising a CHIS. I am satisfied that although RIPA does not apply, SIS seek to apply the same principles and that the relevant points are being considered in relation to authorising a CHIS. It would be better for operational reasons as well as from an oversight/compliance perspective if all relevant considerations were recorded in one document. When they have long term CHIS I have encouraged them to re-consider regularly whether the necessity and indeed proportionality case is still made out making it appropriate to continue tasking the CHIS.

- GCHQ

GCHQ is primarily a sigint (signals intelligence) organisation but they are able to undertake CHIS activity if it is in support of one of their statutory functions. I was content that GCHQ has systems in place to properly authorise and regularly review CHIS operations to ensure they remain necessary and proportionate and the authorisation remains justified.

- CHIS Reviews

In accordance with the code of practice CHIS activity must be kept under review to ensure that the use or conduct of the CHIS remains within the parameter of the extant authorisation because circumstances can change during the 12 month duration of the authority. The authorising officer should set the frequency of these

reviews. I have been concerned that these reviews are not always recorded as formally as they should be. In MI5 I have seen instances which imply that reviews have been ongoing even after tasking ceased so the "date reviewed" was clearly being automatically generated without a review taking place. This must not happen. In the new MI5 system, the authorising officer selects the review period and can comment on what they expect to see reviewed so the reviewing officer is required to manually populate the field to confirm that a review has taken place.

Conclusion

The level of intrusion into privacy in CHIS operations is relatively low level. Consideration must be given to the privacy of the CHIS and also to the subject of the investigation. The safety and welfare of the CHIS is essential and I take this into account when conducting my oversight. In the cases I reviewed I have been satisfied that proper consideration has been given to necessity and proportionality. My primary concern has been the duration of authorisations which must be authorised for 12 months so I have made it clear that they must be properly reviewed and cancelled when no longer required.

v. Intelligence Services Act (ISA) section 7 authorisations

ISA section 7 is intended to ensure that certain activity of SIS and GCHQ overseas, which might otherwise expose their officers or agents to criminal or civil liability in the UK, is exempt from any liability if authorised by the Secretary of State. A section 7 authorisation would of course have no effect on the law in the country where the act is to be performed. Under section 7 of ISA the Secretary of State (normally the Foreign Secretary) may authorise activity outside of the United Kingdom necessary for the agencies to properly discharge one of their functions. Authorisations may be for a particular operation or may relate to a broader class of operations. Before granting an authorisation the Secretary of State must be satisfied of the necessity and reasonableness of activity to be authorised. In this context reasonableness includes acting so as not to intrude on privacy any further than justified by the necessity to achieve what is authorised.

Privacy

Section 7 authorisations can be used for highly intrusive activities. Some operations under section 7 class authorisations are conducted under internal authorisations. To obtain an internal authorisation a case has to be made of necessity and proportionality for the intrusion into privacy. These are principles applied and accepted to apply whether or not the Convention on Human Rights or the Human Rights Act strictly applies. In other words anyone seeking authorisation to conduct a particular operation must make a strong case explaining why:

- less intrusive means cannot be used; and
- the necessity of obtaining the information outweighs the invasion of privacy.

Assessment of ISA section 7 authorisations use

There are two aspects of my oversight in this area. Firstly the grant of a section 7 and secondly internal approvals under that authorisation.

Oversight of the granting of a section 7 authorisation

Section 7 authorisations fulfil two functions. First they will relieve the officers acting in accordance with the authorisation from liability under UK law. Second they provide political approval of activities carried out under such an authorisation.

Some Non-Governmental Organisations have expressed concerns about the broad nature of section 7 authorisations and the fear that they may be used to permit SIS or GCHQ to commit serious offences. This is not the case:

- firstly the process for establishing the necessity of the intelligence required by the government and the priority for this is set for the agencies by government. The agencies do not self-task and must justify everything they do in relation to government priorities.

- secondly it is the Foreign Secretary who decides if the proposed operation is both necessary and reasonable. The Foreign Secretary is accountable to Parliament for the actions of both SIS and GCHQ.

Thirdly as I said in my report for 2013, GCHQ and SIS staff have no desire to operate unlawfully. In both SIS and GCHQ legal compliance is an integral part of the culture, but they do need protection for activities carried out abroad so far as section 7 can give it.

An application to the Foreign Secretary is accompanied by a submission which sets out the planned operation, the potential risks and intended benefits. They usually include a comprehensive legal annex and most importantly from my perspective, includes why any intrusion into privacy is justified by the intelligence sought to be obtained. These applications are submitted through the Foreign Office who provides additional comments for the Foreign Secretary to consider. The Foreign Office are also accountable to me for any decisions they take and I am satisfied that they can and do refer applications back to the relevant agency if they are not satisfied about any aspect of the proposal.

Class Authorisations

Class authorisations cover the essential and routine business of SIS and GCHQ. Again they fulfil two functions. First they give protection for liability under UK law and second they provide political approval for activities authorised by the class authorisation.

I oversee the use of section 7 authorisations by visiting GCHQ and SIS and the warrantry unit of the Foreign Office. But SIS is tasked with operating overseas, dealing with threats and gathering intelligence in order to protect the UK and UK interests, and an important element of my SIS oversight is to visit and scrutinise certain of the overseas stations in which they operate. On these visits I have two main priorities:

- to check that legal requirements set out in the authorisations are being complied with; and
- to see how staff operate in-country and the ethics and principles they apply.

In all my visits I have been impressed at the dedication of the officers and by their evident desire to act in accordance with high ethical principles. This in fact goes for all those that work for the agencies and the MOD whether home or abroad.

- SIS Internal Approvals

For each operation there is a controlling officer in the UK who is in constant communication with the overseas station.

Although RIPA does not apply to the majority of SIS activity overseas, in overseeing the internal use of class authorisations I look to see that the principles are applied. I do this by:

- looking at the audit trail setting out the thought process, in large measure recorded in e-mails with the controlling office in Head Office; and
- checking the necessity and proportionality of activity taking place.

I have **recommended** that SIS implement a better audit trail of operations taking place similar to the RIPA procedure used in the UK. This would allow for improved accountability for the work and allow greater oversight by management as well as by me as Commissioner. I am confident that proper consideration is given to the necessity and proportionality from my interviews and the e-mail trail but it is not currently possible to see this set out in one document and can be a time consuming process to find.

I have also **recommended** that when I visit stations overseas I am provided with the stations' operational objectives, priorities and resources to help reassure me that all of the work undertaken is properly authorised and in support of their statutory functions.

- GCHQ Internal Approvals

GCHQ primarily operate under class authorisations and have very few specific section 7s. They provide for my oversight the internal approvals they make under each class authorisation and have implemented my **recommendation** to ensure that the paperwork reflects that these approvals are only valid as long as the class authorisation is in place. They are approved by a GCHQ senior official but if there is any additional sensitivity or political risk it will only be signed after a senior Foreign Office official or the Foreign Secretary has been consulted and agreed the operation is appropriate. I have made it clear that the senior official cannot authorise necessity and proportionality; this decision must be made by the Secretary of State and cannot be delegated.

GCHQ's internal approvals are supplemented by what they call an "addition". To help me to gain a better understanding I spent a day in GCHQ:

- looking more closely at the system;
- questioning the staff who undertake the approvals; and
- questioning the staff who undertake the activity.

I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion.

I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I **recommended** that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ.

vi. Consolidated Guidance

Figure 5: Areas subject to my oversight include:

- When a detainee is interviewed by UK personnel whilst in the custody of a third party
- When information is sought by HMG from a detainee in the custody of a third party
- When unsolicited intelligence related to a detainee is received from a third party
- When information is passed from HMG to a liaison service in relation to a detainee
- When soliciting the detention of an individual by a third party

On 27 November 2014, under section 59A of RIPA, the Prime Minister published a direction which put my oversight of the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees (the Consolidated Guidance) onto a statutory footing. The Consolidated Guidance sets out principles that UK intelligence and security agency officers and members of the UK Armed forces and employees of the Ministry of Defence must adhere to when they interview detainees overseas or pass and receive intelligence relating to detainees.

How I oversee the Consolidated Guidance

I oversee the Consolidated Guidance during my formal inspections of the agencies. I follow the same method to review the Consolidated Guidance as I use for other areas within my remit. Further detail on how I fulfil my oversight can be found in my 2013 Annual Report.

My objective is to ensure that intelligence officers and military personnel are aware of and follow the Consolidated Guidance so that when they are faced with situations which involve detainees, they are able to apply the Guidance and take decisions at the correct level. I do this by:

- reviewing the "detainee grid" which sets out the date, details of occasions when the agencies have assessed that there may be a need to apply the Consolidated Guidance or where the Consolidated Guidance has been applied including the operation/overarching submission, risk assessment, reference to senior personnel, legal advisors or Minister and the level at which the decision was taken.
- reviewing the audit trial which demonstrates that operational staff engaged in detainee matters are following the Guidance.
- ensuring that the agencies are providing the appropriate levels of assurance to me and Ministers that the Guidance is being followed.

Developing the Grid

Cases of the Consolidated Guidance which fall within my remit[2] are set out for me in a grid format for me to select from. The grid has developed over the years but my preference is that it sets out what liaison country and liaison service is involved and then reflects under headings the following questions:

- Are you passing information relating to an existing detainee?
- Is this a detention request or is detention the likely outcome?
- Are you attending the interview of detainee?
- Will information be put to a detainee?
- Is information to be derived from a detainee?
- Is there serious risk of mistreatment?

The grid will also set out for me who was consulted, the level the decision was taken and a narrative of the action taken.

This format directs people through the consolidated guidance process and if all the answers are "no" then the guidance needs no further consideration. I have **recommended** that, rather than sticking to a strict date order, operations should be grouped together so that I can review every occasion it has been considered.

I select a random sample of cases for closer scrutiny although in doing so I try to ensure that I select different foreign liaison services as well as different decision levels.

During my inspection I review the detainee grid in relation to the cases I selected to ensure that the grid has been completed accurately. If it has then I believe I can be assured that the consolidated guidance process is being followed in all cases.

In my report for 2013 I **recommended** to SIS that they ensure they capture all cases in stations overseas where consideration was given as to whether the guidance applied even if a decision was taken ultimately that it did not. They implemented an email system of selection. This ensured that I could also see cases where the guidance was considered and a decision taken either that the guidance was not engaged or that intelligence was not to be shared. However at the start of 2014 I **recommended** to SIS that they consider how this method of selection could be more formalised. SIS responded to this by converting their emails from the group email box into a grid format. This was an improvement with both the benefit of the grid and the flexibility required for a global organisation but I **recommended** that they set out their grid in my preferred method.

2 The areas that fall within my remit are set out in full on my website and in the Prime Minister's direction in the appendix to this report. It does not relate to people in the custody of the UK.

I also **recommended** to GCHQ and MI5 that they reformat their grid so that it reflected in more detail the level that the decisions were taken.

Form

To support the grid both MOD and MI5 have very useful forms in terms of the way they force consideration of the relevant questions. These forms are also available for my inspection. I have **recommended** that GCHQ and SIS consider having similar forms.

Liaison Relationships

An important part of my oversight of the guidance relates to the risks associated with working with overseas liaison partners and how the agencies mitigate against any risk. In November 2014 the Prime Minister tasked me to examine the concerns the ISC raised on the government's responsibilities in relation to partner counter-terrorism units overseas. As part of this inquiry I am seeking to establish whether the procedures now in place address the concerns of the ISC. I will report on this further when my inquiry is complete.

During station visits I am briefed and discuss with intelligence officers their work with liaison partners. This is a highly sensitive and complex area in which to operate. The obtaining of assurances upon which, for example, decisions around the passing and receipt of intelligence in relation to detainees are often based is vital as is the assessment of the extent they can be relied on.

During my inspections I have asked the agencies to inform me about significant developments in knowledge or belief that mistreatment has occurred. I have asked that these developments are recorded to help build up a record of behaviour with the liaison service. This is already covered by SIS's compliance work within the Consolidated Guidance.

Due Process

On occasion there may be cases where there is a greater than serious risk of a detainee being denied due process. Individuals must be allowed access to a lawyer and be given the opportunity to appear before a judge and ultimately have a fair trial. As part of the country assessment it is important to understand what legal system is in place and a qualitative assessment made of whether the system will be followed. I have **recommended** that as well as recording the specific assurances sought, there should be an assessment of whether it is likely that the liaison service in question will comply with those assurances.

Assurances

I have emphasised the importance of obtaining signed written assurances from the foreign liaison but failing that to provide liaison with a written record of the assurances provided verbally. It is obviously preferable to obtain signed written assurances but if this is not possible I have **recommended** that assurances must

be recorded in writing and sent to liaison as a preference to relying on verbal assurances.

Sharing intelligence *in extremis*

Paragraph 12 of the Consolidated Guidance allows for time sensitive military operations which involve questioning a detainee held by another liaison partner when time constraints do not allow the opportunity to apply the Guidance in advance. In such circumstances they must apply the Guidance "so far as it is practicable" and report to senior personnel as soon as possible. The Guidance does not have some general provision allowing for example the sharing of intelligence in extremis situations where lives are at risk.

MOD brought a situation to my attention which involved sharing intelligence with foreign liaison during a time sensitive operation when there were lives at risk. There was no opportunity to refer to senior personnel or Ministers for guidance on any concerns over standards of detention or treatment so a decision had to be taken by the most senior person present. I consider there to be an oversight in the Guidance which does not allow for a more general application of such a principle. I **recommend** that the Consolidated Guidance be amended to allow for in extremis sharing of intelligence.

Informing Liaison that no intelligence was held

On occasion the intelligence agencies receive trace requests from liaison partners seeking information about individuals already in their detention or who are judged likely to be detained. The question has arisen as to whether a 'no trace' reply was the passing of intelligence to which the Guidance applied. If the Guidance applied that might lead to a person being continued to be detained while authorisation was sought for making such a reply. In such circumstances I have said a 'no trace' reply was not 'passing of intelligence' to which the Consolidated Guidance applied.

Statistics

In my report for 2013 I published statistics for the first time indicating the number of occasions when the Consolidated Guidance has been applied and the extent of my checking. When I did so I explained that the figure can easily be misrepresented both by the public and misused by those who might wish to do this country harm, or make false allegations against it. I have decided that I would continue to give these figures, but with strong warning against misrepresentation.

The total number of cases where the Consolidated guidance was considered during 2014 was 516. I have full details of all 516 including what decision was taken and by whom. The statistics do not show the number of individuals subject to unacceptable conduct; only that proper consideration was being given to that risk in a number of cases.

It is important to emphasise that what I am seeking to monitor is whether the Guidance is being followed so that when a detainee of a third party is involved, people immediately appreciate the Guidance should be considered and that decisions are then taken at the correct level. I do this scrutinising by the grid setting out the way in which the Guidance was applied in the 516 cases and taking a random sample to cross check that the information with which I am being supplied is accurate. That sample was 64 ie 12.5% of the 516 cases.

Conclusion

In all the instances I reviewed staff demonstrated they had considered the risk of mistreatment or unacceptable conduct of any detainee as set out in paragraphs 9 – 11 of the Consolidated Guidance. I found that the grids presented to me had been completed properly.

Because SIS staff work with overseas liaison they have a more difficult role to play and are most likely to have to consider Consolidated Guidance issues. They will work with liaison to help mitigate risk of mistreatment and seek signed assurances that detainees will be treated in accordance with those assurances. GCHQ, MI5 and the MOD may rely on SIS in relation to country assessments and assurances. I noted that SIS record keeping for Consolidated Guidance issues has improved. Their new system for selection captures cases where the Guidance has been considered even when it does not apply. Senior managers in SIS are keen to see record keeping improve and have agreed to talk to overseas staff about this.

vii. Bulk Personal Data

On 12 March this year, under section 59A of RIPA (as inserted by section 5 of the Justice and Security Act 2013), the Prime Minister published a direction which continued and put on a statutory footing my oversight of the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets, including the misuse of data and how this is prevented. Essentially I oversee how the intelligence services store and use bulk personal data (BPD).

There is no statutory definition of BPD, but in essence BPD refers to data belonging to a range of individuals acquired by or held on one or more analytical systems in the intelligence services. The majority of these individuals are unlikely to be of intelligence interest. I consider the most important aspect of my role is to see that the agencies have systems in place to protect privacy of those individuals.

Acquisition and Retention of Bulk Data

Section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 provide, in effect, that the intelligence services may only obtain information for the proper discharge of their functions.

In addition, section 19 of the Counter-Terrorism Act 2008:

- allows a person to disclose information to any of the intelligence services for one of those functions;
- permits information they obtain in connection with one function to be used by the intelligence services in connection with any of their other functions; and
- provides that disclosing information to the intelligence services overrides any duty of confidentiality or other restriction on disclosure.

The Head of each agency is responsible for ensuring that no information is obtained or disclosed unless it is necessary for the proper discharge of its functions.

So far as BPD is concerned each dataset is separately authorised before it is made available on analytical systems for use by intelligence officers. The authorisation sets out the necessity and proportionality argument for exploiting the data and considers any sensitive data which might be included in that dataset.

The agencies assess each dataset individually including:

- a statement of necessity for retaining the dataset,
- an assessment of intrusion into privacy,
- measures to minimise intrusion into privacy.

The agencies each have a review panel of senior managers who meet regularly to review:

- the retention of datasets,
- the decision to ingest any new dataset into analytical systems,
- examples of its use during any previous period,
- the decision to delete datasets.

Some datasets have very little private data or even publicly available data in them so the justification for retention is much easier as long as the dataset is still being used and contributing towards the aims of the organisation. Other datasets may contain intrusive data and any containing sensitive confidential data should be flagged.

Data Protection Act

Each agency recognises that the acquisition, retention, exploitation and disclosure of personal data about individuals constitutes "processing" for the purpose of the Data Protection Act (DPA). Any such processing of personal data therefore has to be considered under the DPA. However, the processing involved in the acquisition, disclosure and exploitation of personal data is exempt from specific provisions of the DPA where such exemption is required in order to safeguard national security. In such cases a Minister of the Crown may issue a certificate under section 28(2) of the DPA, confirming that the exemption under 28(1) is required, such a certificate being conclusive evidence of that fact. In accordance with section 28(3), the ministerial certificate may identify the personal data to which it applies by means of a general description and be prospective in its effect. The agencies' certificates effectively provide exemption from the 1st, 2nd, 6th and 8th Data Protection Principles (DPPs). In summary:

DPP		
1st	Personal data shall be processed fairly and lawfully	EXEMPT
2nd	Personal data shall be obtained and processed only for specified and lawful purpose	EXEMPT
3rd	Personal data shall be adequate, relevant and not excessive in relation to the (statutory) purpose for which they are processed	NOT EXEMPT
4th	Personal data shall not be kept for longer than is necessary for the (statutory) purpose for which they are being processed	NOT EXEMPT
5th	Personal data shall not be kept for longer than is necessary for the (statutory) purpose for which they are being processed	NOT EXEMPT
6th	Personal data shall be processed in accordance with the rights of the data subject	EXEMPT
7th	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data	NOT EXEMPT
8th	Personal data shall not be transferred outside the European Economic Area unless the relevant country ensures an adequate level of protection for the rights of the data subject	EXEMPT

It is also still open to the agencies to argue on a case by case basis that exemption from one or more of the DPPs was required in order to safeguard national security.

How I oversee Bulk Personal Data

In summary I oversee BPD in a number of ways.

- first I require the services to provide me with a full list of all datasets they hold. I see the records of the internal review bodies which consider the retention of datasets. I inspect these documents along with the formal justification for acquiring the dataset and making it available for use on analytical systems. I assess whether the review bodies have properly applied the test of necessity and proportionality in retaining and making the data available.
- I then inspect how members of the intelligence services access the data sets including the training required before gaining access and restrictions in place to limit access as well as reviewing how they apply the necessity and proportionality justifications of intrusion into private information.
- finally I review the possible misuse of BPD and how this is prevented. This is a key part of my oversight. Access to BPD must be tightly controlled and

what must be guarded against is the risk that some individuals will misuse the powers of access to private data.

As part of my oversight I ask for an explanation of how the datasets I select for closer examination are used. In general I have no difficulty with the justification for retaining the datasets. In essence the justification will be that although the particular dataset has information on individuals of no intelligence interest it will also have important information on persons who will be or are of intelligence interest and which will provide important links assisting in the identification or movements of those individuals.

It is important I stress that the acquisition of datasets can be justified on the basis that it is necessary and proportionate to have them. Thus for example, in SIS with two linked older datasets I had concerns that they had acquired them for one reason and now wished to use them for another. I have required SIS to:

- provide me with justification for the necessity and proportionality for continued retention; and
- keep the datasets locked up until/unless their data review panel approve their continued use and I have had a chance to review that decision.

Training

Before officers are allowed access to BPD they must undergo formal training and in MI5 agree to and sign a code of conduct. The training explains that users have personal responsibility for any use of the system and managers are responsible for their staff. The code of conduct explains that BPD needs to be managed to ensure that the privacy of those whose data is held is respected and that data is held, accessed and disclosed only to the extent necessary for the purpose of the statutory functions of the agency and where it is proportionate to those aims.

This standard is reflected at the other two agencies without a formal code of conduct.

Use

The agencies have systems in place to ensure that BPD cannot be trawled indiscriminately by analysts. Access to BPD is restricted by individual user login. If an officer gives their personal login to someone else or leaves their system unattended this is considered a security breach and subject to disciplinary procedures. The login is post specific.

Before an individual analyst is allowed access to BPD GCHQ have a system in place which requires them to justify the necessity and proportionality of their proposed search. This justification box is audited regularly and available to me for inspection.

SIS have also introduced a system where officers have to complete mandatory fields setting out the purpose of the search and justification for the search (business need) in the free text box.

I was pleased to see that SIS implemented a system but was not satisfied that it prompted the user to consider if the anticipated invasion into privacy would be justified by the desired outcome. I have **recommended** that they amend the fields to reflect how a decision is made, that access to the BPD and possible intrusion into privacy is justified.

MI5 does not use a "justification box" but require their analysts to adhere to their internal policies and guidance which require that searches must be necessary and proportionate for the business they are conducting. Adherence to policy is in part achieved by user training, signing a code of conduct and their protective monitoring regime. BPD access is also restricted to staff who have a valid business reason to use BPD.

During my selection of SIS's bulk data I had particular concern about datasets which had been obtained but not yet put onto analytical systems. I required SIS to provide me with a list of all datasets they had acquired but were not currently exploiting including the date they acquired each dataset. SIS provided the list on the inspection day along with an explanation of each dataset. I made clear that SIS cannot justify the necessity for retaining datasets if they have not been exploited within a reasonable period and **recommended** that they should be deleted unless an exceptional case for necessity can be made. This is a point which I have also taken up with GCHQ and MI5.

Each agency has a limited number of specialist analysts who can perform more detailed searches by reference to particular datasets, but again they are subject to the same policy, guidance and safeguards such as through protective monitoring of their enquiries. I take into account this advanced ability to search datasets when I scrutinise their use of BPD.

Protective Monitoring of BPD

In my oversight of BPD I monitor extremely carefully the steps taken to see how the misuse of BPD is prevented.

Access to BPD is audited through a system of protective monitoring by all agencies. To provide me with confidence in the system as a whole I do not limit my oversight of protective monitoring to BPD so I scrutinise details of general misuse of information and security breaches.

In all three services there is an automatic monitoring system which uses predefined search terms as well as random audits of individual users. I scrutinise these search terms and the results of the audit as part of my oversight. Obviously it would be

inappropriate to give details of the way the monitoring works in a public document. Queries arising from these audits were primarily "false positives"; that is although they initially met a search term designed to catch misuse there is, on investigation, a fully justified explanation for their use in each case.

Misuse of Bulk Data

The agencies take any deliberate misuse of the system seriously and sanctions include dismissal, revocation of security clearance and possible criminal prosecution. Any breach of the system may result in a breach notice being issued. When a breach notice is served it remains on a person's personnel file (HR record) and is taken into account in the event of any subsequent breach.

When I first began monitoring misuse of data there were two serious breaches where officers had undertaken unnecessary queries of bulk data with no proper business justification. Both were contractors and in both cases, following investigation they were escorted from the premises and their contract revoked. Fortunately such action is rare but I am very clear that the agencies accept that any inappropriate use is unacceptable and will be treated very seriously.

Unacceptable uses are in fact few in number and not as serious as the cases referred to. For example well intentioned work-related instances such as failure to properly limit the parameters of a search are treated as serious breaches and I have made it clear that this it is absolutely right that that should be so.

In MI5 a note has been circulated to all users informing them of my recommendation endorsing MI5's policy to tighten up its procedures so that data on staff remains properly protected. The note introduced an automatic security breach if the procedures were not followed. There has not been a single breach in MI5 for access to BPD since that note was circulated.

In one recent instance of misuse in SIS an officer accessed the BPD system despite having moved to another role which did not require access. The access was for a legitimate work purpose but still unacceptable and a breach notice was issued. However, I informed SIS that the corporate failure which allowed the officer to retain access to the system was a more serious breach.

BPD systems hold highly personal data and it is vital that staff only have access if they have a business need. The officer should not have been able to retain access to the system after moving post so I have asked SIS:

- to investigate if any more staff have access bulk data when they do not have a business need and to update me on this investigation;
- to inform me what has been done to ensure people are removed from the bulk data register when they move post.

I have **recommended** to all three intelligence services that they work together to treat all misuse of data in the same way to ensure fairness to all staff.

Conclusion

The case for holding BPD has been established in each service. The data review panels consider and regularly review the necessity and proportionality of retaining data. They also recommend deleting any datasets which cannot be justified for retention. When datasets are acquired there is a good system in place to consider if the dataset should be incorporated into analytical systems and made available to users.

The agencies all have strict procedures in relation to handling, retention and deletion.

Misuse of data is fortunately rare. My experience is that officers work with a high degree of integrity and an awareness that the systems they have access to contain highly sensitive information which must be protected.

Access to information held on BDP must be justified so the vast majority of data the agencies acquire is not used because no case can be made justifying access to it.

I have made a number of recommendations relating to the agencies use, retention and protective monitoring of BPD. Most of these recommendations have related to improving privacy considerations or protecting individual privacy.

5. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS

This chapter is concerned with product obtained through warrants or internal authorisations.

I have noted that submissions often state that "normal procedures" would be adopted for handling any product obtained. However, unlike the Interception of Communications Commissioner I do not have express oversight of these arrangements. With this in mind in the confidential annex to my report for 2013, using the power given to me under RIPA s59A(3) I asked the Prime Minister to extend my oversight to the use by the agencies of operational data obtained under Part II of RIPA or ISA sections 5 and 7. I have repeated this request this year but in the mean time I consider that on a broad reading of my remit I can and should oversee at least the retention storage and deletion of product obtained from those warrants and authorisations which fall within his remit.

I am considering how I can oversee the agencies compliance. Taking into account the existing statutory oversight undertaken by the Interception of Communications Commissioner I will particularly focus on:

- the retention policy for information which is not of intelligence interest (which should by preference be immediately destroyed);
- the procedure used to handle information retained for evidential purposes which could include information which is not of intelligence interest;
- the procedure to handle unwanted information so that submissions would not need to set this out each time; they could simply refer to the policy;
- the policy for deletion of all product; and
- procedures enforcing compliance with handling arrangements.

6. ERRORS

Figure 6: Categories of errors

Category A

An administrative error such as where a typing error has occurred and the correction is obvious

Category B

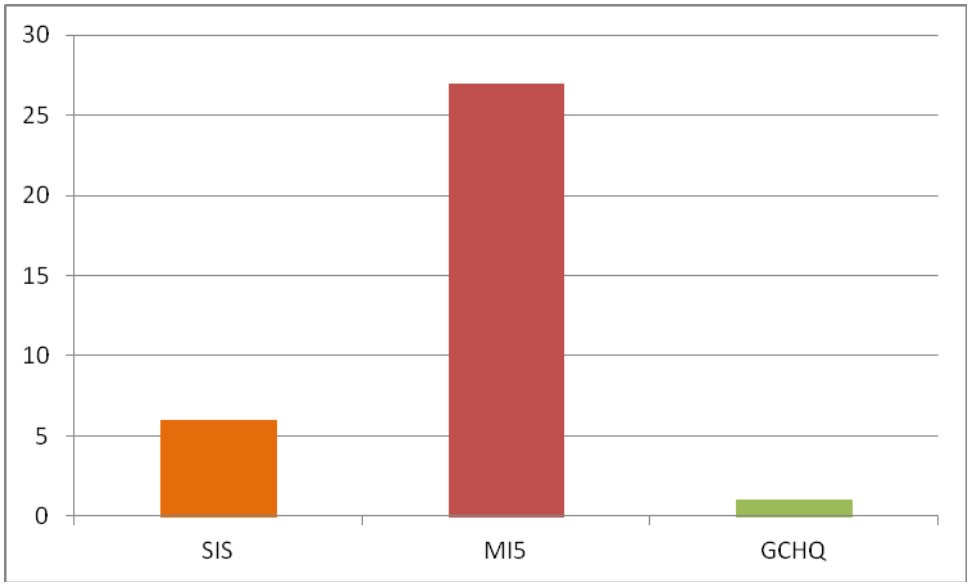
A situation where there has been, for example, an inadvertent failure to renew a warrant or obtain authorisation in time and where, if done properly, the application would have been granted

Category C

A deliberate decision to obtain information without proper authority and with no intention to obtain proper authority.

In addition to my bi-annual inspections, I require the agencies to report to me any errors that might have occurred during a warrant application, authorisation or when the warrant was put into operation. Examining these reports is an important element of my oversight of how the agencies use their intrusive powers. I expect the reports to explain: (1) when an error occurred, (2) when it was discovered, (3) the nature of the error, (4) how it happened and (5) what, if any, unauthorised invasion of privacy resulted. The reports also include details of the steps taken to avoid errors happening again. In 2014 there were **43 errors**. The agencies reported **34 errors** to me and I discovered nine during my inspections.

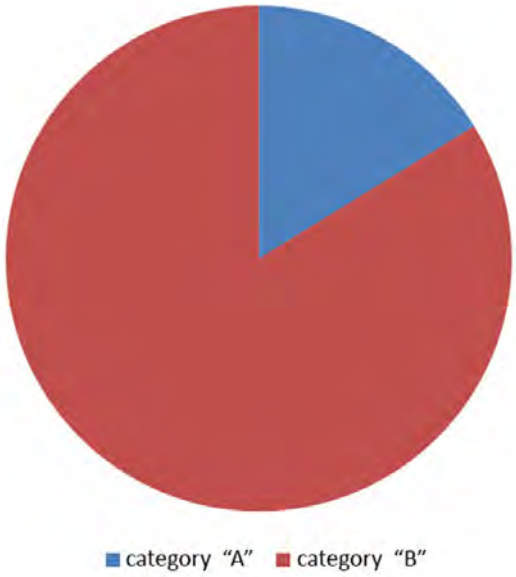
Figure 7: Number of errors reported in 2014



Please note that MI5 obtain a larger number of warrants and authorisations than the other agencies, so their error rate is low as a proportion of authorisations.

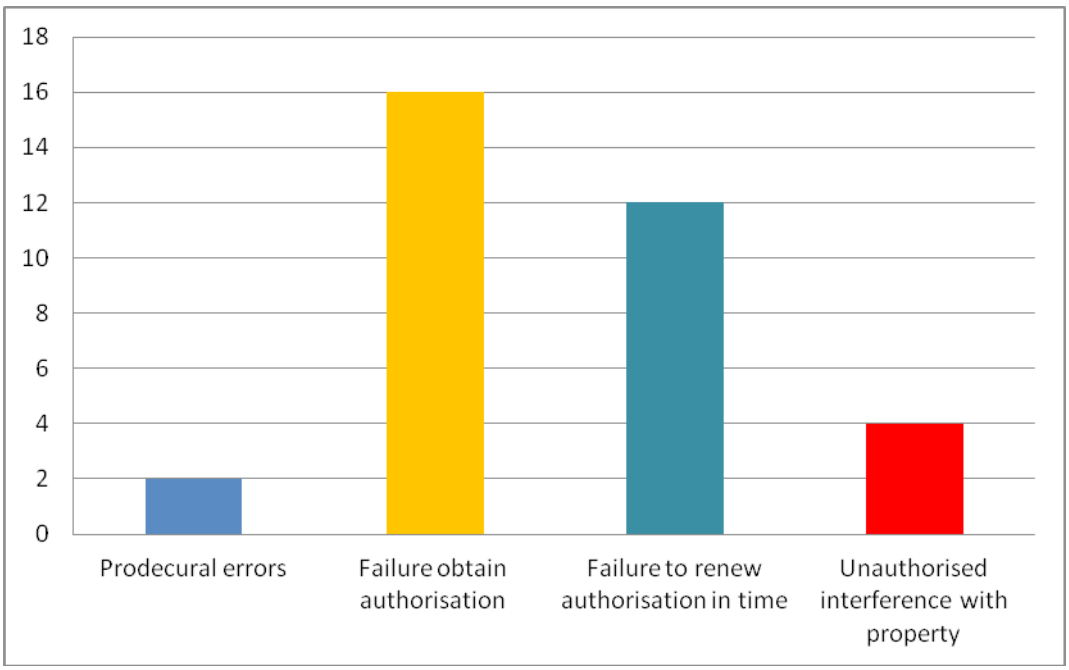
All of the errors reported to me were caused by human error and all resulted in intrusions into privacy to some degree. None were deliberately caused by those involved. Of these, 31 were Category "B" errors or inadvertent errors and 6 were category "A" or administrative errors:

Figure 8: Errors reported in 2014 by category



Of all the errors, the most common error was because of a failure to obtain authorisation in time. The least common error was due to unauthorised interference with property.

Figure 9: Types of errors reported in 2014



Breakdown of errors by organisation

Security Service (MI5)

In 2014, MI5 reported 27 errors to me. I discovered an additional four Category "A" administrative errors during my inspections.

Of the 31 errors:

- almost all were caused by human error and all resulted in intrusion into privacy to some degree;
- none were caused with the intent to obtain information without the proper authority;
- 10 were the result of a failure to renew an authorisation in time;
- 12 were the result of a failure to obtain authorisation;
- 4 were the result of unauthorised interference with property;
- 5 were the result of procedural errors.

MI5 reported an error which occurred when a Directed Surveillance Authorisation (DSA) lapsed because of an administrative oversight. The original authorisation was obtained to assist in identifying and disrupting new terrorist activity.

The investigation team discovered the error seven days after the authorisation had expired while they were reviewing the DSA. During the period when there was no authorisation in place surveillance had continued but they did not review the surveillance product and deleted it from MI5's systems because they assessed it not to be of intelligence interest. The investigation team responsible for the error were reminded of the importance of renewing authorisations in a timely way.

I have had some concerns which I have raised during my inspections as to the circumstances in which it was permissible to retain product obtained when through an "unintentional error" there was no authorisation in place. I was first inclined to the view that it should take exceptional circumstances to allow retention, but I have been persuaded that if the circumstances are ones in which 1) authorisations would have been granted if sought and 2) retaining the product is necessary and proportionate in the interests of national security, it is not in the public interest to prevent such product being retained.

Administrative errors

During my inspection I discovered four typological errors including one where the date was shown to be 2010 instead of 2012 on a warrant. These were errors at the Home Office but I reminded MI5 that when they review warrants they should check it since it is they who need the authority to act lawfully.

SIS

In 2014, SIS reported six errors to me. During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

Of the six errors:

- almost all were caused by human error and resulted in intrusion into privacy to some degree;
- none were caused with the intention to obtain information without the proper authority;
- two were the result of a failure to renew an authorisation in time;
- four were the result of a failure to obtain an authorisation.

SIS reported an error which occurred when an officer failed to obtain an authorisation.

Although the operational team initiated an electronic RIPA authorisation 10 days before the operation was due to take place, it was not approved until after the operation had been carried out. The initiating officer did not carry out a final check that the authorisation was in place before the operation went ahead. The team's RIPA co-ordinator discovered the error during a review of the RIPA authorisation requests.

The team destroyed all the information gathered during the operation and they implemented a new monitoring system for RIPA requests to ensure that breaches did not occur again. The SIS Compliance Team gave the operational team involved a reminder briefing on RIPA requirements.

GCHQ

In 2014, GCHQ reported one error to me which happened when an internal monitoring system of some staff communications was found to be capturing more information than it was authorised to. I followed up on this error during my May inspection and the team explained that because of a lack of understanding of the systems' full capability more data than had been authorised had been collected. It was clear to me that this was a technical error and not deliberate. Following the discovery of the error GCHQ deleted the captured data and reconfigured the system to ensure that it only collected the information that it was authorised to collect. I continue to monitor this project to ensure that this error does not happen again.

Administrative errors

During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

Home Office

During my inspection of the Home Office Warrantry Unit, I discovered three administrative errors or Category "A" errors which I asked the Home Office to write formally to me about.

- The first error happened when a warrant incorrectly referred to an operation as a counter-espionage investigation when it was in fact an investigation into Islamist terrorism.
- The second error was a typographical error. The Home Office, on behalf of MI5, sought urgent authorisation from the Home Secretary to conduct activity in response to an urgent operational requirement. However, the application for the warrant which was signed by a Senior Official under the authority of the Home Secretary contained a typographical error which erroneously stated that the authorisation was specified in 1(ii) of the warrant, when it was in fact specified in 1(iii). The error was identified promptly, the warrant cancelled and replaced with a new warrant before any unauthorised action was taken.
- The third error was also a typographical error which included incorrect wording which only authorised one specified property belonging to the subject rather than several properties.

Ministry of Defence

In 2014, the Ministry of Defence did not report any errors to me. However I discovered two slips or Category "A" errors during my inspections.

The first error happened when an authorising officer failed to cross out "disagreed" in a warrant. To do so was required as part of the form to be completed at the time. However, I was informed during the inspection that the form had been updated and the new form did not have the requirement to strike out "disagree".

The second error happened when a directed surveillance authority (DSA) was only renewed two days after the original authority had expired. Although there was no unauthorised invasion of privacy, I advised the MOD that they should have made another application for a new authorisation rather than a renewal, once they had realised the original authorisation had expired.

Category C errors

Once again this year, I have not found any Category "C" errors. A Category "C" error or act is essentially when someone takes a deliberate decision to obtain information without proper authorisation and with no intention to obtain authorisation. In my 2013 Annual Report, I said that it would require dishonesty on the part of more than one person including a person of some seniority for such a situation to take place without discovery. However, in his latest report, the Interception of Communications Commissioner disclosed that a GCHQ employee

deliberately undertook a number of unauthorised searches. This error did not occur within the boundaries of my oversight, but it demonstrates the need to remain vigilant.

Despite this, I would emphasise that the likelihood of a Category "C" error occurring is low for the reasons I articulated in my Annual Report for 2013. Were I to discover such a deliberate decision, I would report it to the Prime Minister immediately and notify the Crown Prosecution Service.

Area of concern – delays in reporting errors

During 2014 I expressed concern that the agencies did not report errors in a timely way. I raised this issue both during inspections and in writing and asked for an explanation for the delays in reporting. The agencies responded that the length of time it took to complete internal reviews and investigations into errors caused the delay.

As a result I now require the agencies to notify me as soon as they anticipate that an error investigation will take longer than the three month limit for reporting.

7. BRIEF SUMMARY OF ASSESSMENTS

SIS

	Round 1	Round 2
Selection	20 March	30 October
Pre-Reading days	16 April	17 November
Inspection days	1-2 May	24 – 25 November
Station Visits	1-9 April (South America)	31 July – 1 August 2014 (North America)
Under the bonnet	14 January and 19 November 2014	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading at SIS made out the case for necessity in all the individual cases.
Proportionality **Was the case for proportionality made In each case inspected?**	The paperwork I selected made the case for proportionality apart from one case where the authorisation had not set out if intelligence could be gained by other less intrusive means. However, after challenging the case officer I was content that the case could be made.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Most of the paperwork I selected for reading made the case for privacy. In one case where internal authorisations were being made under a thematic property warrant, proportionality and privacy were not set out in enough detail to reassure me that proper consideration had been given. The warrant set out the details in full but I would like to see separate consideration in the individual internal authorisation. Consideration must always be given to collateral intrusion and what will happen to any information acquired or where none was expected.

Warrantry and authorisations

SIS take compliance seriously. It would however be better if instead of following an e-mail trail they recorded their considerations including necessity and proportionality in one document preferably a form which pointed to the questions to be considered.

I will continue to monitor closely:

- error reporting;
- record keeping

During my first under the bonnet visit I saw an example of the processes in place in SIS to help ensure their actions are legally compliant. In my second visit to a planning meeting I saw how teams consider where resources should be focused and look at legal and compliance issues.

I made a number of recommendations mostly in relation to ensuring SIS made a written record in one place. When I challenged the officers they demonstrated they had properly considered the necessity and proportionality but I would like to see it recorded. I continue to monitor thematic property warrants.

Bulk Personal Data

SIS have a proper system in place for considering whether BPD sets should be held and retained; they have good systems in place to ensure analysts have to justify access on a necessity and proportionality test which means that searches are aimed at subjects of intelligence interest; and they have a strong monitoring system to prevent individuals misusing BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved SIS take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they do comply with the guidance but this is an area where putting all the considerations on one form would be an improvement.

MI5

	Round 1	Round 2
Selection	20 May	15 November
Pre-Reading days	11 & 12 June 2014	27 – 29 November
Inspection days	20 June 2014	11 December 2014
Under the bonnet	15 April 2014 and 13 January 2015	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity in all individual cases.
Proportionality **Was the case for proportionality made in each case inspected?**	The paperwork I selected for reading made the case for proportionality.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out in the paperwork selected for reading. However, I noted that the paperwork for some urgent warrants did not have a separate box for considering privacy. At my request MI5 provided a copy of their "handling arrangements" concerning how operational data obtained from warrants and authorisations is managed and shared.

Warrantry and authorisations

MI5 also take compliance extremely seriously. I made a number of **recommendations** about selecting and presenting warrants in order to develop a broader picture of operations and handling arrangements where I was concerned in one case about the retention, storage and deletion of product obtained from a warrant.

My under the bonnet inspections supported my view that there is a high level of professionalism and a great deal of rigour given to the authorisation process. I will continue to monitor closely thematic warrants and the protections in place concerning product obtained without proper authority due to administrative errors.

Bulk Personal Data

MI5 have good systems in place to make sure the retention of and access to BPD is justified. They also have good systems in place to ensure that analysts only have access to BPD if they can justify the necessity and proportionality of their access with the result that intrusion into privacy is as far as it can be limited to that of subjects of intelligence interest. MI5 also have a good monitoring system in place to prevent individuals misusing BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved MI5 take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they have a good form which has to be filled out demonstrating in one place all the relevant considerations and compliance with the guidance.

GCHQ

	Round 1	Round 2
Selection	6 May 2014	2 October 2014
Inspection days	27 and 28 May 2014	11-12 November 2014
Under the bonnet	11 September 14 and 9 December 14	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made out the case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	In the paperwork I selected for reading the case for proportionality was set out
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out for the operations I selected for inspection. GCHQ have recently updated their RIPA template and renewals now have separate headings forcing applicants to outline separately proportionality and the anticipated degree of intrusion into privacy.

Warrantry and authorisations

GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips. Following a recommendation I made during my May inspection, GCHQ agreed to propose a new form of words for warrants which make it clear that the Secretary of State is authorising on the basis that GCHQ will act in accordance with the accompanying submission. I made a number of recommendations primarily concerning the conditions set out in the submissions and instruments. I will continue to monitor thematic property warrants closely.

My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration given to each operation; it was clear to me that a great deal of thought was going into the process.

Bulk Personal Data

GCHQ have a strong system in place which considers on a regular basis whether the retention is and continues to be justified. They also ensure that analysts must justify their access and demonstrate both necessity and proportionality with the result that intrusion into privacy is so far as possible aimed at subjects of intelligence interest. They also have a strong monitoring system to prevent improper access to the BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved GCHQ take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they do comply with the guidance.

MOD

	Round 1	Round 2
Selection	8 May 2014	4 November 2014
Inspection days	16 & 21 May 2014	26 November 2014

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity.
Proportionality **Was the case for proportionality made In each case inspected?**	The paperwork I selected made the case for proportionality.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The privacy argument was set out in the paperwork I selected for reading. In some applications for CHIS the paperwork focused on the privacy of the CHIS. I advised that consideration must also be given in the paperwork to the privacy of the target of the tasking and any subsequent collateral intrusion.

Authorisations

MOD voluntarily apply a high compliance standard to RIPA principles. Generally the paperwork provided by the MOD was in good order although there was a minor slip because the wrong form had been used to apply for a DSA. In particular the Special Forces were doing well and I had little to comment on except to say that the paperwork was extremely good.

I commended the MOD RIPA forms which set out in simple terms the areas which must be considered. I requested a copy of the template in order to share best practice; in particular their practice at the point of renewal of assessing the benefits already obtained and re-assessing privacy and intrusion.

Consolidated guidance

Compliance is taken seriously and the MOD have a good form which is filled in whenever consideration is given to circumstances involving a detainee and in particular whether there is a risk of mistreatment, and the MOD do comply with the guidance.

Home Office

	Round 1	Round 2
Selection	2 May 2014	11/12/14
Inspection days	13 May 2014	16/12/14

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	The paperwork selected for reading made the case for proportionality. Many of the submissions contained assurances that collateral intrusion of non intelligence value would be deleted. However a number did not. Whilst these assurances would have applied, I said that it was vital to make it explicit and the Home Office should see that it was included in submissions.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I selected for reading. The proposed new wording for renewing warrants does not set out how the intelligence to be gained outweighs the invasion of privacy. Although this does not make the warrant unlawful I would prefer that this wording is reflected.

The Home Office warrantry unit provided a useful paper setting out the significant progress and developments since the last inspection and they are well on the way towards achieving the recommendations I made last year. They are generally doing

well with a few recommendations which I will continue to monitor. I saw evidence that the warrantry unit questioned the submissions made by MI5. I saw evidence that the warrantry unit questioned as and when appropriate the submissions made by MI5.

The inspections focused on the use of thematic warrants where I sought more information about their use and restrictions.

The Home Secretary takes her responsibility to consider the necessity and proportionality of what she will be authorising very seriously.

NIO

	Round 1	Round 2
Selection	24 March 2014	21 September 2014
Inspection days	14 – 15 April	6 – 7 November 2014
Senior Official follow up	30 June 2014	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I scrutinised made out a case of necessity. In one case I questioned the necessity of continuing surveillance and subsequently spoke to MI5 about this. Both NIO and MI5 were able to reassure me that the correct authority was in place and the operation ceased as soon as it was no longer required. However, they accepted they were slow to cancel the warrant.
Proportionality **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed. The language of submissions should reflect any limitations applied to the use of the warrant. When authorising a warrant the Northern Ireland Secretary may put limitations on that warrant for example by setting a time for her to review it. I regard such limitations as good practice.

Detail	
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork selected for reading although some submissions could contain more precise wording in order to set out how privacy will be protected. Submissions now set out: • What interference there is likely to be with the target of the operation's privacy and any other individual's privacy • How this will be limited • Why the expected intelligence cannot be gained by other less intrusive means The wording of the warrants reflects this. Renewal submissions at present do not always set out what interference with privacy there has been including collateral.

The paperwork provided by NIO was in good order. I made a number of **recommendations** mostly around the area of thematic property warrants which I will monitor. Generally NIO take a great deal of care looking at the submissions from MI5 and asking questions to clarify what is required by the Service before submitting to the Secretary of State. I have asked NIO to inform me of any cases where either NIO or the Secretary of State has had doubts. I am not looking to second guess the decisions but would like to see the consideration given to each case and discuss this.

The Secretary of State for Northern Ireland shows a keen interest in the case for necessity and proportionality. She can and does refuse warrants.

Foreign Office SIS

	Round 1	Round 2
Selection	20 March 2014	30th October 2014
Inspection days	12 May 2014	18 December 2014

Detail SIS	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I reviewed on the pre-read make out a case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed during the pre-read.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	No questions of privacy arose during the inspection but I asked that privacy is set out in a separate heading and not incorporated into a general heading in the submission.

Foreign Office GCHQ

GCHQ	Round 1	Round 2
Selection	6 May 2014	4 December 2014
Inspection days	21 May 2014	15 December 2014

Detail GCHQ	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I reviewed on the pre-read make out a case for necessity. I have been looking closely at the case for necessity in relation to internal approvals and accept that the agencies do not self task. Their intelligence priorities are set out for them by government.
Proportionality **Was the case for proportionality made in each case inspected?**	The proportionality argument was clearly set out in the operations I selected for review.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I selected for reading. Internal approvals supplied for FCO or Ministerial consideration had set out that the level of intrusion is justified by the expected intelligence gain.

FCO warrantry unit carefully consider submissions and seek clarification from SIS or GCHQ when necessary. Detailed consideration appears from the documents I inspect and from my meetings with officials. Necessity and proportionality is carefully addressed. I saw good examples in the GCHQ and SIS papers of good and proper administration.

The Foreign Secretary is supported by notes on the documents and considers points very carefully.

I will continue to review the use of thematic property warrants.

8. CONCLUSIONS

As appears from the body of my report human errors have occurred as they will in any large organisation. I have also made a number of recommendations. But my overall conclusion is that the agencies and the MOD take compliance extremely seriously and seek to obtain their authorisations on a correct legal basis, establishing necessity to do what they seek to do, and properly considering proportionality and the justification for any intrusion into privacy. Equally where a warrant or authorisation has to be obtained from a Secretary of State, the warrantry units consider with care whether the case for necessity and the justification for any intrusion into privacy has been made out and the ministers themselves only sign the warrants or authorisation if they are satisfied of the necessity and proportionality of the activity they are authorising.

In light of the fact that new legislation in this area is likely to be considered I would draw attention to my recommendations in relation to the ability to combine warrants and to my concern for clarification as to the duration of warrants.

As regards Bulk Personal Data I am satisfied that the agencies properly consider and keep under review whether it is necessary and proportionate to hold or continue to hold Bulk Personal Data. I am also satisfied that access to that data is only permissible if a case of necessity justifies access and that any intrusion into privacy is kept so far as it can be to intrusion into the privacy of subjects of intelligence interest. I am also satisfied that the agencies have monitoring systems which are as effective as possible in preventing any individual having access to Bulk Personal Data other than that which they can properly justify for a business purpose.

As regards the Consolidated Guidance I am satisfied that the agencies and the MOD and those employed by them take compliance with the Consolidated Guidance extremely seriously and that the Guidance is properly followed.

APPENDIXES

Useful Background Information

By way of background to my oversight role, I believe it is useful to be aware of the directions from the Prime Minister placing my oversight on a statutory footing as well as the functions imposed upon each of the intelligence services and certain constraints to which they are all subject.

In this appendix I have set out

Appendix 1 The statutory functions of the Intelligence Services

Appendix 2 A summary of the Regulation of Investigatory Powers Act 2000 (RIPA)

Appendix 3 A summary of warrants and authorisations under RIPA

- Directed Surveillance
- Covert Human Intelligence Source
- Intrusive Surveillance

Appendix 4 A summary of warrants and authorisations under the Intelligence services Act 1994 (ISA)

- Section 5
- Section 7

Appendix 5 Article 8 of the European Convention on Human Rights

Appendix 6 Definition of Necessity and Proportionality

Appendix 7 Bulk Personal Data Direction

Appendix 8 Consolidated Guidance Direction

Appendix 1

The Statutory Functions of the Intelligence Services

Security Service (MI5)

The functions of MI5 are:

The protection of national security, in particular against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means;
Safeguarding the economic well-being of the UK against threats posed by the actions or intentions of persons outside the British Islands; and
To act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime.

Secret Intelligence Service (SIS)

The functions of SIS are to obtain and provide information and to perform other tasks relating to the actions or intentions of persons outside the British Islands either:

In the interests of national security, with particular reference to the UK government's defence and foreign policies;
In the interests of the economic well-being of the UK; or
In support of the prevention or detection of serious crime.

Government Communications Headquarters (GCHQ)

GCHQ's functions are:

To monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material, but only in the interests of national security, with particular reference to the United Kingdom government's defence and foreign policies, or in the interests of the UK's economic well-being in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime; and
To provide advice and assistance about languages (including technical terminology) and cryptography (and other such matters) to the armed services, the government and other organisations as required.

Appendix 2

The Regulation of Investigatory Powers Act 2000 (RIPA)

The commencement of the Regulation of Investigatory Powers Act 2000 (RIPA) introduced a number of changes to existing legislation. The most significant of these was the incorporation into surveillance powers of the fundamental protections afforded to individuals by the Human Rights Act 1998. RIPA was also designed to remain relevant in the face of future technological change through technologically neutral provisions. The full text of RIPA is available at www.legislation.gov.uk.

Part I:	is concerned with the interception of communications (the content), and the acquisition and disclosure of communications data (the who, when and where). Oversight of Part I activities is provided by the Interception of Communications Commissioner who produces his own report on Part I activities.
Part II:	provides a statutory basis for the authorisation and use of covert surveillance (both directed and intrusive) and covert human intelligence sources (undercover officers, informants etc.) by the intelligence agencies and certain other public authorities. Part II regulates the use of these intelligence-gathering techniques and safeguards the public from unnecessary and disproportionate invasions of their privacy.
Part III:	contains powers designed to maintain the effectiveness of existing law enforcement capabilities in the face of the increasing use of data encryption by criminals and hostile intelligence agencies. It contains provisions to require the disclosure of protected or encrypted data, including encryption keys.
Part IV:	provides for the independent judicial oversight of the exercise of the various investigatory powers. This includes provisions for the appointment of Commissioners, and the establishment of the Investigatory Powers Tribunal as a means of redress for those who complain about the use of investigatory powers against them. This section was amended by the Justice and Security Act 2013 to extend the powers of the Intelligence Services Commissioner so that the Prime Minister may direct me to keep under review the carrying out of any aspect of the functions of the Intelligence Services. Part IV also provides for the issue and revision of the codes of practice relating to the exercise and performance of the various powers set out in RIPA and ISA.
Part V:	deals with miscellaneous and supplementary matters. Perhaps the most relevant to my functions is section 74, which amended section 5 of the Intelligence Services Act 1994. This relates to the circumstances in which the Secretary of State may issue property warrants, in particular by introducing a criterion of proportionality.

Appendix 3

Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA)

Part II of RIPA provides a statutory basis for the authorisation of covert surveillance and covert human intelligence sources, and their use by the intelligence agencies and other designated public authorities. Part II regulates the use of these techniques and safeguards the public from unnecessary and disproportionate invasions of their privacy.

Directed Surveillance Authorisation (DSA)

What is directed surveillance?

Surveillance is defined as being directed if all of the following criteria are met:

It is covert, but not intrusive surveillance;
It is conducted for the purposes of a specific investigation or operation;
It is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
It is conducted otherwise than by way of an immediate response to events or in circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

How is directed surveillance authorised?

Under section 28 of RIPA designated persons within each of the intelligence services and the armed services may authorise surveillance. The authoriser must believe:

That the DSA is necessary for a specific human rights purpose (for the intelligence agencies this is in the interests of national security, for the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK; for the armed services it is, in addition, for the purpose of protecting public health or in the interests of public safety);
That surveillance is undertaken for the purposes of a specific investigation or operation; and
That it is proportionate to what it seeks to achieve and cannot be achieved by other (less intrusive) means.

Duration	Urgent	Renewal
Ceases to have effect [unless renewed or cancelled] at the end of a period of three or six months beginning with the time at which it took effect.	Unless renewed ceases to have effect after 72 hours beginning with the time when the authorisation was granted	May be renewed for a further period of six months (three months for the MOD) beginning with the date on which it would have ceased to have effect but for the renewal. Application to be made shortly before the authorisation period is drawing to an end.

How is directed surveillance used in practice?

An example of directed surveillance could include surveillance of a terrorist suspect's movements in public, in order to establish information about their pattern of life.

Covert Human Intelligence Source (CHIS)

What is CHIS?

A CHIS is essentially a person who is a member of, or acting on behalf of, one of the intelligence services and who is authorised to obtain information from people who do not know that this information will reach the intelligence or armed services. A CHIS may be a member of the public or an undercover officer.

A person is a CHIS if:

a) He establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
b) He covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

How is CHIS authorised?

Under section 29 of RIPA designated persons within the relevant intelligence service or the armed services may authorise the use or conduct of a CHIS provided that the authoriser believes:

That it is necessary for a specific human rights purpose (for the intelligence agencies this is in the interests of national security, for the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK; for the armed services it is, in addition, for the purpose of protecting public health or in the interests of public safety);
That the conduct or use of the source is proportionate to what it seeks to achieve; and
That the information cannot be obtained by other (less intrusive) means.

The legislation requires a clear definition of the specific task given to a CHIS, and the limits of that tasking. It also requires close management of a CHIS, including having regard to his or her security and welfare. All of this must be recorded for accountability purposes and managers are required to ensure that their staff comply with the legislation.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of 12 months beginning with the day on which it took effect [except juveniles].	Unless renewed ceases to have effect after 72 hours beginning with the time when the authorisation was granted	Renewal for a further 12 months. Renewal takes effect at the time at which the authorisation would have ceased to have effect but for this renewal. Application to be made shortly before the authorisation period is drawing to an end.

How is CHIS used in practice?

This could include the authorisation of the conduct of an informant tasked with developing a relationship with a suspected terrorist, in order to provide information to an intelligence agency.

Intrusive Surveillance

What is intrusive surveillance?

Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and involving the presence of an individual on the premises or in the vehicle, or the deployment of a surveillance device. The definition of surveillance as intrusive relates to the location of the surveillance, as it is likely to reveal private information.

How is intrusive surveillance authorised?

Under section 32 of RIPA, the Secretary of State may authorise a warrant to undertake intrusive surveillance which is necessary for the proper discharge of one of the functions of the intelligence services or the armed services.

Before the Secretary of State can authorise such action he must believe;

That it is necessary in the interests of national security, the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK;
That the authorised surveillance is necessary and proportionate to what it seeks to achieve; and
That the information cannot be obtained by other (less intrusive) means.

As a result of the naturally heightened expectation of privacy in the locations in which intrusive surveillance takes place, it is not necessary to separately consider whether the surveillance is likely to lead to private information being obtained.

How is intrusive surveillance used in practice?

Typically this would involve planting a surveillance device in a target's house or car, normally combined with a property warrant under section 5 of ISA.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued. They expire at 23.59 on the last day so an authorisation given at 09:00 on 12 Feb will cease to have effect at 23:59 on 11 Aug,	Oral authorisation may be given by the Secretary of State will cease to have effect [unless renewed] at the end of the second working day following the day of issue.	Where renewed it ceases to have effect at the end of six months beginning with the day it would have ceased to have effect if not renewed again Application to be made before the warrant expires.

Appendix 4

Warrants and Authorisations under the Intelligence Services Act 1994 (ISA)

The Intelligence Services Act 1994 was introduced to make provisions for the issue of warrants and authorisations to enable SIS, the Security Service and GCHQ to carry out certain actions in connection with their functions. The Act is available in full at www.legislation.gov.uk.

Section 5 Warrants

What is a section 5 warrant?

Under section 5 of ISA the Secretary of State may issue warrants authorising the Security Service, SIS or GCHQ to enter on to, or interfere with, property, or to interfere with wireless telegraphy. Often referred to as property warrants, their use must be necessary for the proper discharge of one of the functions of the applying agency.

How are section 5 warrants authorised?

Before the Secretary of State gives any such authority, he must first be satisfied of a number of matters:

That the acts being authorised are necessary for the purpose of assisting the particular intelligence agency to carry out any of its statutory functions;
That the activity is necessary and proportionate to what it seeks to achieve and it could not reasonably be achieved by other (less intrusive) means; and
That satisfactory arrangements are in place to ensure that the agency shall not obtain or disclose information except insofar as necessary for the proper discharge of one of its functions.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued.	Oral authorisation may be given by the Secretary of State which will cease to have effect [unless renewed] at the end of the period ending with the fifth working day following the day on which it was issued.	The warrant may be renewed in writing for a further period of six months beginning with the day on which it would otherwise cease to have effect.

How are section 5 warrants used in practice?

A section 5 warrant might be used to authorise entry to a property and concealment of a listening device within it. In such cases, a section 5 warrant will be used in conjunction with an intrusive surveillance warrant.

Section 7 Authorisations

What is a section 7 authorisation?

Under section 7 of ISA the Secretary of State (in practice normally the Foreign Secretary) may authorise SIS or GCHQ to undertake acts outside the United Kingdom which are necessary for the proper discharge of one of its functions. Authorisations may be given for acts of a specified description.

How are section 7 authorisations authorised?

Before the Secretary of State gives any such authority, he must first be satisfied:

That the acts being authorised (or acts in the course of an authorised operation) will be necessary for the proper discharge of an SIS or GCHQ function;
That satisfactory arrangements are in force to secure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of an SIS or GCHQ function;
That satisfactory arrangements are in force to secure that the nature and likely consequences of any acts which may be done in reliance on the authorisation will be reasonable having regard to the purposes for which they are carried out; and
That satisfactory arrangements are in force to secure that SIS or GCHQ shall not obtain or disclose information except insofar as is necessary for the proper discharge of one of its functions.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued.	Oral authorisation may be given by the Secretary of State which will cease to have effect [unless renewed] at the end of the period ending with the fifth working day following the day on which it was issued.	ISA states: "If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of six months beginning with that day."

How are section 7 authorisations used in practice?

These authorisations may be given for acts of a specified description, in which case they are referred to as class authorisations. In practice this could mean obtaining intelligence by way of agent operations overseas.

Appendix 5

The European Convention on Human Rights (ECHR)

The ECHR was introduced into UK law on 1 October 2000 when the Human Rights Act came into force.

Article 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Appendix 6

Necessity and Proportionality

When deploying intelligence gathering techniques, the intelligence services always aim to take courses of action that are effective, minimally intrusive into privacy, and proportional to the identified threat. Before intrusive methods of intelligence gathering are utilised, the intelligence services much justify to the relevant Secretary of State that what they propose to do is both:

Necessary for the protection of national security, or for the purpose of safeguarding the economic well-being of the UK against threats from overseas, or in order to prevent or detect serious crime, or, additionally in the case of the armed services, protecting public health or in the interests of public safety; and
Proportionate to what the activity seeks to achieve, i.e. that the intelligence gain will be sufficiently great to justify the intrusion into the privacy of the target, and any unavoidable collateral intrusion into the privacy of individuals other than the target.

The relevant Secretary of State also needs to be satisfied that the information that is expected to be obtained could not reasonably be obtained by other less intrusive means.

These are important tests, and the intelligence services take care to apply for warrants only where they believe the threshold is clearly met.

Appendix 7

Bulk Personal Datasets Direction

Regulation of Investigatory Powers Act 2000

Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015

The Prime Minister, in exercise of the power conferred by section 59A of the Regulation of Investigatory Powers Act 2000 ("the Act"), directs the Intelligence Services Commissioner appointed under section 59 of the Act as follows:

Citation and Commencement

1. This Direction may be cited as the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015.

2. This Direction comes into force on 13 March 2015.

Additional Review Functions

3. The Intelligence Services Commissioner must continue to keep under review the acquisition, use, retention and disclosure by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the Security and Intelligence Agencies") of bulk personal datasets, as well as the adequacy of safeguards against misuse.

4. The Intelligence Services Commissioner must seek to assure himself that the acquisition, use, retention and disclosure of bulk personal datasets does not occur except in accordance with section 2(2)(a) of the Security Service Act 1989, sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994. As part of this, the Intelligence Services Commissioner must seek to assure himself of the adequacy of the Security and Intelligence Agencies' handling arrangements and their compliance therewith.

5. For the purposes of this Direction, a bulk personal dataset means any collection of information which:

   a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;

   b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;

   c. Is held, or acquired for the purpose of holding, on one or more analytical systems within the Security and Intelligence Agencies.

Signed: David Cam

Date: 11.3.15

Appendix 8

Consolidated Guidance Direction

Regulation of Investigatory Powers Act 2000

Intelligence Services Commissioner (Additional Review Functions) (Consolidated Guidance) Direction 2014

The Prime Minister, in exercise of the power conferred by section 59A of the Regulation of Investigatory Powers Act 2000 ("the Act"), directs the Intelligence Services Commissioner appointed under section 59 of the Act as follows:

Citation and Commencement

1. This Direction may be cited as the Intelligence Services Commissioner (Additional Review Functions) (Consolidated Guidance) Direction 2014.

2. This Direction comes into force on 28 November 2014.

Additional review functions

3. The Intelligence Services Commissioner must keep under review the compliance of persons falling within paragraph 4 with the guidance referred to in paragraph 5 in relation to the circumstances set out in paragraph 6

4. The persons are:

    a. officers of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters;
    b. members of the Armed Forces of the United Kingdom and employees of the Ministry of Defence, so far as any of them engage in intelligence activities within the meaning of section 59A of the Act.

5. The guidance is the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees which was published on 6 July 2010, as amended from time to time.

6. The circumstances are those in which one or more persons falling within paragraph 4:

    a. interview a detainee who is in the custody of a third party;
    b. request a third party to seek information from a detainee in the custody of that party;
    c. pass information to a security or intelligence service of a third party in relation to a detainee held by that party;
    d. receive unsolicited information from a third party which relates to a detainee;
    e. solicit the detention of an individual by a third party.

Signed: David Cameron

Date: 27th November, 2014

ISBN 978-1-4741-2111-8





Report of the Intelligence Services Commissioner for 2015

The Rt Hon Sir Mark Waller

Presented to Parliament pursuant to
section 60(4) of the Regulation of
Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed 8 September 2016

Laid before the Scottish Parliament by
the Scottish Ministers 8 September 2016

HC 459
SG/2016/96



Report of the Intelligence Services Commissioner for 2015

The Rt Hon Sir Mark Waller

Presented to Parliament pursuant to
section 60(4) of the Regulation of
Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed 8 September 2016

Laid before the Scottish Parliament by
the Scottish Ministers 8 September 2016

HC 459
SG/2016/96

© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications and www.intelligencecommissioner.com

Any enquiries regarding this publication should be sent to info@iscom.gsi.gov.uk

Print ISBN 9781474135535
Web ISBN 9781474135542

ID 30061601 09/16

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

CONTENTS

1.	**INTRODUCTION**	**2**
	My Oversight	2
	Functions	4
	Changes from previous annual reports and my website	5
	Inspection Reports and Confidential Annex	6
	Developments since my last annual report	6
2.	**RISKS**	**8**
3.	**THEMES**	**9**
	i. Covert Human Intelligence Source (CHIS)	9
	ii. Directed Surveillance	12
	iii. Intrusive Surveillance and Property Warrants	16
	iv. Section 7 Authorisations	19
	v. Equipment Interference	23
	vi. Bulk Personal Datasets (BPDs)	27
	vii. Consolidated Guidance	40
4.	**PRODUCT OBTAINED AND HANDLING ARRANGEMENTS**	**46**
5.	**ERRORS**	**47**
6.	**RIPA/ISA STATISTICS**	**52**
7.	**BRIEF SUMMARY OF ASSESSMENTS**	**53**
8.	**CONCLUSIONS AND RECOMMENDATIONS**	**65**
APPENDIX		**67**
	Expenditure	67

The Rt Hon Sir Mark Waller
Intelligence Services Commissioner
2 Marsham Street
London
SW1P 4DF

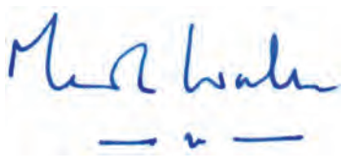
The Rt Hon Theresa May MP
The Prime Minister
10 Downing Street
London
SW1A 2AA

21 July 2016

I enclose my fifth Annual Report covering the discharge of my functions as Intelligence Services Commissioner between 1 January 2015 and 31 December 2015.

It is for you to decide, after consultation with me, how much of the report should be excluded from publication, on the grounds that any such publication would be contrary to the public interest, or prejudicial to national security, to the prevention or detection of serious crime, to the economic well being of the United Kingdom, or to the discharge of the functions of those public authorities subject to my review.

I have continued to write my report in two parts, the Confidential Annex containing further details including techniques and operational matters which in my view should not be published. I hope you find this convenient.



The Rt Hon Sir Mark Waller

1. INTRODUCTION



This is my 5th annual report since first taking up office as the Intelligence Services Commissioner on 1 January 2011. Even since my last, covering 2014, there have been a number of significant developments affecting the areas I oversee which I cover in more detail later in this introduction. I will also address my oversight in general, changes I have made to this report compared with previous reports and recent important developments.

My Oversight

The areas I oversee cover some of the most intrusive powers available to the intelligence agencies, including intrusive surveillance, property and equipment interference and obtaining and accessing bulk personal datasets. I oversee the surveillance activities of the Ministry of Defence. I also oversee compliance by the agencies and the Ministry of Defence of the 'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees', known as the Consolidated Guidance, a complex area involving difficult decisions relating to intelligence sharing.

In essence my oversight role requires me to check:

- that warrants and authorisations which enable the intelligence services to carry out their functions are being granted by the Secretaries of State and/or being internally authorised only after a proper case of necessity has been demonstrated and a proper case that what is to be authorised is proportionate has been made;
- that bulk personal datasets are being obtained, retained and used only where it is shown to be both necessary and proportionate to do so;
- that the Consolidated Guidance is being complied with so that proper consideration is given as to whether a detainee of a third party state is being and/or will be properly treated before intelligence is shared with that country.

To do this I scrutinise how the agencies and MOD carry out their activities. I do so in a number of different ways:

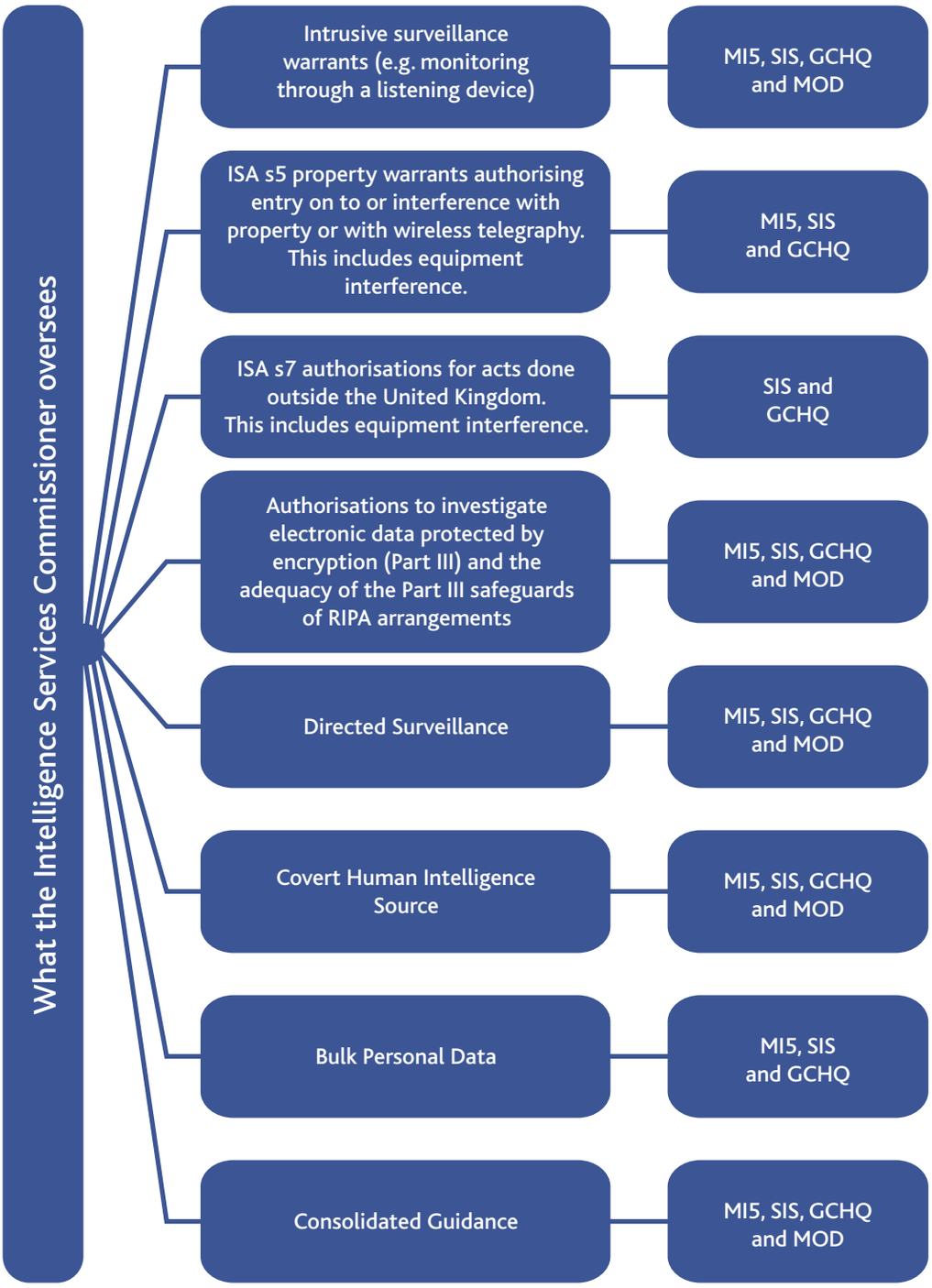
- First, there is the 'after the fact audit' carried out twice a year of all the above about which I have written in detail in my annual reports e.g. those for 2013 and 2014;
- Second, I look at the safeguards in place within the agencies to prevent inappropriate access to and/or use of powers, information or systems; the policies and procedures in place to deal with acquisition, use, retention and deletion of information obtained by use of the powers available to them and to prevent misuse; and the systems and processes officers must go through to access material;
- Third, observing the culture and ethos across the organisations including by, for example, attending training courses for new recruits and established staff.

I am also asked to carry out further activities by the Prime Minister.

A cornerstone of my regime is personal responsibility and I do my job rigorously, independently of government, Parliament and the agencies, without political favour or personal bias. All Commissioners are required to be holders or past holders of high judicial office, meaning that they are independent and will form their own impartial judgement, that they will have had long experience of drawing out the facts and that they should be seen to carry authority because of their position.

Functions

My statutory functions are set out in full on my website but in summary my primary role as Intelligence Services Commissioner is to ensure the UK intelligence agencies and parts of the Ministry of Defence act lawfully and appropriately use the intrusive powers available to them including:



Other statutory functions include:

- assisting the Investigatory Powers Tribunal when required;
- reporting to the PM (Annual Report);
- overseeing any other aspects of the functions of the intelligence services, HM Forces or the MOD when directed by the Prime Minister;
- advising the Home Office on the propriety of extending the TPIMS regime.

Terrorism Prevention Investigation Measures (TPIMS) Act 2011

One of my functions is to advise the Home Office on the propriety of extending the TPIMS regime as part of the consolation process under section 21(3) of the TPIMS Act. TPIMS expire 5 years after the date the Act came into force unless an order is made by the Secretary of State to extend or repeal. TPIMS will expire on 15/12/16 which will be the first time such a consultation process will be required.

Section 94 of the Telecommunications Act 1984

In 2010 GCHQ asked my predecessor to oversee the activity of GCHQ in relation to data acquired by means of directions given by the Secretary of State under section 94 of the Telecommunications Act. This oversight was on an extra-statutory basis and was not avowed. When I took up appointment in 2011 I continued to oversee GCHQ's use of section 94 directions. My oversight involved (a) examining the justification for the directions and (b) examining the acquisition and use of the data acquired on the same basis as I oversaw bulk personal data. However, in January 2015 the Interception of Communications Commissioner agreed to formally oversee these directions.

Changes from previous annual reports and my website

In January of 2016 my team revamped the content of my website, adding significantly more information than it previously held. I hope it is a useful resource for those with an interest in the areas I oversee.

In previous annual reports I included detail on my statutory functions, the methods I use to audit warrants and authorisations, my assessment of inspection visits and summaries of relevant legislation among other things. Further details about my statutory functions, the method of my warrant and authorisation review and information about relevant legislation are now available on my website.

Last year I introduced 'thematic' sections to my reports on the various powers that I oversee with the intention of making information about use of those powers by the agencies and MOD clearer and more readily accessible to the layperson. This year I have expanded the thematic sections, provided more detailed statistics and focused on an important element of oversight which risks being lost in discussion of judicial authorisation and auditing after the fact, that is the risk of rogue activity and how the agencies themselves, and I as part of my oversight, work to mitigate that risk.

Inspection Reports and Confidential Annex

In this report I have continued to be as transparent about my oversight role as possible subject to the national security restrictions which are in place for good reason. As intelligence and security services, secrecy is critical to the agencies' ability to function effectively. If I were to disclose certain information in my report, as well as aiding hostile intelligence services doing so could reduce or risk reducing the value of particular methods, techniques or equipment in current or future operations and potentially cause damage to operational capabilities or personnel which would be harmful to the national security of the UK.

After each inspection the head of my secretariat produces an inspection report which is specific to that organisation and sets out the emerging findings from that inspection and any recommendations I have made to demonstrate or to improve compliance. During my inspection I scrutinise ongoing operations so these reports are highly classified. I reflect the general findings from these reports and the various themes that emerge over the year in my annual report and I provide the Prime Minister with a confidential annex containing more classified material including details and techniques.

Developments since my last annual report

Since my last annual report was written in 2015, there have been a number of significant developments affecting the areas I oversee. These developments include two fundamental reviews into the authorities' use of investigatory powers and the Investigatory Powers Bill (IP Bill) which was introduced to Parliament on 1st March 2016. Reports of the reviews, 'A Question of Trust' by David Anderson Q.C. and 'A Democratic Licence to Operate' by the Royal United Services Institute (RUSI), alongside the Intelligence and Security Committee's Privacy and Security Report published in March 2015 were a starting point for many of the provisions in the government's Investigatory Powers Bill. The Government also avowed the existence of powers I oversee which were not previously publically avowed.

A key feature of the Bill, if it is passed, will be to introduce what is termed a double lock in the authorisation process for some but not all authorisations granted by Ministers – the double lock being the necessity to obtain approval by judicial commissioners.

Much of what I at present oversee i.e. authorisations granted to the intelligence agencies to interfere with property other than interference with computers (equipment interference) and authorisations to those agencies to conduct intrusive surveillance is not proposed to be subject to the double lock and is to be authorised and overseen as now.

Some may think that inconsistent in that a listening device in a car or a home might be thought to be as intrusive as an interception of a telephone call. But the important point is that there is a recognition, with which I agree, that ministers can and do properly assess in the national security context necessity and proportionality and that an auditing system by a senior judge or a retired senior judge after the event checking that warrants and authorisations have been and are being granted on a proper legal basis is an effective oversight system.

The reason why it is effective in my judgment is that there is a culture both in the agencies, the MOD and at the offices of the Minister which wants to ensure that they act within the constraints that Parliament has imposed and to get things right – the fact that a senior judge is going to come in and probe and ask questions of all persons involved in the process discourages the pushing of boundaries never mind worse. If the agencies themselves were as institutions determined to act unlawfully that would take a massive conspiracy from top to bottom and they would not be seeking warrants or authorisations to so act. A thing of primary importance is to check that there are systems in place to prevent a rogue using the very powerful tools available without authorisations. But I stress it is important to have a system of oversight which seeks to ensure that the boundaries that the law imposes are strictly complied with and my experience is that the after the event audit does meet that requirement because the authorisers do not want criticism or worse to be told the authorisation was in fact unlawful.

Finally, in November 2014 the Prime Minister requested me to investigate concerns raised by the Intelligence and Security Committee in their report on the murder of Fusilier Lee Rigby. In their report the ISC were critical of SIS for their handling of allegations of Michael Adebolajo's mistreatment in Kenya made during his interview by police under the Terrorism Act 2000 on his return to the UK. My report on that investigation is being published supplementary to my annual report.

2. RISKS

As already indicated what must be guarded against is any individual, or group of individuals, who seek to abuse the systems. They would not seek authorisation. They would try to circumvent the system for their own ends.

So a vitally important part of my oversight is about mitigating that risk. To do so I look at: the safeguards in place within the agencies to prevent inappropriate access to or use of information obtained by the agencies to allow them to carry out their statutory functions; the policies and procedures the agencies have put in place to deal with the acquisition, use, retention and deletion of information obtained by use of the powers available to them and to prevent any misuse; the systems and processes officers must go through to access such material; that individuals are not free to act on their own or without supervision; and the culture and ethos in an organisation.

Of course discussing what these processes and policies are in any detail here would be counter productive, allowing anyone who would attempt to abuse the system the knowledge by which to do so. But I can say that the systems and policies in place in all the agencies are designed to ensure that no one person can act on their own or access information on any of the systems holding sensitive information individually, without someone else knowing about it and without having to go to a more senior officer.

This would deal with a rogue individual. But not with a top down conspiracy, the scale of which would have to be massive to be successful. A further mitigation is an effective appointments process, thorough vetting at the outset and appointing individuals of integrity at the top. The culture and ethos across the agencies must be closely monitored. In addition to my interactions with staff during my inspections, my under the bonnet visits and visits to stations overseas, I regularly attend training courses for new recruits and established staff all of which give me a good insight into the culture and ethos of the organisation and its staff.

3. THEMES

i. Covert Human Intelligence Source (CHIS)

Part II of RIPA and the associated code of practice provide the legal framework for authorising the use and conduct of a CHIS. A CHIS may be a member of the public reporting to one of the agencies, or to the MOD, or an intelligence officer or a member of military personnel operating under an alias. They are authorised to obtain information from people who do not know that this information will reach the intelligence agencies or armed services. CHIS are often referred to as agents.

The agencies maintain an unshakeable commitment of confidentiality regarding the identity of CHIS which remains indefinitely. Revealing the role a CHIS has played could result in reprisals by a state or an organisation which could threaten the life of the CHIS or their family. In conducting my oversight and in scrutinising the authorisations this is an important consideration.

My overall assessment of CHIS use and conduct

From the cases I have examined in relation to the use and conduct of CHIS I can see the documentation provided has demonstrated that proper consideration is given to necessity and proportionality and in particular the possible invasion of privacy and the justification for this. Officers have also made themselves available to brief me about their specific agent running or undercover operation and answer my questions. **There are however some points to be made.**

CHIS Reviews

MI5's business model is designed to ensure that the case management team, and in particular the case officer and controller, are constantly reviewing the cases for which they have responsibility and I have no reason to believe this is not taking place. However, I noted that the formal, documented review of the CHIS authorisations I scrutinised was inconsistent including:

- no documented reviews beyond those conducted at renewal for three cases: one renewal stated that no formal review was necessary, although there was a recorded requirement for regular updates on the case to be provided to the authorising officer;
- five new authorisations did not mention reviews;
- one CHIS had been reviewed regularly;
- one had been inherited from the police with no mention of reviews;
- one mentioned a review date but there was no paperwork; and
- two had been reviewed once but there was no record of subsequent review.

This has been an ongoing problem, as I mentioned in my report for 2014. MI5 explained that reviews should have been carried out by the authorising officer in accordance with the code of practice paragraph 5.17. I reminded MI5 that under the code they should review each CHIS regularly. I **recommended** they record these reviews to demonstrate that they have given proper consideration to reviews and completed them, and that the activity still meets necessity and proportionality requirements for oversight purposes. Since my recommendation MI5 have been more consistently conducting formal written reviews, and will extract the information from the decision log and make it available to me at future inspections

MI5 were unable to explain the automatically generated random review dates that appeared in some of the paperwork but believe there was a technical problem and agreed to look into it.

I also saw examples of this in SIS where I **recommended** that the authorising officer set realistic review dates at the point of authorisation in line with the code of practice para 5.17.

Confidential Information

One authorisation was referred to me because it had the potential to obtain confidential information, specifically spiritual counselling. This in fact goes further than the requirement of the code of practice paragraph 4.18 which only requires cases to be referred to me when information has been obtained.

In my view the authority gave good consideration to religious sensitive information and the paperwork showed that confidential material was not the desired intelligence outcome, in fact the CHIS tasking was clear that the information to be gathered should not include spiritual counselling. I agreed that the authorisation was appropriate and had given good consideration to the possibility of obtaining confidential information. In my view it must be possible in such circumstances where there is an immediate threat to life to investigate. Religious cover should not be used to protect criminal behaviour.

Duration of Authorisations

In my 2014 Report I noted that some CHIS applications had been made for three months and some for twelve months. The code of practice suggests that an application for the use and conduct of a CHIS must be made for a twelve month period even if it is known at the outset that activity will only take place for a matter of days. In my view it is arguable that it is neither necessary nor proportionate to issue for the full twelve month period when it is known at the outset that the operation will be for a shorter period but I recommended that the code of practice should be applied in all cases and the authorisation cancelled when it is no longer required. This has been monitored throughout my inspections in 2015 and I am confident that this recommendation has been implemented.

Agent Participation in the Commission of an Offence

There may be occasions where a CHIS participates in a criminal offence in order to gather the required intelligence, for example membership of a proscribed organisation or handling stolen goods. However in specific situations where the intelligence dividend justifies it, a good argument can be made that it is in the public interest and for the greater good to become involved. Although such activity cannot be made lawful I have **recommended** that the agency must justify the public interest test.

ii. Directed Surveillance

Directed Surveillance is surveillance which obtains private information in a covert but not intrusive manner. Although directed surveillance is not intrusive, proper consideration must still be given to the necessity and proportionality of the activity. Specific consideration must be given to ensuring that the necessity of obtaining the information outweighs privacy considerations. While Part II of RIPA does not impose a requirement for public authorities to obtain DSAs before conducting directed surveillance, RIPA authorisations are in fact used to authorise such surveillance.

My overall assessment

From the submissions I have examined the applications to undertake directed surveillance have made out a proper case. The documentation provided has demonstrated proper consideration of necessity and considered properly whether any intrusion into privacy is justified and the extent to which it is justified. Officers made themselves available to brief me about their operation and answer my questions. This helps me to confirm that the necessity case is justified and that the operation is limited to what has been authorised in the RIPA application. **There are however certain points to be made.**

Completing Forms

At SIS, once the authorisation has been finalised it is not possible to amend it. This is a good thing and where I did come across a typographical error (such as saying 2015 instead of 2016) I noted that the authorising officer would minute a correction on the day of authorisation so no error occurred.

In one case, a month after the operation, SIS noticed that, although a form had been properly authorised it had not been published; publishing locks the form down. As a consequence SIS explained to me that the original text had degraded and the proportionality box appeared empty. I asked for an explanation how SIS or I could be confident that proper consideration had been given since, with no text in the box, it appeared that proportionality had not been considered. In my view this is not satisfactory and should not happen. The team responsible for legalities and compliance explained that they had a discussion with the authorising officer who had seen a version of the form with this information completed. I requested this version of the form but unfortunately after conducting a search the authorising officer returned to say that it was no longer on their personal drive because it is automatically cleared every three months. Having heard an explanation from the compliance team and the authorising officer, I was satisfied that on a balance of probabilities, this was a failure to follow SIS internal guidance but no error had occurred. However, it should not happen and I **recommended** that these important documents should be "locked down" when they are authorised. In retrospect, it would have been better if SIS had recorded the explanation which they provided to me.

Actions Authorised

By far the majority of directed surveillance authorisations that I see are at MI5 so the majority of points relate to them.

During 2015 MI5 briefed me on their plans to better explain the standard range of actions on the DSA authorisation form. They planned to:

- merge similar actions;
- remove unnecessary or obsolete actions;
- add new actions which had not previously been specified;
- clarify any actions which may have been unclear.

Having reviewed the plans I was content that this should help improve officer's understanding and reduce errors.

Filler Text

I was concerned to see that there continues to be odd occasions where an automatic nonsensical filler text appears in DSA renewal and modification forms. I have spoken to MI5 about this repeatedly throughout the last few years. This filler text must not be used to populate any section of any form and nor should they say 'not applicable' which has appeared in another situation. If, for example, the modification or renewal does not require specific consideration in relation to one part of the form then this should be set out. If for example a DSA is modified and no extra consideration of necessity and proportionality is required I **recommended** that it would be acceptable to say "see previous form". If however, a DSA is modified and another intelligence target is added, within this specific operation, then proper consideration must be given to intrusion into privacy, collateral intrusion or why the intelligence cannot be gained by less intrusive means. Care should be taken to give specific consideration and not to use stock language. Staff have been reminded so I do not expect this to happen again.

Stock Forms

MI5's stock form for cancelling a DSA includes the wording "*Before making this authorisation, the authorising officer satisfied themselves that the actions in question were necessary for the protection of national security and were proportionate to what was sought to be achieved*." This language is obviously not appropriate; the DSA is being cancelled because it is no longer necessary and proportionate so I **recommended** that the form should be amended to correct this.

Modification to DSAs

Directed Surveillance may be broadly termed if for example it authorised surveillance against a particular terrorist operation. The legislation requires that it is

"for the purpose of a specific investigation or a specific operation". In such thematic style surveillance operations, the authorisations should:

- make it clear what the expected outcome is;
- identify the targets, preferably by name;
- keep track of any amendments during the course of the operation through a modification document.

In my report last year I said that although MI5 were diligent in modifying authorisations, it was sometimes difficult to keep track of the amendments. To improve my ability to inspect MI5 gave me and my office access to documents on a computer system which enables us to cross check modifications to ensure they are always accurate. This has been an asset to the scrutiny process.

At the MOD they were re-authorising a DSA rather than modifying the original. This had the potential to cause confusion, particularly if the original DSA was not cancelled. I **recommended** they create and implement a stock form for DSA modifications and advised that the form should set out:

- what had been modified;
- why the purpose of the original DSA is still met;
- why it remains necessary and proportionate and;
- consideration of intrusion into privacy.

I suggested that the MI5 template would be a good starting point. By my second inspection I was pleased to see that MOD had drafted a modification template based on the MI5 form.

Open Source Information

As I indicated last year, the law, including Article 8 of the ECHR, applies to online activity equally as to activity in the physical world and the agencies are obliged to comply with the law when it comes to collecting open source internet data just as much as collecting any other type of intelligence. At the time the agencies were working on clearer guidance which I asked to see. To date the agencies have agreed the broad principles, but do not have a joint policy as yet.

The broad principles recognise that:

> "... human behaviour is shifting rapidly so that far more activity and communication now occurs online than ever before and there is much more concern about privacy online, undermining the traditional concept of putting information on the internet as being akin to publishing in the print media."

It includes the legal basis for authorisation which says:

> "However the collection and retention in a permanent record by MI5 of open source internet data about a person is capable of amounting to an interference with that person's Article 8 rights, because it will arguably exceed a person's reasonable expectation of privacy and give rise to private life considerations, depending on the totality of the retained data.
>
> This is a similar principle to the observation of a person's public movements. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information."

I was pleased to see that my recommendation had been implemented in this way and look forward to a finalised cross agency agreement.

Duration

On a few occasions I have noted that a DSA had been authorised a few days before it was to come into force. I have commented on this above but in summary I have **recommended** that the authority begins on the day it is signed by the authorising officer.

The MOD reported to me at inspection that a DSA operation had deployed before the paperwork was concluded. I advised that this error should be formally reported either as a failure to obtain a DSA or failure to obtain an urgent authority for 72 hours.

Combination

In my previous Annual Report I explained that I had become concerned that there is room for error when directed surveillance is required in combination with a property warrant. As I said last year, when a DSA is required in combination with a property warrant the property warrant is signed by the Secretary of State but the DSA must be authorised separately by the relevant agency. Added to this, property warrants and DSAs have different duration periods which means that the warrants and authorisations have different renewal/cancellation deadlines. In view of this I **recommended** that if the legislation were to be amended there should be room for flexibility in issuing combined warrants and around the duration of warrants so that they can be combined and synchronised. As the IP Bill has not updated part II of RIPA or ISA this opportunity has been missed.

iii. Intrusive Surveillance and Property Warrants

Intrusive Surveillance

Intrusive surveillance is covert surveillance related to anything taking place on residential premises or in a private vehicle, and involving an individual being present on the premises or in the vehicle, or deployment of a surveillance device. The agencies must make a strong case to explain why the information to be obtained cannot be obtained by less intrusive means and that the necessity of obtaining the information outweighs the intrusion into privacy.

Surveillance is defined as intrusive or not depending on the location in which that surveillance takes place. So, since surveillance in residential premises or vehicles is likely to involve a greater intrusion into privacy, it is defined as intrusive. The agencies also consider other situations where a person would have a reasonable expectation of privacy. Because intrusive surveillance can take place inside family homes and cars it is the most intrusive power. I keep this in mind when I am reviewing applications and when they come up for renewal I expect to see evidence of the intelligence gained to help justify the continued intrusion into privacy.

Section 5 Property Warrants

Under Section 5 of ISA the Secretary of State may issue warrants authorising MI5, SIS or GCHQ to enter into, go onto, or interfere with property, or to interfere with wireless telegraphy. They are often referred to as property warrants. A property warrant may be used for remote interference with a computer which is covered in my chapter on Equipment Interference.

In this section I am concerned with property warrants used to authorise entry into or interference with a domestic residence for the purpose of concealing a listening device. In such cases a combined warrant is used.

Combined Warrants

The vast majority of intrusive surveillance warrants I see are combined with an ISA Section 5 property warrant. Under section 42(2) of RIPA a Secretary of State may issue a single warrant combining an intrusive surveillance warrant with a property warrant. However, proper and separate consideration must be given in the submission to both the property warrant and the intrusive surveillance. This could be planting an eavesdropping device in a car or residential home.

A combined property and intrusive surveillance warrant can be highly invasive and as such separate consideration must be given to limit any unnecessary intrusion into privacy and specifically collateral intrusion into the privacy of any family members or friends of the person. A strong case must be made to explain why the information cannot be obtained through less invasive means and that the necessity of obtaining the information outweighs the invasion of privacy.

My overall assessment

In the submissions I have examined proper cases for necessity have been made and proper consideration has been given to limiting unnecessary intrusion into privacy and minimising collateral intrusion. The invasion of privacy authorised has also been justified by the necessity. I am satisfied that the agencies, the warrantry units and ultimately the Secretaries of State recognise the degree of intrusion and great care goes into making and submitting these applications. The agencies must explain why the intelligence cannot be obtained by a less intrusive means.

My only concern during 2015 relates to the fact that submissions do not always set out as fully as they could the steps to be taken to mitigate collateral intrusion.

Collateral Intrusion

Many submissions for Intrusive Surveillance and Section 5 Property Warrants recognised that collateral intrusion was likely to occur but then failed to stipulate what would happen to the unwanted product or steps taken to limit the intrusion. These are standard techniques and recognised procedures are in place for such a situation which the agencies can and do explain to me. However, in order to demonstrate proper compliance I **recommended** that this information is set out clearly in the submission.

Retrieval of Equipment

The code of practice in relation to Property Interference Warrants recognises that it may be necessary to renew a warrant in order to retrieve a device which is no longer needed for intelligence purposes. In such cases it is in fact no longer necessary or proportionate to continue with the matters authorised by the accompanying Intrusive Surveillance Warrant but it has not yet been possible to remove the equipment, and some authorisation is still required.

I have agreed that while a device is awaiting extraction, it is possible to transfer the device onto a thematic warrant which properly reflects the basis for the continued presence of the device.

Thematic Property Warrants

I continue to scrutinise particularly what might be termed thematic property warrants issued under Section 5 of ISA. When a proper case can be made for authorising these broadly termed warrants I have **recommended** that the agencies devise a method of recording any reliance on the warrant in relation to individual operations. Overall I have made it clear that they are the exception rather than the rule and must never be used for operational convenience.

In my previous report I made a number of recommendations in relation to thematic property warrants and said:

> "This has led to one of the agencies withdrawing a thematic property warrant in order to better define the specified property. We remain in discussion to find a way to do so but I am anxious to ensure that they are not missing intelligence opportunities which might endanger national security."

During my inspections of 2015 I reviewed the revised warrant which better defined the property to be interfered with. I still felt there was room for improvement and my **recommendation** in that regard was also implemented.

My recommendations relating to thematic warrants have largely been accepted and implemented. The lists provided for my inspection have, for the most part, highlighted any which may be considered thematic but on occasion my office has had to remind agencies of this particular requirement. I have kept a close eye on the terms of the warrant to ensure that the Secretary of State is able to assess the necessity and proportionality.

GCHQ have introduced a "record of reliance" document to formally record each occasion on which a thematic warrant is used. This is not a requirement under legislation but I encourage others to implement a similar process. At GCHQ I **recommended** that they include a section in the form to direct the user to give specific consideration to confidential material. This recommendation has now been implemented.

It is the submission applying for the warrant which does and should set out all the limitations to the use of the warrant and identifies, for example, what action is being taken to minimise intrusion into privacy. I have **recommended**, that the warrant instrument should indicate expressly that any activity taking place was on the basis of the terms of the submission. GCHQ have already adopted this recommendation and I strongly encourage SIS and MI5 to do so as well.

Renewing Warrants

Although the legislation does not require it, when renewing a warrant I have in the past said that the warrant renewal instrument should state that the Secretary of State still considers the activity to be necessary and proportionate. It is important that it is clear that the Secretaries of State have applied their mind to necessity and proportionality when a warrant is renewed. For the most part my recommendation has been implemented but during 2015 I have on occasion noted that the short form renewal is still being used.

iv. Section 7 Authorisations

Under Section 7 of ISA the Secretary of State, in practice normally the Foreign Secretary, may authorise SIS or GCHQ to undertake acts outside the UK which are necessary for the proper discharge of one of their functions. When authorised by the Secretary of State it seeks to remove personal liability under UK law where the officer has been acting in good faith within the parameters of the authorisation. Authorisations under Section 7 can be for a specific act or for a broader class of activity, known as class authorisations.

Oversight of Section 7 can be particularly challenging because of the multitude of possible acts that could be authorised. Some Section 7s have a standard consideration of necessity and proportionality while in others there is no intrusion into privacy but they may require a lengthy legal consideration.

Authorisations may be for a particular operation or may relate to a broader class of operations. As an overview a Section 7 authorisation:

- removes liability;
- can only be issued to GCHQ and SIS;
- can be highly intrusive or may have no intrusive element;
- must relate to the agency's statutory purpose; and
- provides ministerial approval for the acts authorised.

The agencies do not self-task, all of their operations must link back to the intelligence requirement set by government.

Before granting an authorisation the Secretary of State must be satisfied of the necessity and reasonableness of activity to be authorised. In this context reasonableness includes, when appropriate, acting so as not to intrude on privacy any further than justified by the necessity to achieve what is authorised.

An application to the Secretary of State is accompanied by a submission which sets out the planned operation, the potential risks and intended benefits. The accompanying submissions can be long and there is room for cutting the length down, however, the submission must cover all the relevant points for example:

- a summary of what the submission is about;
- necessity for the proposed action;
- proportionality or reasonableness;
- a separate headed paragraph for privacy and intrusion if applicable;
- risks;

- legal issues which should set out the relevant aspect of law from commercial to criminal and international law; and
- at renewal the benefits obtained so far.

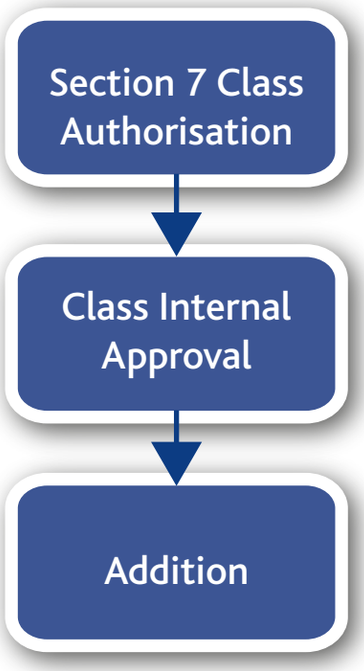
An executive summary may also be useful.

Class Authorisations

Class authorisations cover the core, routine business of SIS and GCHQ. Again they fulfil two functions. First they give protection for liability under UK law and second they provide political approval for activities authorised by the class authorisation. There are arrangements for the internal approval for the activity under class authorisations.

Government Communications Headquarters (GCHQ) Class Authorisations

Under class authorisations arrangements are in place for internal approvals and beneath those, specific 'additions'. A class authorisation could be for, for example, equipment interference operations overseas to obtain intelligence. An internal approval might be for implant operations within a specific context and then beneath this an addition which could refer in detail to the specific operational activities to be undertaken.



As I said in my previous annual report, I have been impressed with the formality of the audit trail and the level of consideration at GCHQ. It was clear to me that a great deal of thought was given to the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible.
I recommended that these approvals including additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ .

During 2015 I was able to scrutinise additions formally and I again commended GCHQ on their formal audit trail. I was impressed with the consideration given to protecting privacy but believe it could be set out more clearly in the paperwork. These additions made under class authorisations are not a legislative requirement but they are important and I **recommended** that, although necessity and proportionality was being considered, there should be headings in the form so that the consideration of those factors were set out more clearly. GCHQ provided me with updated versions of the forms to implement this recommendation.

These approvals did not have an expiry date but following a **recommendation** I made GCHQ, are conducting an internal review of each one. As they are being reviewed a date is then set for the next review period which may be 6, 12 or 18 months depending, for example, on sensitivities. This is not an expiry date and there is no requirement to set an expiry date but I commend GCHQ for implementing this process.

Secret Intelligence Service (SIS) Class Authorisations

SIS is tasked with operating overseas, dealing with threats and gathering intelligence in order to protect the United Kingdom (UK) and UK interests and the core of their operational work, including agent running, takes place under eight class authorisations. A Section 7 authorisation is there to protect an individual officer from personal civil and criminal liability when acting in the course of their employment. SIS authorisations set out considerations of necessity and reasonableness. When the operation involves intrusion into privacy, they are also required to set out consideration of proportionality and how the intrusion into privacy is justified by the intelligence to be gained.

Record Keeping

As I have said previously, I am keen to see SIS introduce a more formal recording process for decision making. Extensive records are kept in email reports. SIS introduced what was termed a "key decision document" to try and meet my recommendation. That has not been universally implemented. Further forms are in the process of being introduced.

The GCHQ method of internal authorisation may not be applicable to SIS particularly when operating overseas under the authority of a Section 7. However, I have suggested that SIS could, for example, apply the principles of the RIPA authority process so that proper consideration can be given to the same issues and then recorded. It is for SIS to determine how record keeping should be done but I have **recommended** that any process should prompt or guide people through important considerations of necessity and proportionality or reasonableness. In my view this will help to focus the mind at the decision making stage but also help with corporate and formal oversight of operations.

SIS Stations

An important element of my SIS oversight is to visit and scrutinise certain of the overseas stations in which they operate. At stations I am provided with their operational objectives and also technical plans, emails and other documents relating to their current ongoing operations. As I have said previously I am greatly impressed by the professionalism and dedication of the officers in stations often working in difficult conditions.

At one station I scrutinised a directed surveillance operation taking place under the authority of a class authorisation. I asked about collateral intrusion and the SIS officer was able to explain how this was taken into account. However, I noted that there had been no consideration given to this in the planning documents or email correspondence and commented that although RIPA does not apply, the principles should still be considered, and this needed recording.

This was not an isolated incident and highlights to me the importance of putting into place a better audit trail of operations taking place under class authorisations. This needs to come from the top of the organisation to introduce a culture of looking for authority and not relying solely on the Section 7.

v. Equipment Interference

Equipment Interference (EI) is the interference, remotely or otherwise, with computers, servers, routers, laptops, mobile phones and other devices under the authority of ISA Section 5 warrants or Section 7 authorisations.

Essentially EI is an intrusive power which allows the agencies to interfere with electronic equipment to obtain information. This could be, for example:

- interfering remotely or otherwise with computers, mobile phones, servers, routers or other equipment in order to obtain information, including about who owns the equipment, the nature and use of equipment;
- to locate and examine, remove, modify or substitute hardware or software;
- to enable and facilitate surveillance; or
- the creation modification or deletion of information on a device, server or network.

Information obtained may include communications content and/or communications data but all activity must be properly authorised and in pursuit of intelligence requirements.

As long as it is properly authorised, an EI warrant can obtain information stored on a computer or phone, including stored communications before or after its transmission. However, it cannot be used to authorise real time interception of communications. That requires an interception warrant under Part I of RIPA.

A draft EI code of practice was published for consultation in February 2015. An amended version was published in November 2015 and subsequently laid before parliament on 28 January 2016. You can find the code here. In its open response to the Investigatory Powers Tribunal in response to two complaints about EI the government confirmed that the agencies would apply the provisions of the draft code throughout the consultation period. The Code made public the powers and safeguards that existed previously.

The Equipment Interference (EI) or Computer Network Exploitation (CNE) terms have been used interchangeably but for the sake of clarity I have used the term EI throughout. It is worth noting that the activity covered by the EI Code is broader than traditional CNE operations. However, all CNE is EI and the safeguards contained in the EI Code apply to these operations.

Authorisation

The agencies' use of EI is governed by warrants and authorisations issued under the Intelligence Services Act. The EI Code contains guidance the agencies should follow before any EI can take place; it does not confer any new powers.

AUTHORISING EQUIPMENT INTERFERENCE		
WHERE	**WHAT**	**WHO**
UK **(4.1 of the Code)**	ISA Section 5	MI5, SIS and GCHQ
Overseas **(4.2 of the Code)**	ISA Section 5 ISA Section 7	MI5 SIS and GCHQ

Oversight

I have overseen the agencies' use of EI since I first took up post in January 2011 but it has not been possible to report publically on my findings since the existence of this technique had not been publically avowed. Reports of my inspections and oversight of this area have been contained in the confidential annexes to my annual reports.

My oversight is conducted alongside all other ISA warrants and authorisations using the same method as set out on my website and in previous annual reports.

As part of my oversight of this area I require that the agencies designate a senior official responsible for engaging with me during my inspections and overseeing implementation of any post inspection action plans I have recommended or approved, and reporting back as required.

The code of practice requires that particular consideration be given to cases where the subject of an operation might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information includes confidential personal information, confidential journalistic material, communications subject to legal privilege or communications between an MP and another person on constituency business.

As part of my inspections, in accordance with the code of practice, I require that:

- any case where a lawyer is the subject of EI be drawn to my attention during the next inspection and that legally privileged material which has been retained be made available to me;
- where legally privileged material has been acquired and retained it should be reported to me as soon as reasonably practicable – as defined by and agreed with me. Any material still retained should be made available if I request it including detail of whether it has been disseminated;
- where confidential material is retained it should be reported to me as soon as is reasonably practicable as agreed with me, and any material which has been retained be made available at my request;

- the agencies have in place additional internal handling arrangements to safeguard the processing, retention, disclosure and destruction of all information obtained by EI which should be made available to me; and
- all breaches of these handling arrangements must be reported to me.

Points Raised During 2015

Action and Property to be Interfered With

In an application for a warrant the agencies are required to detail the property which is the subject of the warrant, for example vehicles or residential houses, and the actions to be carried out in respect of the property i.e. techniques used by the agencies. Property and actions must be clearly set out so that the Secretary of State is clear what he or she is being asked to authorise. This information is used to construct the warrant instrument signed by the Secretary of State.

On occasion I have noticed that interference with computers is described in the section relating to actions when it should clearly be described as property to be interfered with. This will tend to happen when a warrant is required to enter a house and it is not known at the outset whether there will be a computer inside. I continue to **recommend** that computers must be an identified property on the face of the warrant instrument as property authorised and not an ancillary reference as action authorised. It could be argued that the warrant did not authorise such interference where a computer is not set out clearly as the property identified. MI5 have since implemented a process to address this problem.

It is not possible to amend a warrant issued under ISA so in relation to existing warrants I have **recommended** that the renewal submission should properly attribute electronic media as property to be interfered with. The danger is that the renewal will not pick up the "actions" section since renewals tend only to repeat the relevant property so computers will no longer be set out.

Under the proposals set out in the IP Bill such activity would require a separate Equipment Interference warrant to cover opportunities such as this.

Mobile Media

I voiced my concerns regarding the use of the wording "or other locations" in a warrant. I felt this to be too broad an interpretation of "property so specified". However, I have been persuaded that this has to be a standard requirement for mobile media.

GCHQ Technical Planning Meeting

At GCHQ I attended one of their weekly technical planning meetings. The meeting provides all relevant parties, including GCHQ's policy and legal, with oversight and assurance that EI tools, techniques and usage have been assessed as necessary given the potential benefit to be gained, and that they have been risk assessed.

This assurance and oversight is provided by peer assessment, covering development, infrastructure, operations and policy implications. Key agreements and decisions made during the meetings are documented to provide an audit trail and may be used in submissions to support the necessity and proportionality of using the technique in specific operations.

The meeting spent some time on the technical capabilities of using the technique and the challenges from peer review were at times adversarial. These are obviously bespoke techniques which are very technical but the meeting had to be in plain English so that the legal and policy people could also understand the proposal.

Bulk Equipment Interference

Current legislation does not allow for a bulk EI warrant. Overseas this can be authorised through a Section 7 class authorisation. In the UK it would be a thematic property warrant but the legislation requires that property covered must "be so specified", I discussed this in detail in my 2014 annual report. I would not expect to see a broadly termed warrant which authorises EI against an unspecified target. Individual consideration must be given to the necessity and proportionality of the EI.

vi. Bulk Personal Datasets (BPDs)

Under section 59A of RIPA, the Prime Minister published a direction on 12 March 2015 which put on a statutory footing my oversight of the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets, including any misuse of data and how this is prevented. There is a considerable public interest relating to the agencies holding of BPD and I would like this to be set out in greater detail than heretofore the way in which BPD is dealt with and how my oversight works.

Although at present there is no *statutory* definition of BPDs they are defined as sets of data which contain personal information about a wide range of individuals, the majority of whom are unlikely to be of intelligence interest. These datasets are often very large and cannot be processed or manipulated manually, and so they are held on analytical systems in the intelligence agencies.

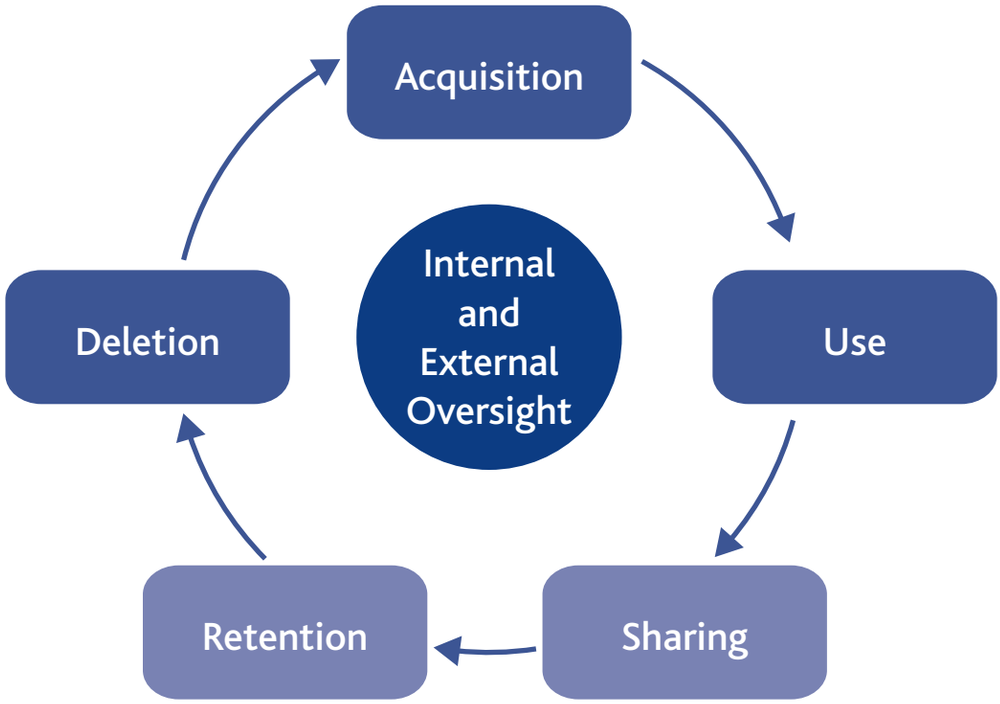
Section 2(2)(a) of the Security Service Act 1989, section 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994, also known as the "information gateway provisions", and section 19 of the Counter-Terrorism Act 2008 allow for the agencies to acquire and retain Bulk Personal Datasets (BPDs) overtly or covertly.

In order to carry out their statutory functions the agencies collect and draw on the datasets using them in conjunction with other information, which could include other datasets that are not bulk personal data, to for example: to fully identify a subject of interest; to obtain travel information of subjects of interest; to find links between them and other individuals or groups of interest; and to validate intelligence acquired by other methods. This capability enables threats to national security to be identified quickly. In my view this capability is a vital tool in the agencies fight against terrorism.

The BPD Lifecycle

Over the last few years a considerable amount of effort has been put into developing and implementing effective processes and policies to manage bulk personal datasets. The agencies have sought guidance and advice from me along the way to ensure that I am content.

There is an overall SIA Bulk Personal Data Policy which guides staff through all stages of the BPD lifecycle: Acquisition; Use; Sharing; Retention; and Deletion, as well as the oversight of BPD. Each agency has their own tailored BPD guidance which is aligned to the joint policy.



Sensitive Personal Data

In handling BPDs the agencies use the definition of 'Sensitive Personal Data' as it is defined in the Data Protection Act 1998 (DPA) and so the following types of information would all be classed as 'sensitive': racial or ethnic origin; political opinions; religious beliefs; membership of trade unions; physical or mental health conditions, sexual life; commission or alleged commission of any offence and any such proceedings for these. In addition to these types of information, the agencies must also record if information on the following is likely to be contained in a BPD:

- UK nationals
- Minors (under 16s)
- Journalistic Sources
- Legal Professional Privilege (LPP)
- Financial

If datasets are likely to include any data which could fall under one of these categories it must be clearly stated on the form requesting authorisation of the dataset. Datasets which contain sensitive information require a more robust justification to evidence why it is necessary and proportionate to acquire and retain the data.

Categories of BPDs

Bulk personal datasets generally fall into the categories below and can be obtained through various channels including: government, law enforcement and covert acquisition. At MI5 I queried that if the BPD is a government database, why they could not just ask the government department for the specific information required rather than holding a copy themselves. MI5 explained that by holding data in house they can fuse it with other sources of data and carry out complex analysis without having to employ more intrusive techniques to receive the same intelligence.

- Population/Biographical
- Travel
- Financial
- Communications
- Commercial

Acquisition of BPDs

In all three agencies before a BPD can be used for operational purposes a senior manager must authorise the use of the dataset. The authorisation form must make clear arguments that acquiring the dataset is justifiable, as well as both necessary and proportionate, in pursuit of the agency's statutory functions. It must also lay out the specific details of the dataset including whether it is likely to include any sensitive information. The agency will assess both the level of intrusion and the level of corporate risk of holding the dataset; which will determine how frequently the BPD is formally reviewed. The form must be endorsed by a legal adviser and a responsible officer designated.

When assessing the level of intrusion of a dataset, careful consideration is given to what the likely expectation of an average person would be about the data, for example would they expect an intelligence agency to hold that information on them. Several factors are taken into account including the expectation of privacy and the level of intrusion that the dataset is likely to represent, the agencies also consider collateral intrusion. This is reflected in whether the dataset is given a high, medium or low intrusiveness rating.

When considering whether to approve or reject an authorisation request, the authorising officer will look at the intrusiveness and sensitivity of the data and the level of corporate risk the agency will bear in holding and using it balanced against the necessity and proportionality case made to acquire and use the data.

If a request is rejected the dataset must not be acquired, or if the dataset is already in the agency's possession then it must be deleted or returned. A BPD cannot be operationally exploited unless the dataset has been authorised.

Use of BPD

Each search the agencies make of BPD must be necessary and proportionate to enable it to fulfil its statutory function. Staff are advised to exhaust less intrusive sources of information before using BPD. BPD is often used to try and identify a subject of interest and to eliminate the need to use more intrusive techniques. The use of BPD is increasingly important to the agencies as the magnitude of the threat increases and other means of acquiring intelligence are made more difficult for example by encryption.

There must be appropriate physical, technical and administrative safeguards in place to prevent and detect misuse of BPD and the analytical system it is held on. Datasets must be hosted on the most appropriate analytical system, taking into account the level of intrusion and the sensitivity of the data. Officers must take the relevant mandatory training and accept the appropriate code of practice or terms and conditions before they can access the systems. Access will only be granted if there is a clear business need and the individual has the correct security clearance.

The position is different as between the agencies. All three have technical systems in place which log all uses of analytical systems and with certain features (which for obvious reasons I am not going to expand on) that identify possible misuse. At SIS for example users have to justify and record the justification for each search of BPD. When I conduct my formal inspections officers know that I can pick any of their searches at random for further scrutiny, they then have to justify why they carried out the search, as well as explain to me why the search was both necessary and proportionate. In addition officers are made aware that disciplinary action will be taken against any staff abusing or misusing the BPDs, more information on the protective monitoring of BPD is covered later in this chapter.

At MI5 all desk officers can apply for access to basic BPD, but their access is limited by their specific role in the organisation and they can only access data that is relevant to their work. There are a much smaller number of 'advanced' users who have access to a larger number of datasets, including those containing more sensitive data. These advanced users are in specialist posts as some of these datasets require more advanced skills to interrogate and are used under a stricter range of security controls. These posts are often subject to sensitive post checks. SIS use a similar regime, they also have advanced analysts who can conduct more complex analysis or search data of a more sensitive nature. If desk officers need such a search they must complete a tasking form setting out the justification for the search.

At GCHQ only a small proportion of the staff have access to BPD, again this depends on the user's specific role, the majority of staff will never have access. Unlike MI5 and SIS, GCHQ does not have advanced users able to conduct more complex searches. Access to a greater number of datasets, or those of a more sensitive nature, is granted on a case by case basis determined by whether the

analyst has a genuine business requirement. Staff who have greater access undergo more comprehensive training on how to undertake complex analysis appropriately.

Sharing

All three agencies have an interest in acquiring and searching BPDs, but they will only seek to acquire a dataset once and will coordinate to prevent duplication of acquisition efforts. Before sharing a dataset with another agency the supplying agency must have justified that it is both necessary and proportionate to do so as well as confirming that it is for the proper discharge of their statutory functions, the receiving agency must do the same for receiving the data. These requests must be approved by a senior staff member at both agencies before any data can be shared.

If the agencies think there is merit in sharing datasets externally then it must meet the necessity and proportionality tests under the Security Service Act or the Intelligence Services Act as well as considering any wider legal, political or operational risks.

Retention

The agencies must keep under review the necessity and proportionality of continuing to retain each dataset. Each agency has a review panel that meets at least every 6 months and invites representatives from the other agencies to ensure consistency across the SIA, as well as legal advisers, technical teams, compliance teams or staff from the relevant business area.

The level of intrusion and the level of corporate risk of the dataset determine how frequently it is formally reviewed. If either level is rated as high the dataset will be assessed by the panel every six months; medium every 12 months; and low every 24 months. MI5 have also implemented additional meetings every two months so that any issues can be raised and discussed straight away, without having to wait for the next formal review panel.

Ahead of the formal review of a BPD at the review panel, the officer responsible for the dataset must update its record to include a retention case including details of how frequently it has been used and, where possible, examples of the operational value it has provided. If a dataset is not being used the review panel can request more frequent reviews to monitor the dataset more closely. They can also revise the levels of intrusiveness or corporate risk if they assess them to have changed since the authorisation or last review, this will also affect the period until the dataset's next review.

In their decision as to whether continued retention should be authorised the panel will consider various factors including: how often the BPD is used; the value of these searches; whether continued retention is necessary and proportionate; the levels of intrusiveness and sensitivity; the currency of the data and how unique it is;

and whether the intelligence benefit could have been achieved by other less intrusive means. If they agree to authorise they can add whether certain caveats or restrictions should be added, or if they reject the case made they will request that the data be deleted. If a retention case is not put forward for a BPD due for review then the panel will want to see evidence of its deletion.

After a dataset has been reviewed by the panel its records are updated with any comments or requests, the date of its next review if authorised or the date of deletion if rejected.

Where a copy of the same dataset is held by more than one of the agencies, each agency must make its own case for its continued retention.

Deletion

The agencies must not hold BPDs for longer than is necessary and proportionate. If the review panel reject the continued retention of a dataset then the appropriate team will be instructed to delete the data as soon as reasonably possible. They usually confirm at the next panel meeting that these datasets have now been removed from all systems.

Similarly if the officer responsible for the dataset can no longer justify the retention of the dataset they request that it be deleted and do not just wait for the next review panel. Or if there is only part of a dataset for which continued retention cannot be justified, then they can request that the appropriate sections be deleted rather than the entire dataset.

When requesting a dataset be deleted the responsible officer must consider whether the dataset has been shared. If the BPD has been shared with another agency the officer must contact them to agree future data ownership responsibilities. The other agency may be able to justify their continued retention if it has a different case.

Oversight

Prior to my inspections I request a list of the BPDs held by each agency. In this list I like to see: a short description of each dataset; the date it was acquired; the date ingested onto an analytical system; the levels of intrusion and corporate risk; when the BPD was last reviewed by a review panel; and if and when I last inspected the BPD. From this list I select a number of datasets at random to inspect in further detail. At the inspection I will be provided with all of the relevant documents and records in relation these datasets to scrutinise, I also speak to the individuals responsible for the dataset. In addition to inspecting individual datasets I also review all of the policies relevant to BPD, I request to see copies of the minutes from recent review panels, as well as overseeing the protective monitoring of the BPD.

At SIS inspections I also make a random selection from the total number of actual searches of BPD that have been conducted by officers since my last visit. I then interview the individuals who have carried out the searches and they must explain how they justified their search to me. It is important that they demonstrate to me: the necessity of why they needed to run the search; why the information could not have been obtained using a less intrusive method; how they narrowed their search criteria to reduce collateral intrusion; as well as explaining the outcome of the search and how the results contributed to their operation. If GCHQ and MI5 could also make this possible during their inspections I would find this particularly useful.

In the list of BPDs provided to me to make my selection the agencies must identify which datasets have been acquired by the interception of communications. I have agreed with the Interception of Communications Commissioner that any BPD acquired via interception, which once processed into a bulk personal dataset no longer identifies itself as intercept product, will be overseen by me in line with my oversight of Bulk Personal Datasets. If the object of an interception is to obtain BPD, the BPD authorisation process will have run in parallel to seeking the warrant. The Interception of Communications Commissioner will of course continue to oversee the interception warrant for obtaining the dataset. I will then oversee the authorisation of the dataset as BPD and its handling in accordance with the BPD Handling Arrangements. If either the Interception Commissioner or I have any concerns about the parts of the process which we individually oversee we have agreed to raise those matters with one another.

In addition to my oversight of BPD, the agencies have a number of internal oversight mechanisms which include controls such as completing mandatory training and signing terms and conditions or codes of practice before access is granted, internal monitoring and audits, this includes the audit of the individual search justifications at SIS and GCHQ.

Findings of the 2015 BPD Inspections

Security Service (MI5)

At the reading days I reviewed the paperwork for each bulk personal dataset that had been reviewed at the most recent BPD Review Panels. For the formal inspections I selected a number of datasets for discussion and closer scrutiny.

On the whole I was very pleased with the level of detail provided in the paperwork and only made some minor points. One of these was around a dataset the ingestion of which into an analytical system had been delayed; I reminded MI5 that the longer the period before the dataset is ingested onto the analytical systems; the harder it is to make a case for retaining the data.

Prior to the inspection MI5 had written to me to report an error in relation to three datasets which, due to an internal error, had not been incorporated into the BPD Review process and so had not been formally reviewed by the review panel, nor had

they been made available for me to inspect. MI5 explained how this had happened and the mitigation now in place to ensure it did not happen again. As soon as this error was noticed the datasets were entered into the next formal review panel. I read the records for these three datasets, and although I made clear that they should have faced a formal review at the correct time, I was content with the justifications detailed in the paperwork for acquiring and retaining them.

At the second inspection I noticed in two instances that despite the paperwork indicating the datasets had been used, in the free text fields of the forms there were comments stating that the dataset had not been used. MI5 explained that although answering the question of how many times the dataset has been used is mandatory, there is not an option to select "No use", therefore officers are selecting the box which states the minimum use possible and adding in as a comment in a free text box that there has not been any use. For clarity I **recommended** that a "No use" box should be added.

I also noticed some inconsistencies in the forms used when a dataset is to be deleted. In some instances a Data Deletion Form had been submitted, whereas in other instances the Data Retention Form was amended to say that there was no longer a case to retain and the BPD Review panel had taken a decision to delete. Following my **recommendation** to be consistent in the forms used for deletion, MI5 have confirmed that there is now one simplified Data Deletion Form which will be used for the deletion of both full and partial datasets.

Secret Intelligence Service (SIS)

During my inspections I was given SIS's updated internal code of practice for conducting BPD searches. This contained some very good information which would go a long way in providing reassurance to the public and would be very useful if this could be published externally. SIS told me that they were looking into how much could be made open.

At SIS staff must complete a justification box for each search to justify that it is necessary and proportionate for the purpose the user has selected, and confirm the intelligence requirement for the search. I requested to see these justifications for the individual searches I had selected for inspection. I advised that the text provided must be enough to evidence that necessity and proportionality were properly considered and users must explain how privacy has been taken into consideration, especially if the search is likely to return results for people of no intelligence interest. On challenging the officers who had conducted the searches I had selected, I was very pleased to see that the necessity and proportionality cases were thoroughly considered. However, I **recommended** that this be recorded, not just for oversight purposes but also for management information purposes. Following my advice SIS have since separated the justification box into 'necessity' and 'proportionality' boxes to ensure both are properly considered.

At SIS I looked at a number of searches conducted by the advanced analysts. I **recommended** that the recorded justifications for each search should specifically give consideration into privacy and that the tasking form should include separate sections for necessity and proportionality. SIS confirmed that advanced analysts always consider ways to minimise intrusion into privacy before they conduct each search. The responsible team communicates regularly with BPD users to encourage them to concentrate on the proportionality of their searches and remind them a disproportionate search would lead to a breach. I **recommended** that the advanced analysts should formally record the ways in which they have minimised intrusion into privacy.

As I reported in my annual report last year I was concerned about the number of datasets that had been acquired but were waiting to be authorised and loaded onto the appropriate analytical system. I was very clear that SIS could not justify the necessity for retaining datasets which they were not exploiting beyond a reasonable period. I am now happy to report that SIS have cleared this backlog and to prevent this problem from reoccurring they have set a target that all datasets will be authorised within six months of acquisition and have implemented a new team to manage this process.

As part of my inspection I was provided with the minutes from the recent review panel. I was very pleased to see that at the SIS BPD review panel held at the end of 2015 a large proportion of the datasets held were reviewed, and all those due for review had been considered.

When I visit stations overseas I speak to the officers who have access to BPD. I question them to confirm they have received the proper training and have signed the code of practice. From their response I was confident the officers understood the need to justify individual searches and that they were happy to request further justifications or refuse requests made by colleagues without BPD access. They explained that this is because users are personally responsible for their searches and that individual searches are subject to random auditing as well as protective monitoring checks, and therefore they would not be willing to take the risk of running a search that was not fully justified.

In my view SIS have made tremendous progress with the internal controls they have implemented for the use of BPD. These processes ensure that all use of BPD is necessary and proportionate and that the considerations are recorded at all stages of the BPD lifecycle.

Government Communications Headquarters (GCHQ)

On the whole I was content with the BPD paperwork provided for my inspections this year. However during the second inspection I discovered a BPD form which was not dated and there were apparent gaps where the internal processes and paperwork had not been properly completed in accordance with the GCHQ BPD

handling arrangements. Despite paperwork in 2013 stating that there was not a sufficient case to retain this particular dataset it remained on the analytical system for a further two years. GCHQ explained that this error had been caused by the dataset not having a nominated responsible officer. When ownership was transferred to another officer they immediately discovered the error and requested the dataset to be deleted. I was very clear that this is exactly what should not happen and was deeply concerned that there might be other examples. I **recommended** that all of the BPD paperwork should be searched to confirm that there were no other cases such as this. GCHQ have since confirmed that they have conducted this search and I expect to see the results at my next inspection.

During the inspection GCHQ brought to my attention a dataset where authorisation was not sought before it was shared with the other agencies, this is not in compliance with the BPD Handling Arrangements which require authorisation to be sought before any BPD is shared. Retrospective authorisation was sought after the error was discovered. I welcomed the fact that GCHQ raised this error, I acknowledged the urgent nature of this particular situation, but made clear the Handling Arrangements are clear and must be followed even in urgent situations.

Protective Monitoring

As I touched on earlier, the agencies employ a number of internal controls to prevent misuse of BPD; protective monitoring is one of these. Protective monitoring is the term given to the audit of BPD including both access to the analytical systems as well as the actual use. I like to see where possible the results of protective monitoring across all systems so I can be sure that the system as a whole works.

At all three agencies there are automatic processes in place to monitor and record each search of BPD in analytical systems. Searches can be triggered for investigation if, for example, a search is made which includes a term which is pre-defined by the protective monitoring team or if an officer attempts to search datasets which are not permitted within their current access rights. There are also random audits on individual searches.

During my inspections the protective monitoring teams at each agency present all of the investigations into possible cases of misuse and the results of random audits they have conducted since my last inspection. From this I am able to discuss any investigations which I feel are particularly concerning, or if I would like further information to determine that the investigations conducted have been thorough and that the correct conclusion has been reached. I am also very interested in what actions have been taken as a result of the investigation conclusions.

Summary by agency

MI5

When I inspect protective monitoring at MI5 this extends beyond the use of BPD and I look at protective monitoring measures in place across the organisation. This provides me with reassurance that the system as a whole works. I saw the results of all of the protective monitoring mechanisms in place, including the "false positives" where potential misuse has been flagged but on investigation a valid business justification was provided for the search.

In relation to non-BPD investigations a large proportion of the breaches issued were for searches of operational data which fell outside of the officer's specific remit of work. Throughout the year there were six instances where unauthorised devices had been inserted into MI5 systems, for example charging a mobile phone. I take these breaches very seriously and I wanted to know what actions had been taken to prevent reoccurrence. MI5 explained that a notice has been circulated re-emphasising that phones cannot be charged at computer terminals. I was also concerned to see that a number of the breaches issued in relation to these non-BPD misuse investigations, as well as one BPD breach, were by individuals who were not permanent MI5 staff. It is very important that the parent organisations treat breaches as seriously as MI5 do when a breach is issued to a member of their own staff. MI5 explained that they had written to the organisations concerned stressing the gravity of the issue and expressed their displeasure at the situation.

I was also keen to understand why the number of breaches had significantly increased in relation to one particular non-BPD database. MI5 explained that this was due to a change in the policy which governs what staff are permitted to search for on this database. Staff were not applying the new policy when they ran their searches. I recommended that a warning could be added to the system, or if this was not possible, then a notice should be circulated to remind staff of the new policy and inform them that I am very concerned about the high number of breaches. At my next inspection I do not expect to see such a high number of breaches.

SIS

The protective monitoring arrangements at SIS are highly classified, access to and knowledge of the techniques is highly controlled. Staff who work in this area are subject to additional security screenings before they gain access to the systems or understand the actual checks that are in operation to detect anomalies and misuse of BPD. The results of these checks are monitored by the team who seek additional information or launch investigations if there are any concerns of misuse. They also provide advice and answer any queries from officers in relation to their searches and the justifications required before a search can be run.

In the first half of the year there were no disciplinary cases, moderate or minor breaches at SIS in regards to their use of BPD. In the second half of the year protective monitoring tripwires led to two moderate breaches being issued. Across both periods SIS carried out regular random investigations. These investigations are not generated by protective monitoring tripwires but look at the justifications given for each search to ensure each search is necessary and proportionate. No breaches were issued as a result of these investigations.

Two breaches have occurred in SIS where users were able to use their previous access to BPD in a different role within the organisation. Use of BPD is job specific and BPD access restrictions must be manually updated each time users change roles. To try and prevent such breaches SIS have briefed the IT Access Management team to ensure they are following the correct procedures when users move roles and have updated their BPD Code of Practice and informed all BPD users to say: "If your role changes and you are required to do work that is different to the role described on your original BPD application form, you must consult the data compliance team".

I am particularly impressed at how rigorously the team monitor the use of BPD, the only point I will continue to repeat is that the disciplinary measures for misuse need to be consistent across all three agencies.

In relation to overseeing the use of protective monitoring across areas other than BPD, I was given a summary of the results of protective monitoring and investigations conducted across SIS' corporate network, which was very useful in showing how effective and comprehensive the protective monitoring checks in place are.

GCHQ

Similarly to SIS the protective monitoring arrangements at GCHQ are highly classified and subject to additional security clearance.

This year I was shown the protective monitoring checks that are in place at GCHQ and I was very pleased to see that the level of monitoring in place was exactly what I would want to see. These do not extend over all operational systems, but they do cover all of the key systems including BPD. Although I recognise my statutory oversight in respect to protective monitoring is limited to bulk personal data I would like access to protective monitoring of personal data across all operational systems at GCHQ. As I have discussed in relation to the other two agencies having sight of investigations and breaches detected in other areas outside of BPD helps to provide assurance that the system as a whole is robust. This year GCHQ have shared with me the results of protective monitoring across a number of their other operational systems

In the first half of the year there was no misuse of GCHQ's BPD holdings. There were however 14 investigations which were triggered as a result of the protective monitoring systems. Although GCHQ confirmed that on investigation all of these searches had a legitimate business reason and were both necessary and proportionate, I requested further information about these flagged searches as well as the investigations conducted.

In the second half of the year there was no misuse of GCHQ's BPD holdings, the results of protective monitoring on another operational system were brought to my attention for which there were four investigations, none of which resulted in a breach.

I raised the point as I also did at MI5 and SIS that I am keen to see the agencies work together to ensure that misuse of data is sanctioned in the same way. In response to this the agencies have set up a working group to align SIA breach and disciplinary policies and I look forward to learning of its progress in 2016.

vii. Consolidated Guidance

The Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees (the Guidance).

The express focus of the Consolidated Guidance is on torture and cruel, inhumane or degrading treatment (CIDT) and this is consistent with there being an absolute prohibition in national and international law on any such conduct and with the fact that the practical concern is with extremely vulnerable individuals, namely, those in State detention outside the UK.

In November 2014 the Prime Minister tasked me to examine the concerns the Intelligence and Security Committee of Parliament (ISC) raised on the Government's responsibilities in relation to partner counter-terrorism units overseas. This report is being published supplementary to my annual report. In this section I report on compliance with the Guidance during 2015.

Overseas Security and Justice Assistance (OSJA) Guidance

On 28 February 2014 a revised version of the OSJA guidance was published which applies to all HMG officials including the intelligence services. During 2015 I have seen that the agencies and MOD take OSJA into account when they share intelligence or receive intelligence. I am required to keep under review compliance with the Consolidated Guidance so I have limited my observations to that. However, I have said more about this in my supplementary report relating to the concerns of the ISC.

What I Oversee

a) When a detainee in the custody of a foreign liaison service is interviewed;

b) When information is sought from a detainee in the custody a liaison service;

c) When detention is solicited;

d) When information is shared with a liaison service relating to a detainee; and

e) When unsolicited information is received from a liaison service relating to a detainee.

With regards to the first three it is normally quite easy to see that the Guidance applies and must be taken into consideration. I have made it clear to the agencies and to the MOD that when information is shared they must also consider if detention is the likely outcome and not just that it relates to a detainee. When unsolicited intelligence is received the agencies must consider if continued receipt of intelligence might be perceived as encouragement to continue sharing or of the methods used to obtain it.

How I Oversee the Guidance

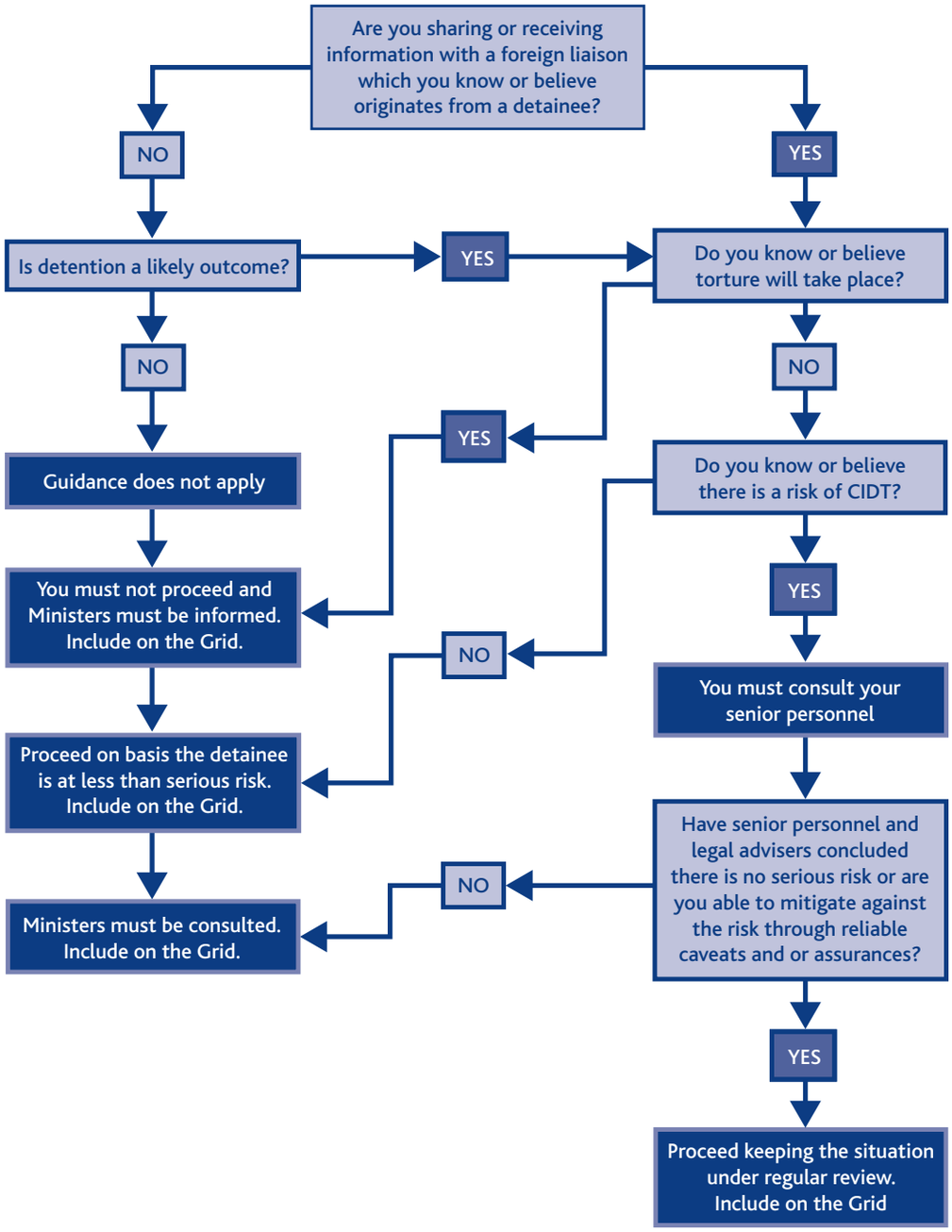
In my oversight of the Consolidated Guidance I seek to monitor whether the guidance is being followed properly so that when a detainee held by a third party is involved staff know and understand immediately that the Guidance applies and that decisions are then taken at the correct level. To do this I apply the judicial review principle so I do not second guess the decision to share or not to share intelligence or consider whether I would come to the same conclusion. Instead I check to see that a reasonable decision was made and the correct tests are applied. I have explained in previous reports that I conduct this oversight though a grid which sets out individual operational cases where the Guidance has been considered and the level at which the decision was taken. I encourage the agencies to include cases where they considered the guidance but determined that it did not apply, either because intelligence would not be shared/received or because the country has a good human rights record and proper due process. For the most part the grids were accurate. Errors were minor and tended to be because the agency was attempting to be helpful. I have **made it clear** the grid must set out what was done at the time and not what the agency now knows to have occurred.

I selected some cases for closer scrutiny. The agencies provided me with supporting documents and/or Ministerial decisions to help demonstrate compliance.

Following my inspection the head of my secretariat produces a separate inspection report relating to the Guidance covering points made during the inspection and recommendations made to either improve or demonstrate compliance.

Does the Guidance Apply?

The Consolidated Guidance provides further information relating to passive receipt of unsolicited intelligence and questioning a detainee but in the majority of situations the officer concerned must consider:



I also expect to see cases included on the grid if at any stage a decision is taken not to proceed because the likely risk of CIDT does not justify sharing intelligence.

Forms

I was content that both the MOD and MI5 had good forms which guided users through the process of considering the Guidance and recorded that consideration and compliance with the guidance. GCHQ had different paperwork and I **recommended** they consider the forms used by MI5 and MOD to guide their application of the Guidance with a view to incorporating it into their process.

At SIS I noted that their record keeping in relation to the Guidance had greatly improved and they were now in line with the grid format. I **requested** that they flag up if they were relying on a Ministerial submission.

Mitigating Against Risk: Liaison Relationships and Assurances

An important part of my oversight of the guidance relates to the risks associated with working with overseas liaison partners and how the agencies mitigate against any risk of CIDT. Given that SIS own the liaison relationships, MI5 and GCHQ use their assessments.

When SIS believe that they are able to work with a liaison partner because they have been able to mitigate against risk through reliable caveats and assurances they will submit to the Foreign Secretary setting out the reasons why they believe that there is a less than serious risk. The guidance only requires submission to a Minister if there is a risk of mistreatment but in this way the Foreign Secretary is made aware of possible risks and how SIS have mitigated them.

I have continued to re-iterate that, when obtaining assurances to mitigate against CIDT by liaison partners, best practice is to obtain them in writing wherever possible. If it is not possible to obtain written assurances from the liaison partner then a written record of oral assurances should be sent to the liaison partner. At a very minimum there must be a written record of any oral assurances. Obtaining written assurances signed by a liaison partner can be difficult and has to be delicately and diplomatically handled. I **recommended** to SIS that they reconsider their form of words used when they seek assurances and tailor them to each situation so that liaison services would be more likely to sign them.

It is important that compliance with assurances is monitored. I was shown evidence that SIS investigate if an allegation is received to suggest that a liaison partner is not complying with the assurances received. If a credible allegation is made they will cease intelligence sharing while the allegations are investigated through diplomatic channels.

Where SIS write to Ministers to set out their belief that there is no serious risk of mistreatment or CIDT because they have received assurances, MI5, GCHQ and MOD often rely on this assessment. When this happens I have asked that this is reflected in the paperwork provided to me and in the grid for oversight. I expect to see that individual assessment is made to ensure that the particular incident of intelligence sharing falls within the parameter of SIS's ministerial submission.

Due Process

In situations involving serious risk of CIDT the Guidance is clear that Ministers must be informed and decisions should be taken on a case by case basis. The Guidance is clear that the lawfulness of arrest and detention must be taken into consideration as unacceptable treatment.

There are occasions where there has not been proper due process because every day inefficiencies in the system caused a detaining authority to miss their own deadline by a day or two, for example for bringing the detainee before a judge. The Guidance does not differentiate between minor failures and more major procedural failures.

In relation to due process, I have discussed with SIS at what point they should revert to the Foreign Secretary on detainee issues when the lack of due process is being considered. Do they have to revert to a minister in each case or could the minister consider the situation in a 'framework' submission? My advice has been that if the consistent point relates to minor issues like missing a deadline by a day, a framework submission could be used, otherwise particular situations must be referred to the minister if the Guidance is to be complied with.

Unsolicited Receipt

The Guidance covers receipt of unsolicited intelligence from countries detaining an individual. If the agencies know or believe the intelligence has come from a detainee who has been mistreated they must not continue to request further intelligence so as to encourage the detaining country to understand they approve of the mistreatment. The agencies also have to deal with situations in which it is a third party country which has received information and has passed it to the agencies. The consolidated guidance does not apply but in such situations I **encourage** the agencies to apply the Guidance as far as they practically can and they are keen to do so. If in doubt a minister should be consulted and the minister should be supplied with all steps being taken to mitigate the risk of mistreatment.

Non-State Armed Groups

The Guidance also does not apply in relation to non-state armed groups. However, in a paper published by Chatham House they recognised that these groups may need to be engaged with for the sake of the people who live in the territories they control. Although the Guidance does not apply I again encourage the agencies to apply the principles of the Guidance as far as they practically can. There are situations where not engaging with these groups would be difficult to defend, for example if they are detaining or have information about the detention of an aid worker. Again Ministers should be informed and that should include action taken to mitigate against risk of mistreatment.

Continued Oversight

The IP Bill does not make provision for oversight of the Consolidated Guidance under the proposed Investigatory Powers Commissioner. However, there is provision for the Prime Minister to issue directions in the same way he has done previously. I hope that such a direction is made and that oversight of the Guidance continues after the Bill is implemented. The agencies welcome oversight of this complex area so I believe they would also prefer for it to continue.

Statistics

These statistics require a strong caveat. The cases provided in the grid include cases when the Guidance was considered but a decision was taken that the Guidance did not apply or cases where the UK was confident that there was a less than serious risk of CIDT. These figures simply reflect that proper consideration of the Guidance was applied and nothing more in these cases.

The total number of cases where the Consolidated Guidance was considered during 2015 was **442**. Of these I reviewed **68** cases.

Conclusion

At MI5, GCHQ, MOD and SIS I was content that in all instances I reviewed agency and MOD staff had considered the risk of mistreatment or unacceptable conduct as set out in the Guidance. Staff demonstrated that they had considered the risk of mistreatment or unacceptable conduct of any detainee as set out in paragraphs 9 – 11 of the Guidance. I found that the grids presented to me had, for the most part, been completed properly. Any errors were minor.

GCHQ reported a number of occasions where the duty officer had not considered that the Guidance applied before sharing intelligence with a foreign liaison. In each case GCHQ quickly recognised that this had happened and conducted a retrospective assessment. All of this was set out for me in the grid and available for my oversight. Although this is unacceptable, GCHQ assured me that it is being reviewed as part of a wider review of the duty officer's functions.

4. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS

In my report last year I said that for the last two years I have asked that my oversight be extended to the use by the agencies of operational data obtained under Part II of RIPA or ISA Sections 5 and 7. This is now an explicit part of my oversight of Equipment Interference and, as I said last year, on a broad reading of my remit I can and should oversee at least the retention storage and deletion of product obtained from those warrants and authorisations which fall within my remit.

Last year I asked the agencies and the MOD to be clearer about:

- the retention policy for information which is not of intelligence interest, which should by preference be immediately destroyed;
- the procedure used to handle information retained for evidential purposes which could include information not of intelligence interest;
- the procedure to handle information not to be retained;
- the policy for deletion of all product;
- procedures enforcing compliance with handling arrangements.

With that in mind I asked the agencies to provide me with their handling arrangements and I have been provided with them by all three agencies and the MOD.

Initially I was supplied with arrangements relating to the rules in place for dissemination of intelligence. I was pleased to see that these arrangements were in place but I also wished to see arrangements in place regarding retention, storage and deletion. This intelligence may relate to an individual's private or family life and may constitute an interference with their Article 8 rights. The authorisation process provides consideration of the necessity and proportionality of obtaining the intelligence but similar consideration must be given to disclosure and retention.

The arrangements are set out in a number of different documents so I have recommended that there should be one document which can then be referenced in submissions. Rather than saying that intelligence will be retained "in accordance with the normal handling arrangements" it ought to reference which section of the arrangements apply and these arrangements should be made available to the Secretary of State, the warrantry units and to the relevant oversight body.

5. ERRORS

The Equipment Interference (EI) code of practice introduced a new, mandatory, category of error reporting any breach of the EI handling arrangements. This is additional to the error reporting process already in place and set out in previous reports. However, in view of this new requirement I have reviewed the categories of error reporting and clarified what I require from the agencies and the MOD.

Category A Errors

Administrative errors are an obvious "slip" where no unauthorised intrusion into privacy had taken place as a result of the slip.

An administrative error occurs where:

- it is clear on the face of a document that a typing error has occurred,
- the correction is obvious, and
- a court would amend it under its "slip rule".

The "slip rule" allows a court to correct an accidental slip or omission in a judgement at any time if it does not reflect the court's intention. In this context, administrative errors could be an obvious administrative mistake such as a misspelling, incorrect year or failure to update a template.

I have asked that when discovered, these administrative errors are bought to my attention. This should be done in writing bi-annually at inspection.

Category B Errors

As I set out in my 2014 Annual Report, as part of my oversight function and in addition to my bi-annual inspection, I require the agencies to report to me any errors that are discovered to have occurred inadvertently during a warrant application, authorisation or during the operation of the warrant.

These could be, for example:

- an inadvertent failure to obtain an authorisation;
- operating under a lapsed authorisation, an inadvertent failure to renew an authorisation;
- operating outside the parameters set out in the authorisation in the mistaken belief that it was authorised; or
- failure to comply with other requirements of the Codes of Practice such as record keeping.

In these cases, but for the inadvertence, the application would have been granted and/or any conduct would have been properly authorised.

In relation to Equipment Interference any breach of handling arrangements must be reported to me in accordance with the code of practice.

For Category B errors the error should be reported formally to me within three months of the date the error was discovered. I expect the report to explain:

1. when the error occurred
2. when it was discovered
3. the nature of the error
4. how it happened
5. what, if any, unauthorised intrusion into privacy resulted
6. what, if any, product has been obtained and what has happened to this product
7. the steps taken to prevent a reoccurrence of this error.

If it is not possible to report the error within this time because of the investigation required then I require the agencies to send an interim notification to my office.

Category C Errors

This would be a deliberate decision taken to obtain information without proper authorisation or in any way to act irresponsibly. Once again this year, I have not found or had reported to me any Category "C" errors. Such deliberate acts must be reported to me immediately upon discovery. If such a deliberate act were to be committed, those involved would be subject to disciplinary action and possible criminal charges.

Reporting Errors

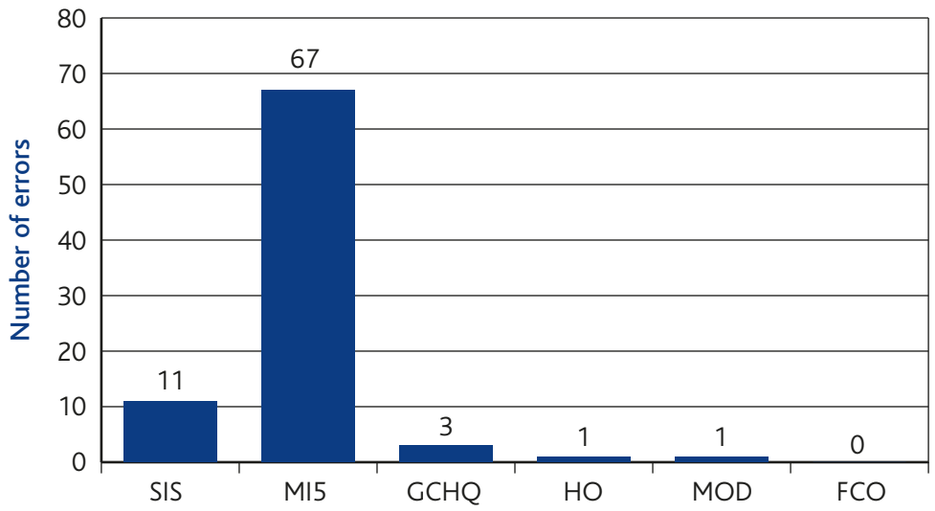
My main concern has been the time taken to report errors. I have agreed with all agencies a procedure by which they notify any potential error they discover which may take longer to investigate and then agree with my office a timescale for reporting if an error has occurred. As I requested last year the agencies now notify me when they anticipate an error investigation will take longer than the three month time limit for reporting errors, and that is an improvement from 2014.

Unfortunately sometimes the agencies still exceed the agreed timescales. For example in one case at GCHQ I was informed that a potential error had occurred in January and following a rigorous and extensive investigation it was then only formally reported in July. But on the whole there has been an improvement and the agencies are conscious of the need to report as early as possible.

Summary of 2015 Errors

In 2015 there were a total of 83 errors. This is quite a significant rise from the 43 errors of 2014.

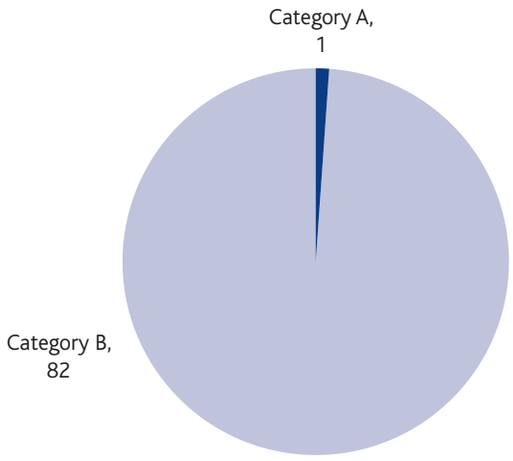
Errors reported in 2015 by organisation



Please note that MI5 obtain a significantly larger number of warrants and authorisations than the other agencies, and their error rate is in fact low as a proportion of authorisations.

82 were Category "B" errors or inadvertent errors and only one was a category "A" or administrative error. There were no Category "C" errors which was the same as 2014.

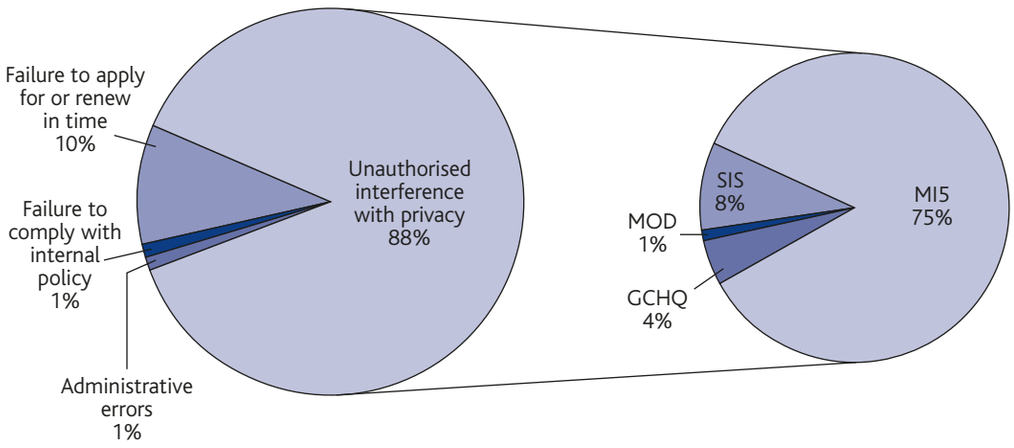
Errors reported in 2015 by category



Of all the errors, the most common error was because of an unauthorised interference with privacy. The least common errors in 2015 were due to administrative reasons. There were no recorded errors that were due to unauthorised disclosure in 2015.

If we look at the breakdown of errors due to unauthorised interference with privacy then we see the majority of these were made and reported by MI5.

Breakdown of 2015 Errors by Type and further breakdown of the unauthorised interference with privacy



Breakdown of errors by organisation

Security Service (MI5)

In 2015, MI5 reported 67 errors to me. Of the 67 errors:

- almost all were caused by human error and all resulted in intrusion into privacy to some degree;
- none were caused with the intent to obtain information without the proper authority;
- if proper authorisation or proper procedures had been followed the authorisations would have been granted;
- these errors were caused by a variety of reasons for example allowing an authorisation to expire, failure to apply in sufficient time or misnaming.

Secret Intelligence Service (SIS)

In 2015, SIS reported 11 errors to me. During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

Of the 11 errors:

- almost all were caused by human error and resulted in intrusion into privacy to some degree;
- none were caused with the intention to obtain information without the proper authority.

Government Communications Headquarters (GCHQ)

In 2015, GCHQ reported three errors to me which resulted in unauthorised interference with privacy. None were caused with the intent to obtain information without the proper authority.

During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

Home Office

During my inspections of the Home Office Warrantry Unit, one administrative error or Category "A" error was brought to my attention which I asked the Home Office to write formally to me about.

MI5 had reported to the Home Office that they had made a slip on the wording on the face of the warrant. I advised that the Home Secretary could correct in manuscript and initial and date the amendment, but the Home Office explained that it had been renewed since then so a new warrant had been sought. In that circumstance I accepted that this was the correct thing to do, advising them to report an administrative error.

Ministry of Defence

The Ministry of Defence reported one error to me during an inspection, which I asked that they formally report to me.

The error occurred during two periods of directed surveillance which took place without any formal authorisation where surveillance teams were deployed for a length of time believing a DSA was in place. Once the error was recognised surveillance stopped until a DSA was in place.

6. RIPA/ISA STATISTICS

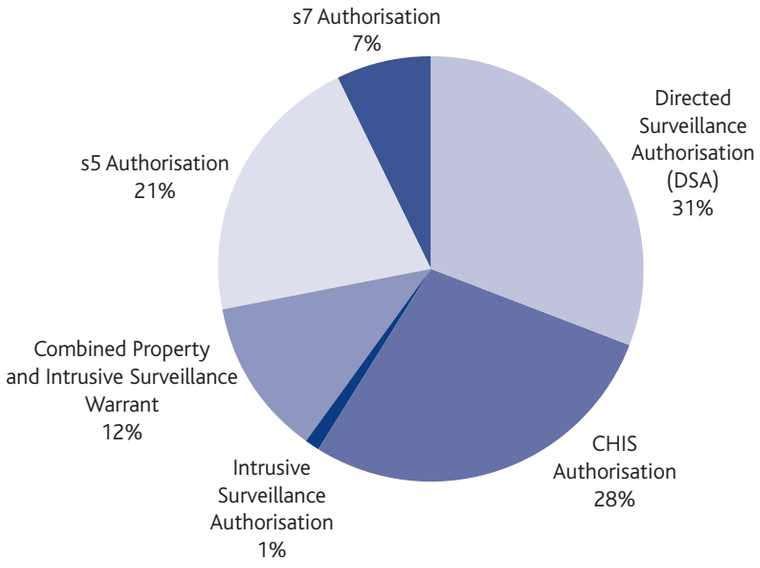
I select warrants to scrutinise from a full list of extant warrants and authorisations provided by the agencies and the MOD. Included in these lists is a short description of each warrant and authorisation. In this list I see *all* authorisations and warrants presently in place. I then select a number of these for closer scrutiny at my formal inspections where I examine the authorisation or warrant itself, as well as all of the supporting documentation including, for example, the submissions written to Ministers.

The total number of RIPA/ISA warrants and authorisations extant at the end of 2015, across the agencies and MOD, was **1,560**.

This figure does *not* include renewals so, for example, if it is necessary and proportionate for the activity to continue a DSA needs to be renewed every six months. The first authorisation is only for three months, each renewal after this is for a six month period. So a DSA could fall for renewal twice in one year.

In broad terms the types of warrants and authorisations I oversee which were authorised during the year, including renewals, are as follows:

Breakdown of Warrants/Authorisations issued during 2015



Of the RIPA and ISA warrants and authorisations in effect in 2015 I scrutinised **499**. Each authorisation or warrant has multiple supporting documents so the number of documents I scrutinise is much higher. I also scrutinise a number of internal approvals made or issued under certain Section 7 authorisations which are not included in the figure above.

7. BRIEF SUMMARY OF ASSESSMENTS

Security Service (MI5)

	Round 1	Round 2
Selection	11 May	20 October
Pre-Reading days	1-3 June	24-28 November
Inspection days	24 June	16 December
Under the bonnet	13 January	29 September

MI5 Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made the case for necessity in the individual cases.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out in the paperwork I selected for scrutiny.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out separately and properly weighted in the paperwork I selected for reading. I would like to see the case set out how MI5 will minimise intrusion into privacy which is not required to meet the intelligence need.

Prior to inspection MI5 informed me about their proposed Retention, Review and Disposal (RRD) policy for warrants, submissions and associated paperwork. They previously stored all paperwork in hard copy at a secure storage facility which was running out of space. They proposed that:

- Live warrants be kept in hard copy;
- Cancelled warrants be retained in hard copy for 5 years then scanned onto their system and kept in soft copy only;
- Pre-existing warrants cancelled more than five years previously would be destroyed;
- Submissions would remain available if required;
- The product obtained through warrants is covered by separate arrangements.

I **agreed** that the proposals appeared both sensible and in line with the code of practice but suggested waiting until IOCCO completed their review of retention of warrantry documentation before taking a final decision.

I raised a number of other issues:

- I asked MI5 and the Home Office to ensure that applications to renew a warrant be made shortly before expiry and the Home Secretary be provided with the most up to date information to consider.
- Ensure training and guidance is sufficient to make sure the correct form of words is used when a device is waiting for extraction so that it reflects that it is no longer proportionate to use the device for intelligence purposes.
- I noted that MI5 often fail to set out in their submissions consideration of the steps taken to minimise or mitigate intrusion into privacy and record what they will do with any product obtained which is not of intelligence interest. I am satisfied that this takes place but believe it should be better recorded.

Secret Intelligence Service (SIS)

	Round 1	Round 2
Selection	8 April	20 October
Pre-Reading days	6-7 May	10-11 November
Inspection days	13-14 May	17-18 November
Station Visits	9-10 March (Europe)	27-29 October (Europe)
Under the bonnet	28 May	18 November

SIS Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity in the individual cases.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The cases for proportionality were set out in the cases I selected for scrutiny. There was one Section 5 warrant which I recommended required further work to ensure the property covered is more specific.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected. In one overseas station visit the cases for privacy were mostly set out in the paperwork viewed although improvements could be made in recording this. In addition collateral intrusion was not evidenced in one particular DSA authorisation.

I assessed that the operations I selected for scrutiny were lawful but in some cases the argument for necessity, proportionality and privacy could have been set out more clearly in the paperwork.

At each inspection, both in the UK and at overseas stations, I discussed SIS substandard paperwork and the need to introduce a more formal process to record decision making and provide a better audit trail. When operating overseas under the authority of an ISA Section 7, SIS should apply the same principles as the RIPA authorisation process so that proper consideration was given to the key issues including necessity and proportionality, and this consideration recorded. Doing so would allow for improved accountability, proper management and facilitate oversight. Although I was confident that proper consideration was given it was not possible to see this set out in one document.

I also raised a point at the FCO. If the Foreign Secretary had commented so as to restrict the use of a warrant then this should be properly reflected on the face of the warrant and, if it was not, SIS should return the warrant to the FCO to reflect this.

At SIS I emphasised that with the advent of the Investigatory Powers Commission it would be more important than ever to ensure record keeping across the organisation is done to a consistently high standard. SIS introduced a 'key decision document' to be used to record decisions. That has not been very effective and recently a further set of forms has been produced which hopefully will produce better records of decisions and how they were reached.

Government Communications Headquarters (GCHQ)

	Round 1	Round 2
Selection	12 March	17 September
Inspection days	21-23 April	21-23 October

GCHQ Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity although this could have been set out more clearly in the Section 7 electronic addition process.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out in the cases I selected for scrutiny although this could have been set out more clearly in the Section 7 electronic addition process.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected apart from additions which did set out separate consideration.

I believe that GCHQ are doing a very difficult job well and that staff are working hard to get things right. GCHQ paperwork was of good quality and the various forms were much improved. The Director of GCHQ said that oversight was useful in emphasising to staff the importance of full and accurate documentation.

The operations I selected to scrutinise were lawful and the paperwork was generally in good order but in some cases the argument for necessity, proportionality and privacy could be set out more clearly in that paperwork.

GCHQ briefed me on their compliance review which took place in April-May 2015. It covered everything from authorisation and storage to retention and deletion of product. One issue the review highlighted was analysts retaining data outside of corporate repositories, for example on local drives, which was not then deleted at the appropriate time in accordance with GCHQ policy. The GCHQ Board strongly endorsed the recommendations made. I asked to see this formal report and GCHQ provided it for me.

Following my earlier **recommendation** GCHQ now sets out clearly in their warrants that they are subject to the conditions described in the accompanying submission.

Ministry of Defence (MOD)

	Round 1	Round 2
Selection	12 May	2 November
Inspection days	4 June	19 November

MOD Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity.
PROPORTIONALITY **Was the case for proportionality made In each case inspected?**	The case for proportionality was set out in the paperwork I selected for scrutiny.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I selected for scrutiny.

HMG does not accept that RIPA Part II applies to activities outside the United Kingdom but the authorisations are obtained as if it did. I was impressed by the high quality paperwork produced in the areas I oversee at the MOD, particularly by the Special Forces.

The MOD voluntarily apply a high compliance standard to RIPA principles. I noted that the paperwork was good and that necessity and proportionality had been properly considered. As a minor point I would like to see some more detail setting out what would happen to intelligence obtained through the use of intrusive techniques. However, I was satisfied that arrangements were in place. I asked that the MOD make their data retention policy available during my scrutiny visits in future and also asked the MOD to set out in the "intrusion" section of the RIPA forms details of how product would be managed, and this could refer to paragraphs of the data retention policy.

I **recommended** they create a stock form to allow them to modify a DSA authorisation.

Home Office

	Round 1	Round 2
Selection	10 June	27 November
Inspection days	25 June	10 December

Home Office Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions provided for the warrants I selected made a case for necessity.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I scrutinised, although consideration of LPP material was missing from one property warrant which I requested be followed up.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected. However, consideration of how to mitigate against unwanted intrusion into privacy was not always evident.

On the whole I commended the Home office for the quality of its paperwork, including comments on applications and appropriate push back to MI5. They provided me with a useful document setting out the significant progress and developments since the last inspection and they are well on the way towards achieving the recommendations I made last year. They are generally doing well with a few recommendations which I will continue to monitor. I saw evidence that the warrantry unit questioned the submissions made by MI5 as and when appropriate.

On one occasion I noted that where a number of people were mentioned in a submission it was not reflected on the face of the warrant. It would be better to name the individuals when known. The Home Office agreed and explained that they would normally do so but there had been an oversight in this case.

There were a number of warrants in which interference with computers was mentioned in the section relating to actions when it should clearly be described as property to be interfered with. I was clear that this was not satisfactory and interference with computers must be set out as property to be interfered with. As the Home Office are responsible for drafting the warrant instrument I asked them to ensure this does not happen in future.

The Home Secretary takes her responsibility to consider the necessity and proportionality of what she will be authorising very seriously. In addition to the submission from MI5 her staff do a detailed one considering the case necessity and the question of proportionality. She applies herself personally to the appropriate considerations.

Northern Ireland Office (NIO)

	Round 1	Round 2
Selection	14 May	29 September
Inspection days	8-9 June	4-5 November

NIO Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The paperwork provided made a case for necessity.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was mostly set out clearly in the paperwork I reviewed. Proportionality could be improved by setting out what will happen to product obtained which is not of intelligence interest.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out in the paperwork I reviewed. Consideration of collateral intrusion, ways to mitigate against this and what would happen to any product obtained was sporadic.

I was satisfied that the paperwork provided was in good order and there were no slips or errors. NIO generally put a lot of care into the papers presented to me and make themselves available to answer any questions or produce any documents I request. I observed that the NIO are thorough and careful when looking at submissions from MI5 and ask for clarification as needed before submitting to the Secretary of State.

I raised points around privacy, collateral intrusion and management of product obtained. Most of the submissions I scrutinised highlighted the potential for collateral intrusion, whether this was into family members', co-habitants' or others' privacy. But many did not then go on to specify how this intrusion would be limited or mitigated and what would be done with any product of collateral intrusion. I **recommended** that NIO and MI5 work together on the description of collateral intrusion and the steps they can take to limit it, as well detailing how any collaterally obtained product would be dealt with. NIO agreed to take this forward with MI5.

Foreign and Commonwealth Office (FCO) for SIS

	Round 1	Round 2
Selection	8 April	20 October
Inspection days	14 April	18 December

FCO (SIS) Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions I scrutinised mostly set out a case of necessity. In one case this could have been set out better.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected.

Foreign and Commonwealth Office (FCO) for GCHQ

	Round 1	Round 2
Selection	13 April	11 November
Inspection days	17 April	30 November

FCO (GCHQ) Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions provided for the warrants and authorisations I selected for inspections made the case for necessity.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I inspected.

Foreign and Commonwealth Office (FCO)

At the FCO I covered in detail how the FCO ensured and oversaw that assurances contained in submissions are met. FCO explained how they tracked conditions against the Secretary of State's requirements including that any such conditions are set out in renewals. I advised that the FCO formalise their policy so they are in a position to demonstrate the tracking process to the new oversight body.

In relation to record keeping the FCO agreed to speak to SIS again about it. I **recommended** that the FCO monitor that GCHQ review internal approvals made under class authorisations appropriately.

I reviewed a sample of GCHQ's monthly update notes to the FCO containing details of the authorisations under a number of class authorisations and was satisfied that the FCO were discharging their duty overseeing this area of operation.

General Points for all Warrants and Authorisations

This section is concerned with general points which apply to all warrants and authorisations.

Information in the Warrant

When I ask to see a particular warrant I have to be provided with the accompanying submission to fully understand what is involved and restrictions accepted. Key features are set out in the submission including necessity, proportionality, privacy considerations and why the action proposed is justified by the intelligence to be received and any restrictions. I have **recommended** that a warrant or authorisation instrument which is signed by a Secretary of State should state that any activity taking place was subject to and in accordance with terms constrained in the submission. GCHQ have already adopted this course and I strongly encourage SIS and MI5 to do so as well.

RIPA PART II Authorisations – Date of Effect

The code of practice for Directed Surveillance states that the authorisation begins on the day "when the authorisation was granted" (para 5.10). RIPA says: "beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect ..." RIPA 43(3)(c).

The code of practice for Covert Human Intelligence Sources states that the authorisation begins on "the day on which it took effect ..." (para 5.14). RIPA 43(3)(b) states "beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect.."

The legislation allows an authorisation to be made on the day, to take effect at a later date. The codes appear not to. It must be more practical to be able to sign a RIPA Part II form on the day to take effect on a later date when the operation begins. Clearly the date of authorisation should be "shortly" before the date when the operation begins. In my view the codes of practice need to be changed but I have **recommended** that because of the language of the codes the only safe course is to calculate the time from the day of signing i.e. date of authorisation.

Cancelling Warrants

ISA s6(3) and RIPA s45 requires that warrants must be cancelled if they are no longer necessary. I noted that this does not happen as a matter of routine and sometimes departments had no effective system in place to check when warrants were no longer required. Instead the warrant is allowed to lapse. I **recommended** that warrantry units and the agencies establish a mechanism to check for warrants no longer in use and to cancel the warrant when the purpose for which it was obtained has been completed so that the information is available to the appropriate oversight body.

8. CONCLUSIONS AND RECOMMENDATIONS

My overall conclusion is that authorisations and warrants are only granted on the basis of a proper case being made for necessity and a proper consideration of proportionality all set out in detailed submissions. It is evident that the agencies, MOD and Ministers together with their officials all take compliance very seriously and put a great deal of effort into ensuring that each interference with privacy is fully justified. I have however made clear that in their submissions it is important where collateral intrusion into privacy is recognised, the mitigating steps should be clearly spelt out.

I have suggested that because submissions contain the important conditions on which warrants and authorisations are granted that there should be an express reference to those terms on the face of the warrant or authorisation. This suggestion has been taken up by GCHQ and I hope that others will follow suit.

So far as DSAs and CHIS authorisations are concerned there are differences in the language between the codes of practice and the legislation. The codes appear to provide that time runs from the date of signature. The legislation would appear to allow for signature and the period to run from a specified date thereafter. The latter allows for sensible planning. The former means that if signing takes place the date prior to the day of the expiry of a previous authorisation, there is a danger of a miscalculation. I have advised that the only safe course it to follow the codes of practice, but I suggest that the language of the codes of practice is brought into line with the statute.

Recommendations I have made previously relating to thematic warrants have largely been accepted and implemented, however I will continue to keep a close eye on the terms of these warrants to ensure they are only being used when absolutely necessary.

I have made several references in this report to inadequacies in the way SIS record their decisions. It is right to record that there have been improvements particularly in relation to the application of the Consolidated Guidance. I have also been shown drafts of forms which if implemented will further improve matters.

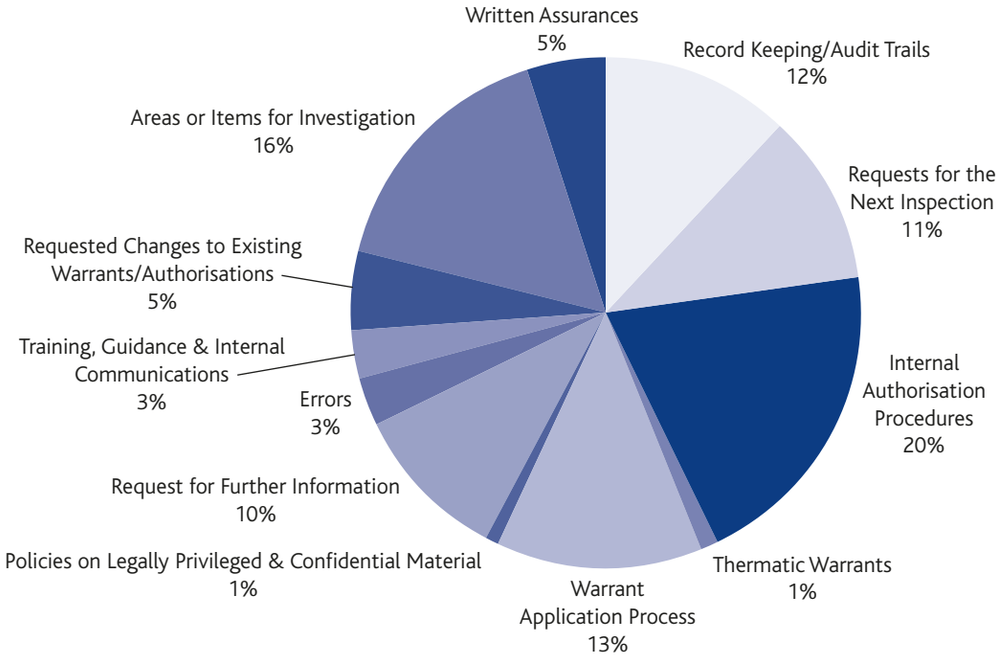
I have drawn attention to "errors". It is right to emphasise that I have not found any evidence of deliberate disregard of the requirements to obtain proper authorisation, and the "errors" found are not more than would be expected in any large organisations required to act at speed and under pressure.

In relation to the agencies use of bulk personal datasets I am satisfied that the agencies have very good systems in place to ensure that no datasets are acquired, exploited or retained where it is not necessary and proportionate to do so, as well as effective protective monitoring systems in place to prevent their misuse.

With regards to the application of the Consolidated Guidance, I am satisfied that the agencies and the MOD take all steps they can to make their personnel aware of the terms of the guidance. It is clear to me that extremely careful consideration is given to its application in increasingly complex situations. In some instances the Guidance may not expressly apply and I am reassured that in such situations the agencies and the MOD follow it and its spirit so far as they practically can. As I mentioned earlier the IP Bill does not currently make provision for the oversight of the Consolidated Guidance. There is a provision for the Prime Minister to issue directions as heretofore and I hope that such a direction will be issued to ensure continued oversight of this very complex area when the new Bill comes into effect.

Throughout the year I have made a total of 143 recommendations to the Security Service, SIS, GCHQ, MOD, Home Office, Foreign Office and the Northern Ireland Office. I have touched on the key recommendations in the relevant sections of my report; the chart below shows a summary of the categories under which all of the recommendations fall.

Recommendations by Category



APPENDIX

Expenditure

My office's total expenditure for the financial year 2015/16 was £408,399.24. The table below provides a breakdown of this expenditure. This expenditure includes costs of the report into 'Concerns Raised by the Intelligence and Security Committee of Parliament about the Government's Responsibilities in Relation to Counter-Terrorism Units Overseas' incurred in the financial year 2015/16.

Description	Total (£)
Staff costs	320,729.42
Travel & Subsistence	17,706.89
Legal fees	49,345.60
IT	17,568.41
Office Costs (including stationery and printing costs)	3,048.92
Total	**408,399.24**

ISBN 978-1-4741-3553-5

Home Office

Rt Hon Ben Wallace MP
Minister of State for Security and Economic Crime

2 Marsham Street
London SW1P 4DF
www.gov.uk/home-office

Rt Hon Dominic Grieve QC MP
Chair, Intelligence and Security Committee
35 Great Smith Street
London
SW1P 3BQ

3 December 2018

Dear Dominic,

GCHQ's planned use of the Investigatory Powers Act 2016 Bulk Equipment Interference Regime

I am writing to inform you that GCHQ's position on the authorisation of equipment interference (EI) operations has evolved since the Investigatory Powers Act received Royal Assent in 2016.

During passage of the then Investigatory Powers Bill through Parliament, HMG indicated that the majority of GCHQ's EI operations would be authorised under targeted or targeted thematic warrants. The reason for this was that the use of bulk EI warrants was anticipated to be limited to overseas "discovery" based EI operations. Under this approach, EI authorised under a bulk warrant would have been the exception and Lord Anderson of Ipswich K.B.E. Q.C. stated in his "Report of the Bulk Powers Review", published on 19 August 2016, that "Bulk EI is likely to be only sparingly used".

EI operations are a critical capability for our security and intelligence agencies in order to keep the country safe. Since the passage of the Bill, the communications environment has continued to evolve, particularly in terms of the range of hardware devices and software applications which need to be targeted. In addition, the deployment of less traditional devices, and usage of these technologies by

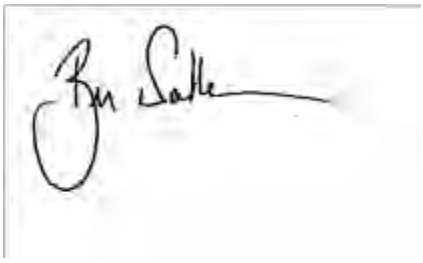
individuals of interest has advanced significantly. Following a review of current operational and technical realities, GCHQ have revisited the previous position and determined that it will be necessary to conduct a higher proportion of ongoing overseas focused operational activity using the bulk EI regime than was originally envisaged.

This interpretation is fully in line with the Act and the EI Code of Practice, as, for the reasons above, it is not always possible to adequately foresee the extent of all interferences with privacy to a sufficient degree to properly and fully assess necessity and proportionality at the point of issue of a warrant. The legislation contains the bulk warrant provisions specifically for these circumstances, and, following careful consideration of any warrant application through the Judicial double lock process, the additional controls and safeguards of the bulk regime will be employed. HMG has informed the Investigatory Powers Commissioner of these proposals, and he has proposed enhanced post facto safeguards for this activity.

Alternatively, where it is possible to ensure a greater degree of foreseeability of the relevant intrusion at the point of issue of the warrant, a targeted thematic warrant is likely to be more appropriate.

I can confirm you will receive a further letter on this matter from GCHQ which will provide additional detail at a higher classification. Should you have any observations or questions please let me know and we will work with GCHQ to address them.

I am copying this letter to the Investigatory Powers Commissioner, The Rt Hon Lord Justice Fulford. A copy of this letter will be placed in the House Library and published on the Government website.

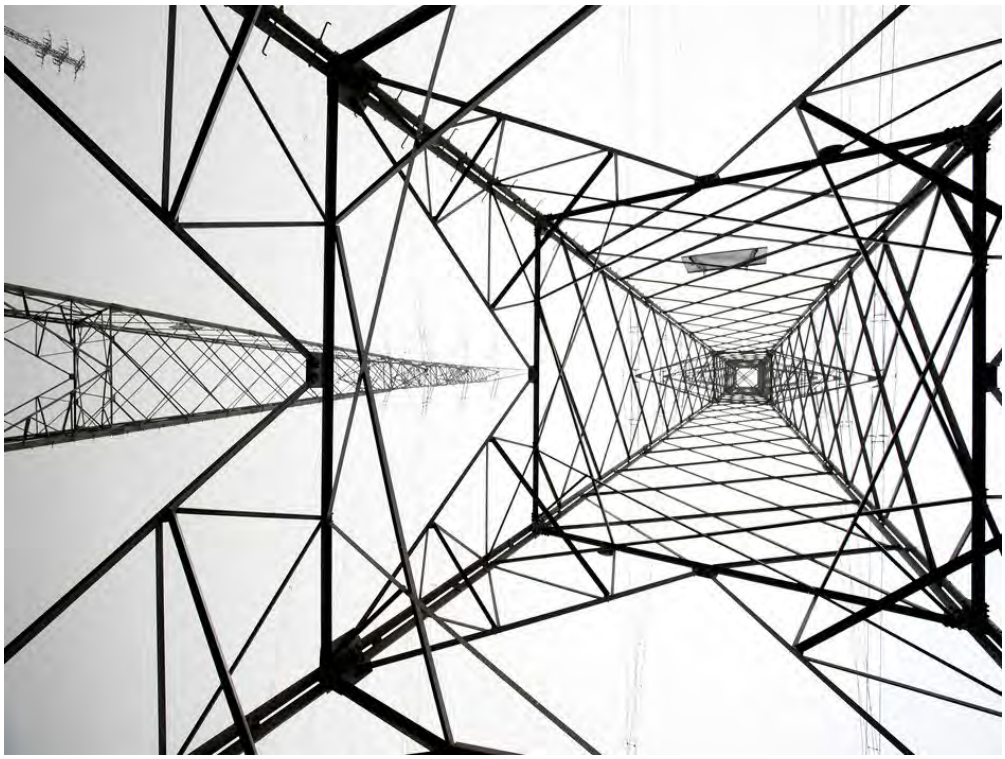


Rt Hon Ben Wallace MP

Minister of State for Security and Economic Crime

KIM ZETTER SECURITY 03.03.16 07:00 AM

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel. Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining re-entry. All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another, eventually taking about 30 substations offline. The attackers didn't stop there, however. They also struck two other power distribution centers at the same time, nearly doubling the number of substations taken offline and leaving more than 230,000 residents in the dark. And as if that weren't enough, they also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.

A Brilliant Plan

The hackers who struck the power centers in Ukraine—the first confirmed hack to take down a power grid—weren't opportunists who just happened upon the networks and launched an attack to test their abilities; according to new details from an extensive investigation into the hack, they were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance.

"It was brilliant," says Robert M. Lee, who assisted in the investigation. Lee is a former cyber warfare operations officer for the US Air Force and is co-founder of Dragos Security, a critical infrastructure security company. "In terms of sophistication, most people always [focus on the] malware [that's used in an attack]," he says. "To me what makes sophistication is logistics and planning and operations and ... what's going on during the length of it. And this was highly sophisticated."

Ukraine was quick to point the finger at Russia for the assault. Lee shies away from attributing it to any actor but says there are clear delineations between the various phases of the operation that suggest different levels of actors worked on different parts of the assault. This raises the possibility that the attack might have involved collaboration between completely different parties—possibly cybercriminals and nation-state actors.

“This had to be a well-funded, well-trained team. ... [B]ut it didn’t have to be a nation-state,” he says. It could have started out with cybercriminals getting initial access to the

network, then handing it off to nation-state attackers who did the rest.

Regardless, the successful assault holds many lessons for power generation plants and distribution centers here in the US, experts say; the control systems in Ukraine were surprisingly more secure than some in the US, since they were well-segmented from the control center business networks with robust firewalls. But in the end they still weren't secure enough—workers logging remotely into the SCADA network, the Supervisory Control and Data Acquisition network that controlled the grid, weren't required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers.

The power wasn't out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers are still not fully operational, according to a recent US report. Ukrainian and US computer security experts involved in the investigation say the attackers overwrote firmware on critical devices at 16 of the substations, leaving them unresponsive to any remote commands from operators. The power is on, but workers still have to control the breakers manually.

That's actually a better outcome than what might occur in the US, experts say, since many power grid control systems here don't have manual backup functionality, which means that if attackers were to sabotage automated systems here, it could be much harder for workers to restore power.

Timeline of the Attack

Multiple agencies in the US helped the Ukrainians in their investigation of the attack, including the FBI and DHS. Among computer security experts who consulted on the wider investigation were Lee and Michael J. Assante, both of whom teach computer security at the SANS Institute in Washington DC and plan to release a report about their analysis today. They say investigators were pleasantly surprised to discover that the Ukrainian power distribution companies had a vast collection of firewall and system logs that helped them reconstruct events—an uncommon bonanza for any corporate network, but an even rarer find for critical infrastructure environments, which seldom have robust logging capabilities.

According to Lee and a Ukrainian security expert who assisted in the investigation, the attacks began last spring with a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. Ukraine has 24 regions, each divided into between 11

and 27 provinces, with a different power distribution company serving each region. The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3—variants of which have infected other systems in Europe and the US—infected their machines and opened a backdoor to the hackers. The method is notable because most intrusions these days exploit a coding mistake or vulnerability in a software program; but in this case the attackers exploited an intentional feature in the Microsoft Word program. Exploiting the macros feature is an old-school method from the 90's that attackers have recently revived in multiple attacks.

The initial intrusion got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid. The companies had wisely segregated those networks with a firewall, so the attackers were left with two options: either find vulnerabilities that would let them punch through the firewalls or find another way to get in. They chose the latter.

Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack.

First they reconfigured the uninterruptible power supply[1], or UPS, responsible for providing backup power to two of the control centers. It wasn't enough to plunge customers into the dark—when power went out for the wider region they wanted operators to be blind, too. It was an egregious and aggressive move, the sort that could be interpreted as a "giant fuck you" to the power companies, says Lee.

Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully. Then they wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations (the converters are used to process commands sent from the SCADA network to the substation control systems). Taking out the converters would prevent operators from sending remote commands to re-close breakers once a blackout occurred. "Operation-specific malicious firmware updates [in an industrial control setting] has *never* been done before," Lee says. "From an attack perspective, it was just so awesome. I mean really well done by them."

The same model of serial-to-Ethernet converters used in Ukraine are used in the US power-distribution grid.

Armed with the malicious firmware, the attackers were ready for their assault.

Sometime around 3:30 p.m. on December 23 they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured. Then they began to open breakers. But before they did, they launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. TDoS attacks are similar to DDoS attacks that send a flood of data to web servers. In this case, the center's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through. Lee notes that the move illustrates a high level of sophistication and planning on the part of the attackers. Cybercriminals and even some nation-state actors often fail to anticipate all contingencies. "What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they're covering all aspects of what could go wrong," he says.

The move certainly bought the attackers more time to complete their mission because by the time the operator whose machine was hijacked noticed what was happening, a number of substations had already been taken down. But if this *was* a political hack launched by Russia against Ukraine, the TDoS likely also had another goal Lee and Assante say: to stoke the ire of Ukrainian customers and weaken their trust in the Ukrainian power companies and government.

As the attackers opened up breakers and took a string of substations off the grid, they also overwrote the firmware on some of the substation serial-to-Ethernet converters, replacing legitimate firmware with their malicious firmware and rendering the converters thereafter inoperable and unrecoverable, unable to receive commands. "Once you ... rewrite the firmware, there's no going back from that [to aid recovery]. You have to be at that site and manually switch operations," Lee says. "Blowing [these] gateways with firmware modifications means they can't recover until they get new devices and integrate them."

After they had completed all of this, they then used a piece of malware called KillDisk to wipe files from operator stations to render them inoperable as well. KillDisk wipes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot.

Some of the KillDisk components had to be set off manually, but Lee says that in two cases the attackers used a logic bomb that launched KillDisk automatically about 90 minutes into the attack. This would have been around 5 p.m., the same time that Prykarpattyaoblenergo posted a note to its web site acknowledging for the first time what customers already knew—that power was out in certain regions—and reassuring them that it was working feverishly to figure out the source of the problem. Half an hour later, after KillDisk would have completed its dirty deed and left power operators with little doubt about what caused the widespread blackout, the company then posted a second note to customers saying the cause of the outage was hackers.

Was Russia the Cause?

Ukraine's intelligence community has said with utter certainty that Russia is behind the attack, though it has offered no proof to support the claim. But given political tensions between the two nations it's not a far-fetched scenario. Relations have been strained between Russia and Ukraine ever since Russia annexed Crimea in 2014 and Crimean authorities began nationalizing Ukrainian-owned energy companies there, angering Ukrainian owners. Then, right before the December blackout in Ukraine occurred, pro-Ukrainian activists physically attacked substations feeding power to Crimea, leaving two million Crimean residents without power in the region that Russia had annexed, as well as a Russian naval base. Speculation has been rampant that the subsequent blackouts in Ukraine were retaliation for the attack on the Crimean substations.

But the attackers who targeted the Ukrainian power companies had begun their operation at least six months before the Crimean substations were attacked. So, although the attack in Crimea may have been a catalyst for the subsequent attack on the Ukrainian power companies, it's clear that it wasn't the original motivation, Lee says. Lee says the forensic evidence suggests in fact that the attackers may not have planned to take out the power in Ukraine when they did, but rushed their plans after the attack in Crimea.

"Looking at the data, it looks like they would have benefited and been able to do more had they been planning and gathering intelligence longer," he says. "So it looks like they may have rushed the campaign."

He speculates that if Russia is responsible for the attack, the impetus may have been something completely different. Recently, for example, the Ukrainian parliament has been considering a bill to nationalize privately owned power companies in Ukraine.

Some of those companies are owned by a powerful Russian oligarch who has close ties to Putin. Lee says it's possible the attack on the Ukrainian power companies was a message to Ukrainian authorities not to pursue nationalization.

That analysis is supported by another facet of the attack: The fact that the hackers could have done much more damage than they did do if only they had decided to physically destroy substation equipment as well, making it much harder to restore power after the blackout. The US government demonstrated an attack in 2007 that showed how hackers could physically destroy a power generator simply by remotely sending 21 lines of malicious code.

Lee says everything about the Ukraine power grid attack suggests it was primarily designed to send a message. "'We want to be seen, and we want to send you a message,'" is how he interprets it. "This is very mafioso in terms of like, oh, you think you can take away the power [in Crimea]? Well I can take away the power from you."

Whatever the intent of the blackout, it was a first-of-its-kind attack that set an ominous precedent for the safety and security of power grids everywhere. The operator at Prykarpattyaoblenergo could not have known what that little flicker of his mouse cursor portended that day. But now the people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be.

[1]*Correction 3/03/16 8:17 a.m. ET: UPS here stands for uninterruptible power supply, not universal power supply.*

ADVERTISEMENT

MOTHERBOARD
TECH BY VICE

GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets

The news comes after the FBI and Homeland Security warned hackers had targeted US energy firms too.

By **Joseph Cox**

Jul 17 2017, 8:59pm



IMAGE: SHUTTERSTOCK/CHETAN BISARIYA

A UK cybersecurity authority has issued a warning about hackers targeting the country's energy sector, and says that some industrial control system organizations are likely to have been successfully compromised, according to a copy of the document obtained by Motherboard.

The warning comes **at the same time as an anonymously-sourced report from *The Times*** stating that suspected Russian military hackers sent emails designed to trick engineers at an Irish energy organization. At the end of June, **the US government warned businesses** of **hackers targeting nuclear** and energy firms as well.

ADVERTISEMENT



The document was produced by the National Cyber Security Centre (NCSC), part of the UK's intelligence agency GCHQ.

"The NCSC is aware of connections from multiple UK IP addresses to infrastructure associated with advanced state-sponsored hostile threat actors, who are known to target the energy and manufacturing sectors," a section of the warning reads. An industry source provided the report to Motherboard. Motherboard granted the source anonymity to provide information on sensitive investigations.

> **NCSC believes that due to the use of wide-spread targeting by the attacker, a number of Industrial Control System engineering and services organisations are likely to have been compromised**

The activity is also targeting other sectors, with a focus on engineering, industrial control, and water sector companies. This recent wave of activity started around June 8, according to the report.

The document adds that it is likely hackers have managed to break into at least some of the targets' systems.

"NCSC believes that due to the use of wide-spread targeting by the attacker, a number of Industrial Control System engineering and services organisations are likely to have been compromised," another section of the warning reads. The report says that these organizations are part of the supply chain for UK critical national infrastructure, and some are likely to have remote access to critical systems.

An NCSC spokesperson told Motherboard in an email, "We are aware of reports of malicious cyber activity targeting the energy sector around the globe. We are liaising with our counterparts to better understand the threat and continue to manage any risks to the UK."

Motherboard confirmed the authenticity of the document with two other sources who also requested anonymity.

The motivation behind these hacking attempts is unclear. As the report mentions, state-sponsored hackers have previously targeted the energy sector for espionage, or for preparation of conflict. The NCSC report obtained by Motherboard does not mention Russia or any of its intelligence agencies by name.

Specifically with the intrusions reported in the NCSC document, the infrastructure in organizations is connecting to a set of malicious IP addresses using SMB, a data transfer protocol, as well as HTTP. The report suggests that the hackers may be trying to capture victims' passwords, and provides a set of mitigations for victims, such as turning on multi-factor authentication for industrial systems.

The NCSC report points to another, separate, non-public report issued by the FBI and US Department of Homeland Security to US businesses last month, which said the same hackers were using spear phishing emails to deliver malware-laden Word documents. The hackers then stole their victims' credentials and attempted to map out their network drives, according to the US report also obtained by Motherboard. The NCSC document does not explicitly say whether spear phishing was used against

UK targets, though *The Times* report says Russian hackers sent emails designed to trick staff.

These UK intrusions appear to be part of a broader campaign across multiple countries and continents.

"Previous Russian intrusions focused on critical infrastructure have targeted the US and the West simultaneously. We have found evidence that this actor has targeted Turkey and Ireland and suspect that their activity is even broader," said John Hultquist, an analyst at cybersecurity firm FireEye who has not seen the NCSC report but is aware of the hacking campaign, in a Twitter direct message to Motherboard.

According to **a report in CyberScoop**, 18 US-based energy companies received phishing emails in the recent wave.

Robert M. Lee, founder and chief executive of Dragos, a company that focuses on the security of industrial control systems, told Motherboard in a Twitter message "Targeted intrusions into civilian infrastructure is only increasing and only becoming more worrisome." Lee has also not reviewed the NCSC report.

However, panic over these incidents would likely be premature. Lee pointed to a 2014 hacking campaign that targeted US and European infrastructure, but with specially tailored malware, rather than the other techniques in this case.

"Both are concerning but we are not to the point where tailored activity by the adversary is setting off alarm bells. At this point we must accept the threat is real but there is no real threat to safety," Lee added.

Update: This article has been updated to include comments from an NCSC spokesperson.

ADVERTISEMENT

The Guardian



This article is more than **2 years old**

NHS could have avoided WannaCry hack with 'basic IT security', says report

National Audit Office says NHS and Department of Health must 'get their act together' or suffer 'far worse' than chaos experienced in May

Alex Hern

Fri 27 Oct 2017 00.01 BST

The NHS could have avoided the crippling effects of the "relatively unsophisticated" WannaCry ransomware outbreak in May with "basic IT security", according to an independent investigation into the cyber-attack.

The National Audit Office (NAO) said that 19,500 medical appointments were cancelled, computers at 600 GP surgeries were locked and five hospitals had to divert ambulances elsewhere.

"The WannaCry cyber-attack had potentially serious implications for the NHS and its ability to provide care to patients," said Amyas Morse, the head of the NAO.

"It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice. There are more sophisticated cyber-threats out there than WannaCry so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks."

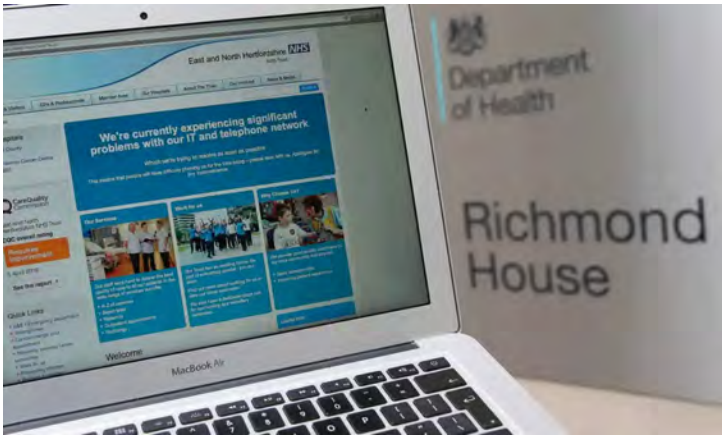
The NAO said the Department of Health was unable to cost the impact of the outbreak and the full extent of the damage may never be known. Overall, 81 NHS organisations in England were affected, a third of the total.

WannaCry was a type of malware known as a ransomware worm. It was capable of travelling from machine to machine directly, infecting new computers by automatically seeding itself across corporate networks. When it did manage to infect a new machine, it first silently worked in the background to infiltrate itself within the operating system, then restarted the computer and began the process of encrypting the hard drive, rendering it impossible to read without the encryption key. Victims were offered the chance to buy the key, for $300.

The worm nature of the virus, spreading automatically, means that some NHS regions were far worse hit than others, the report says. The North and Midlands & East regions contained 32 of the 37 NHS trusts affected, simply because they were the first regions to be hit, giving the virus most of the day to spread throughout their networks.

The damage would have been substantially worse had a young security researcher, Marcus Hutchins, not found and activated a “kill switch” that prevented future infections from locking devices. After the kill switch was enabled, infections continued to mount: a further 92 organisations appear to have been infected after that point, all of which owe their continued operation to luck.

Yet the attack could the been prevented by basic IT practices, the report says. As early as 2014, the Department of Health and the Cabinet had written to NHS trusts, saying it was essential they had “robust plans” to migrate away from old software. In March and April 2017, NHS Digital issued critical alerts warning organisations to fix the exact bug in their Windows computers that later enabled WannaCry to rapidly spread.



As early as 2014, the Department of Health and the Cabinet had written to NHS trusts, saying it was essential they had ‘robust plans’ to migrate away from old software. Photograph: Daniel Leal-Olivas/AFP/Getty Images

Before the attack, NHS Digital carried out an “on-site cybersecurity assessment” at 88 out of the 236 health trusts in England. None passed, but the agency had no powers to make them “take remedial action even if it has concerns about the vulnerability of an organisation”, the report says.

Dan Taylor, NHS Digital’s Head of Security, said WannaCry had been “an international attack on an unprecedented scale” and the NHS had “responded admirably to the situation”.

He added: “Doctors, nurses and professionals from all areas pulled together and worked incredibly hard to keep frontline services for patients running and to get everything back to

normal as swiftly as possible."

Meg Hillier, the chairwoman of the public accounts committee, said: "The NHS could have fended off this attack if it had taken simple steps to protect its computers and medical equipment. Instead, patients and NHS staff suffered widespread disruption, with thousands of appointments and operations cancelled.

"The NHS and the department need to get serious about cybersecurity or the next incident could be far worse."

The WannaCry ransomware managed to spread to more than 150 countries in less than a day, using a computer exploit discovered by the NSA and leaked by a suspected Russian hacking group called The Shadow Brokers to bounce from machine to machine. When it was installed on a computer, it proceeded to encrypt the hard drive, stopping it from being used and preventing the recovery of any data.

The software demanded a ransom to be paid in the cryptocurrency bitcoin worth $300 for the key to unlock the drive. More than £100,000 was eventually paid to the hackers, who withdrew the funds in August.

Since WannaCry, two other major ransomware attacks have been recorded: NotPetya, which began in Ukraine in July and brought down businesses including Maersk and Merck, and Bad Rabbit, which hit Eastern Europe earlier this week.

In June, Britain's National Cyber Security Centre completed an internal investigation into WannaCry and concluded that North Korean actors were behind the malware. While the NCSC did not release its findings, other security researchers came to the same conclusion based on elements in the code of the program that were similar to known North Korean malware.

You've read 7 articles...

... in the last month. If you've enjoyed reading, we hope you will consider supporting our independent, investigative journalism today. More people around the world are reading and supporting The Guardian than ever before. And unlike many new organisations, we have chosen an approach that allows us to keep our journalism accessible to all, regardless of where they live or what they can afford. But we need your ongoing support to keep working as we do.

The Guardian will engage with the most critical issues of our time - from the escalating climate catastrophe to widespread inequality to the influence of big tech on our lives. At a time when factual information is a necessity, we believe that each of us, around the world, deserves access to accurate reporting with integrity at its heart.

Our editorial independence means we set our own agenda and voice our own opinions. Guardian journalism is free from commercial and political bias and not influenced by billionaire owners or shareholders. This means we can give a voice to those less heard, explore where others turn away, and rigorously challenge those in power.

We need your support to keep delivering quality journalism, to maintain our openness and to protect our precious independence. Every reader contribution, big or small, is so valuable.
Support The Guardian from as little as £1 - and it only takes a minute. Thank you.

FREEDOMS



Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Volume II: field perspectives and legal update

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

This report addresses matters related to the respect for private and family life (Article 7), the protection of personal data (Article 8) and the right to an effective remedy and a fair trial (Article 47) falling under Titles II 'Freedoms' and VI 'Justice' of the Charter of Fundamental Rights of the European Union.

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Photo (cover & inside): © Shutterstock

More information on the European Union is available on the internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2017

FRA – print:	ISBN 978-92-9491-766-9	doi:10.2811/15232	TK-04-17-696-EN-C
FRA – web:	ISBN 978-92-9491-765-2	doi:10.2811/792946	TK-04-17-696-EN-N

© European Union Agency for Fundamental Rights, 2017

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Union Agency for Fundamental Rights copyright, permission must be sought directly from the copyright holders.

Printed by Imprimerie Centrale in Luxembourg

Neither the European Union Agency for Fundamental Rights nor any person acting on behalf of the European Union Agency for Fundamental Rights is responsible for the use that might be made of the following information.

Printed on process chlorine-free recycled paper (PCF)

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Volume II: field perspectives and legal update

Foreword

Intelligence services perform vital work, and the growing threats of terrorism, cyber-attacks and sophisticated criminal networks have rendered more urgent their efforts to protect our security. Technological advancements have also made their work more complex, and the transnational nature of today's threats has made it ever more challenging.

But intelligence work to counter these threats, particularly large-scale surveillance, can also interfere with fundamental rights, especially privacy and data protection. As this report underscores, effective oversight and remedies can help minimise the risk of such interference.

The report is the second publication addressing a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including its oversight.

With technological advances constantly introducing both new threats and new ways to fight those threats, legislators have been kept busy. Many of the legislative changes enacted since 2015 have increased transparency. But legal frameworks remain diverse and, according to some interviewees, too complex and imprecise. Moreover, while safeguards have in some cases been strengthened, room for improvement remains – particularly in the context of international intelligence cooperation. Similarly, remedies are available where individuals' rights have been infringed, but remain inherently limited.

Clarifying the applicable legal requirements, introducing solid safeguards and giving teeth to remedies would all help ensure that intelligence work is conducted in a rights-compliant manner. This, in turn, would reinforce the credibility of the information obtained by intelligence services – bolstering trust amongst the public, encouraging effective cooperation, and – ultimately – strengthening national security.

We are extremely grateful to the key partners and individual experts who took the time to participate in our interviews, providing invaluable real-life perspectives on the continuing effort to protect fundamental rights and national security.

Michael O'Flaherty
Director

Country codes

Country code	Country
AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	Netherlands
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SK	Slovakia
SI	Slovenia
UK	United Kingdom

Acronyms and abbreviations

Acronym/ abbreviation	Name	English translation
AIVD	Algemene Inlichtingen en Veiligheidsdienst	General Intelligence and Security Service (the Netherlands)
BND	Bundesnachrichtendienst	Federal Intelligence Service (Germany)
BNDG	Bundesnachrichtendienst Gesetz	Law on the Federal Intelligence Service (Germany)
CIVD	German Federal Intelligence Service	
CJEU	Court of Justice of the European Union	
CNCTR	Commission nationale de contrôle des services de renseignement	National Commission of Control of the Intelligence Techniques (France)
CNIL	Commission nationale de l'informatique et des libertés	French Data Protection Authority
COPASIR	Comitato parlamentare per la sicurezza della Repubblica	Parliamentary Committee for the Intelligence and Security Services and for State Secret Control (Italy)
CTIVD	De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten	Oversight Committee for the Intelligence and Security Services (the Netherlands)
DGSE	Direction générale de la sécurité extérieure	General Directorate for External Security (France)
DPA	Data Protection Authority	
ECHR	European Convention on Human Rights	
ECtHR	European Court of Human Rights	
FDN	French Data Network	
GCHQ	Government Communications Headquarters	
GDPR	General Data Protection Regulation	
GISS	General Intelligence and Security Service (Belgium)	
IOCCO	Interception of Communications Commissioners Office	
IPA	Investigatory Powers Act	
IPC	Investigatory Powers Commissioner	
IPT	Investigatory Powers Tribunal	
ISC	Internet Systems Consortium	
NCND	Neither confirm nor deny	
OCAM	Coordination Unit for Threat Analysis	
PKGr	Parlamentarisches Kontrollgremium	Parliamentary Control Panel (Germany)
PKGrG	Parlamentarisches Kontrollgremium Gesetz	Parliamentary Control Panel Act (Germany)
PNR	Passenger Name Records	
QPC	Question prioritaire de constitutionnalité	Priority preliminary ruling on the issue of constitutionality (France)
RIPA	Regulation of Investigatory Powers Act 2000	
SIGINT	Signals Intelligence	
SIN	Commission on Security and Integrity Protection	
SIS	Secret Intelligence Service	
SIUN	Statens Inspektion för försvarsunderrättelseverksamheten	The State Inspection for Defence Intelligence Operations (Sweden)
SSEUR	Signals Intelligence Seniors Europe	
TET	Tilsynet med Efterretningstjenesterne	Danish Intelligence Oversight Board

Contents

FOREWORD 3

EXECUTIVE SUMMARY 9

FRA OPINIONS 11

INTRODUCTION 17

PART I: THE LEGAL FRAMEWORK FOR INTELLIGENCE 25

1 Intelligence services in the EU-28: a diverse landscape 27
2 Surveillance measures in the digital age 29
3 Interference with the right to respect for private life 33
4 Surveillance "in accordance with the law" 37
5 Legality in case of international intelligence cooperation 49
6 Surveillance for a legitimate aim: need for 'national security' definition(s) 53

PART II: ACCOUNTABILITY 55

7 An imperative: control from within 59
8 Oversight framework of intelligence services 63
9 Features of oversight bodies 73
10 Stages of intelligence service oversight 93
11 Oversight of international intelligence cooperation 101

PART III: REMEDIES 109

12 The remedial route 111
13 Raising individuals' awareness 123
14 Remedial bodies' challenges: access to classified information and necessary expertise 129

GENERAL CONCLUSIONS 135

REFERENCES 137

INDEXES 145

ANNEX 1: DATA COLLECTION AND COVERAGE 153

ANNEX 2: OVERVIEW OF INTELLIGENCE SERVICES IN THE 28 EU MEMBER STATES 157

ANNEX 3: KEY FEATURES OF EXPERT OVERSIGHT BODIES' ANNUAL REPORTS 162

ANNEX 4: KEY FEATURES OF PARLIAMENTARY OVERSIGHT COMMITTEES' REPORTS 164

Figures and tables

Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015 20
Figure 2: Intelligence cycle in the Netherlands 31
Figure 3: Stages of control by ECtHR in the context of surveillance 33
Figure 4: Different understandings of 'interference' (EU and US) 35
Figure 5: Intelligence services' accountability scheme 65
Figure 6: Parliamentary oversight of intelligence services in EU Member States 66
Figure 7: DPAs' powers over national intelligence services, by Member State 81
Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State 82
Figure 9: Implementing effective remedies: challenges and solutions 114
Figure 10: DPAs' remedial competences over intelligence services 117

Table 1: Oversight framework: main actors and scope of control 64
Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU 68
Table 3: Effective oversight: legal standards and views of key actors 74
Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-28 95
Table 5: Approval/authorisation of general surveillance of communications in France, Germany, the Netherlands, Sweden and the United Kingdom 97
Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State 112
Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State 115

Executive summary

With terrorism, cyber-attacks and organised crime posing growing threats across the European Union, the work of intelligence services undoubtedly remains vital. Technological advancements have introduced both new threats and means of fighting those threats, meaning such work has also become increasingly complex. In addition, the globalisation of conflicts and the transnational nature of threats faced have made international cooperation between intelligence services both more common and indispensable – within and beyond the EU's borders.

Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communications and metadata to hacking and database mining. But – as the 2013 Snowden revelations underscored – these activities may also seriously interfere with diverse fundamental rights, particularly to privacy and data protection.

This report constitutes the second part of a research effort triggered by a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis (*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks)*. In addition, it presents findings from over 70 interviews with experts – conducted largely in 2016 – in seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom. The report focuses on large-scale technical collection of intelligence, referred to as general surveillance of communications.

Intelligence laws remain diverse and complex

Much has happened since 2015. New threats and new technology have triggered extensive reforms across several Member States, particularly France, Germany, the Netherlands and the United Kingdom, and Finland is in the midst of an overarching reform.

These intelligence law reforms have increased transparency. Nonetheless, the legal frameworks regulating intelligence work in the EU's 28 Member States remain both extremely diverse and complex. International human rights standards require defining the mandate and powers of intelligence services in legislation that is clear, foreseeable and accessible. But experts voiced concerns about a persisting lack of clarity as a major source of uncertainty.

According to both European Convention of Human Rights (ECHR) and EU law, the mere existence of legislation allowing for surveillance measures constitutes an interference with the right to private life, and European courts consider the collection of data by intelligence services to amount to an interference. Such interference needs to be justified to be human rights compliant.

Targeted surveillance – which applies to concrete targets based on some form of individualised suspicion – is regulated in some detail by almost all EU Member States. By contrast, only five Member States currently have detailed legislation on general surveillance of communications. Safeguards do limit the potential for abuse, and these have been strengthened in some Member States – though less so in case of foreign-focused surveillance. Similarly, safeguards are generally weaker – and less transparent – in the context of international intelligence cooperation, suggesting a need for more regulation of such cooperation.

Oversight bodies ensure some accountability, but room for improvement remains

Various entities oversee the work of intelligence services across the EU-28, including the judiciary, expert bodies, parliamentary committees and data protection authorities. In a field dominated by secrecy, such oversight is crucial: it helps ensure that intelligence services are held accountable for their actions, and encourages the development of effective internal safeguards within the services.

The judiciary and expert bodies are most commonly involved in overseeing surveillance measures. Specialised parliamentary committees generally focus on assessing governmental strategic policies – 21 Member States have set up such committees for this purpose. Data protection authorities have significant powers over intelligence services in seven Member States, but their powers are limited or non-existent in the rest of the EU – mainly due to an exception for national security matters enshrined in data protection law.

Almost all interviewees from oversight bodies maintained that they are able to resist external influence, but some lawyers, civil society, and academics questioned both their independence and their effectiveness. Interviewed experts emphasised that full access to all relevant data and information is key to effective oversight – as is the ability to benefit from such access. With oversight bodies largely staffed by legal specialists, the inability to do so sometimes boils down to limited technical capacities. Interviewees

acknowledged that these pose a problem – and that the sensitivity of the work can discourage individuals from seeking external expertise.

The power to issue binding decisions is also vital. While all EU Member States have at least one independent body in their oversight framework, some lack such decision-making powers. The importance of public scrutiny was also highlighted, with some interviewees deeming insufficiently informative the reports issued by oversight bodies. In addition, the respondents underlined the importance of countering the fragmentation of oversight through cooperation among the various actors involved in the oversight process, both nationally and internationally.

FRA's research revealed that oversight of international intelligence cooperation is less fully developed – 17 Member States do not require oversight of such activity, while others limited its scope. Some Member States have introduced safeguards specifically tailored to international intelligence sharing, but only requiring prior approval from the executive has been embraced in significant numbers (27 Member States).

Towards accessible and effective remedies

The need for secrecy in the intelligence field can affect both the effectiveness of oversight and individuals' abilities to seek remedies for violations. While the right to seek remedy is not absent in the context of secret surveillance, it is inherently limited. Interviewed experts indicated that individual remedial bodies receive about 10 to 20 complaints a year.

Non-judicial remedies are generally more accessible than judicial mechanisms because they are cheaper, faster and involve less strict procedural rules. Twenty-five Member States do allow individuals to lodge complaints regarding surveillance with such bodies. To be effective, remedial bodies also require certain powers – specifically, to access classified information and issue binding decisions. Expert bodies or data protection authorities have such powers in most Member States.

Nonetheless, lawyers, civil society representatives and academics consulted during FRA's research tended to question the effectiveness of existing remedies. They noted that few individuals are even aware that remedies are available. In addition, the rights to access information on individual files and to be notified about surveillance are not consistently implemented. Both of these can be curtailed based on various grounds linked to national security.

The lack of expertise in dealing with secrecy and with technical matters is also an issue, both with judicial and non-judicial actors. In the judicial context, Member States have found several ways to address this issue, including by developing alternative adversarial procedures to allow for the use of classified information; creating cooperation mechanisms, including with intelligence services, to tackle the lack of expertise; and establishing quasi-judicial bodies.

Such solutions underline that hurdles to obtaining effective remedies can be overcome. Similarly, establishing truly clear legal frameworks, developing appropriate safeguards, and ensuring potent oversight is feasible – and the best way to ensure that enhanced security measures made possible by surveillance fully comply with fundamental rights.

FRA opinions

Providing for a clear legal framework

Intelligence services help protect national security. To do this successfully, they often need to work in secrecy. However, international and European human rights standards require the mandate and powers of intelligence services to be clearly defined in a legal framework, and for this framework to establish safeguards against arbitrary action to counterbalance secrecy. The European Court of Human Rights (ECtHR) has held that national legal frameworks must be clear, accessible and foreseeable. It obliges Member States to enshrine minimum safeguards in law, such as specifying the nature of offences that may lead to interception orders and defining the categories of people who may be put under surveillance. FRA's fieldwork shows that surveillance legislation is considered complex and that a clearer legal framework with meaningful definitions is needed.

FRA opinion 1

EU Member States should have clear, specific and comprehensive intelligence laws. National legal frameworks should be as detailed as possible on intelligence services' mandates and powers, and on the surveillance measures they can use. Fundamental rights safeguards should feature prominently in intelligence laws, with privacy and data protection guarantees for collecting, retaining, disseminating and accessing data.

Ensuring broad consultation and openness during the legislative process

The preparation of intelligence legislation should involve an open debate among key stakeholders. During discussions on draft intelligence laws, governments should take the time to clarify the needs of intelligence services and to explain which fundamental rights guarantees the bill has established. FRA data show that most EU Member States have reformed their intelligence and counter-terrorism legislation in recent years. Some of these legislative processes unfolded during FRA's fieldwork. The interviewed experts emphasised the need for a broader inclusion of key actors and stakeholders in the development of intelligence legislation. In some Member States, online public consultations and lively parliamentary discussions are taking place instead of new legislation being fast-tracked. FRA's *Fundamental Rights Report 2017* underlined the need for such an approach.

FRA opinion 2

EU Member States should undertake broad public consultations with a full range of stakeholders, ensure transparency of the legislative process, and incorporate relevant international and European standards and safeguards when introducing reforms to their legislation on surveillance.

Providing independent intelligence oversight with sufficient powers and competences

Setting up a strong oversight mechanism is an essential part of an intelligence accountability system. The oversight framework should reflect the powers of the intelligence services. European Court of Human Rights case law provides that oversight bodies should be independent and have adequate powers and competences. FRA's research findings show that all EU Member States have at least one independent body in their oversight framework. However, the findings also identified limits to full independence, with some oversight bodies remaining strongly dependent on the executive: the law does not grant them binding decision-making powers, they have limited staff and budget, or their offices are located in government buildings.

FRA opinion 3

EU Member States should establish a robust oversight framework adequate to the powers and capacities that intelligence services have. The independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies' decisions are binding.

Bolstering oversight with sufficient technical expertise

Particularly in light of rapidly evolving technology in the digital area, technical expertise and capacity among oversight bodies is crucial. FRA's fieldwork indicates that limits on oversight bodies' IT expertise and their technical capacity to fully access intelligence data poses, and will continue to pose, a major challenge. Interviewed experts stated they sometimes need to rely on external expertise to complement their own legal expertise. FRA's legal research shows that some EU Member State laws explicitly require oversight bodies to have technical expertise.

FRA opinion 4

EU Member State laws should ensure that oversight bodies have staff with the required technical expertise to assess independently the intelligence services' often highly technical work.

Ensuring oversight bodies' openness to public scrutiny

The European Court of Human Rights has underlined that intelligence services and oversight bodies should be held accountable for their work. They should be transparent and effectively inform parliaments and the public about their activities. FRA's research shows that in some Member States, enhanced transparency is achieved while respecting necessary secrecy. Experts interviewed during FRA's fieldwork consider enhanced transparency to be particularly important. However, oversight bodies' approaches to transparency vary considerably across Member States, ranging from publishing regular reports to having websites or using social media.

FRA opinion 5

EU Member States should ensure that oversight bodies' mandates include public reporting to enhance transparency. The oversight bodies' reports should be in the public domain and contain detailed overviews of the oversight systems and related activities (e.g. authorisations of surveillance measures, on-going control measures, ex-post investigations and complaints handling).

Fostering continuity of oversight

The European Court of Human Rights has held that effective oversight requires 'continuous control' at every stage of the process. FRA's research findings show extremely diverse oversight structures across EU Member States. When different bodies are involved in the various steps of oversight – from approving a surveillance measure to the oversight of its use – possible gaps or overlaps can result. Such shortcomings undermine the adequacy of the safeguards. FRA's fieldwork highlights that institutional and informal cooperation between the oversight bodies within individual Member States is crucial.

FRA opinion 6

EU Member States should ensure that the oversight bodies' mandates complement each other, so that overall they provide continuous control and ensure proper safeguards. Such complementarity can be achieved with informal cooperation between oversight bodies or statutory means.

Enhancing safeguards for protected professions

The European Court of Human Rights has held that enhanced safeguards are needed to protect journalistic sources in the context of surveillance. This principle similarly applies to other professions which, due to overarching principles such as parliamentary privileges, independence of the judiciary and confidentiality in lawyer-client relations, also require greater protection. FRA's research shows that while diverse approaches exist, several EU Member States have laws stipulating enhanced authorisation and approval procedures for, as well as stricter controls on, the processing of data collected through surveillance of individuals belonging to protected professions.

FRA opinion 7

EU Member States should establish specific legal procedures to safeguard the professional privilege of groups such as members of parliament, members of the judiciary, lawyers and media professionals. Implementation of these procedures should be overseen by an independent body.

Ensuring efficient whistleblower protection

The European Court of Human Rights has held that whistleblowing by civil servants should be ensured. Whistlebowers can significantly contribute to a well-functioning accountability system. FRA's research revealed different whistleblowing practices across EU Member States. Interviewed experts expressed diverging views about whistleblower protection.

FRA opinion 8

EU Member States should ensure efficient protection of whistleblowers in the intelligence services. Such whistleblowers require a regime specifically tailored to their field of work.

Subjecting international intelligence cooperation to rules assessed by oversight bodies

FRA's comparative legal analysis shows that almost all Member States have laws on international intelligence cooperation. However, only a third require intelligence services to draft internal rules on processes and modalities for international cooperation, including safeguards on data sharing. When they exist, these rules are generally secret. Only a few Member States allow for external assessments of international intelligence cooperation agreements.

FRA opinion 9

EU Member States should define rules on how international intelligence sharing takes place. These rules should be subject to review by oversight bodies, which should assess whether the processes for transferring and receiving intelligence respect fundamental rights and include adequate safeguards.

Defining in law oversight bodies' competences over international intelligence cooperation

FRA's comparative legal analysis shows that most Member States' laws do not have clear provisions on whether oversight bodies can oversee international cooperation exchanges. Eight EU Member States establish oversight bodies' competences over international intelligence sharing – either with or without limitations; laws in three EU Member States exclude any form of independent oversight. In the remaining 17 Member States, legal frameworks are subject to interpretation to determine oversight bodies' competences over international intelligence sharing.

FRA opinion 10

EU Member States should ensure that legal frameworks regulating intelligence cooperation clearly define the extent of oversight bodies' competences in the area of intelligence services cooperation.

Exempting oversight bodies from the third-party rule

In international intelligence service cooperation, the third-party rule prevents a service from disclosing to a third party any data received from a partner without the source's consent. FRA's research underlines that the third-party rule protects sources and guarantees trust among intelligence services that cooperate. However, FRA's data show that oversight bodies are often considered as 'third parties' and therefore cannot assess data coming from international cooperation. In some Member States, oversight bodies are no longer considered as 'third parties' and so have full access to such data.

FRA opinion 11

Notwithstanding the third-party rule, EU Member States should consider granting oversight bodies full access to data transferred through international cooperation. This would extend oversight powers over all data available to and processed by intelligence services.

Providing for effective remedies before independent bodies with remedial powers

The European Court of Human Rights has held that an effective remedy is characterised by investigative and decisional powers granted to judicial and non-judicial bodies. In particular, the remedial body should have access to the premises of intelligence services and the data collected; be given the power to issue binding decisions; and inform complainants on the outcome of its investigations. The individual should be able to appeal the body's decision. FRA's data show that 22 EU Member States have at least one non-judicial body with remedial powers. In six Member States, though, these bodies lack the powers to issue binding decisions and access classified data.

FRA opinion 12

EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals' complaints related to surveillance.

Ensuring availability of non-judicial bodies with remedial powers

FRA's data show that non-judicial oversight mechanisms are more accessible to individuals than judicial remedies as they are simpler, cheaper and faster. FRA's comparative legal analysis shows that in the area of surveillance, individuals can lodge a complaint with a non-judicial body in 25 EU Member States. In ten Member States, one single non-judicial body has remedial powers, while in most Member States, individuals can lodge a complaint with two or more bodies with remedial powers.

FRA opinion 13

EU Member States should ensure that both judicial and non-judicial remedial bodies are accessible to individuals. Notably, Member States should identify what potential gaps prevent individuals from having their complaints effectively reviewed, and ensure that non-judicial expert bodies can complement the remedial landscape where needed.

Allowing for awareness of completed surveillance measures

FRA's comparative legal analysis shows that all EU Member States have a national security exception in their freedom of information laws. FRA's findings also show that all Member States limit either individuals' right to be notified or their right to access their own data based on the confidentiality of intelligence data and protection of national security or of on-going surveillance operations. Some Member States' laws provide for alternative ways to make individuals aware of surveillance measures and so enable them to seek an effective remedy.

FRA opinion 14

EU Member States should ensure that the legitimate aim and proportionality tests are conducted by intelligence services before limiting access to information based on national security. A competent authority should assess the confidentiality level. Alternatively, controls should be carried out by oversight bodies in the name of complainants when notification or disclosure are not possible.

Ensuring a high level of expertise among remedial bodies

Remedial bodies need to have a good understanding of surveillance techniques. FRA's fieldwork has identified ways to informally address shortcomings in technical expertise. Exchanges between remedial bodies, expert bodies, and intelligence services, while respecting each other's role and independence, have proven to deepen the technical understanding of reviewers and foster mutual trust. National practices of appointing specialised judges or establishing specialised courts or chambers to hear complaints about surveillance by intelligence services contribute to the development of judicial expertise in the area. Such systems can also facilitate different arrangements on judicial access to classified information.

FRA opinion 15

EU Member States should ensure that where judicial or non-judicial remedial bodies lack relevant expertise to effectively assess individuals' complaints, specific systems are established to address these gaps. Cooperation with expert oversight bodies, technical experts or members of the intelligence services can support effective remedial systems.

Supporting other human rights actors

FRA's fieldwork underlines that national human rights institutions, civil society organisations and, in some cases, ombudsperson institutions can play a crucial role in an enhanced intelligence services accountability system. However, FRA's fieldwork also shows that civil society organisations often lack adequate resources, with few able to offer comprehensive services to victims of alleged unlawful surveillance.

FRA opinion 16

EU Member States should broaden the operational space for national human rights bodies and institutions and civil society organisations, which can play a strong role as 'watchdogs' in the oversight framework.

Introduction

Intelligence services play a crucial role in protecting national security and helping law enforcement to uphold the rule of law. This is particularly true across the European Union (EU) today, with terrorism, cyber-attacks and organised crime groups located outside of the Union all posing serious threats to Member States.

EU Member States working both nationally and in partnership – and in cooperation with other states, such as the United States – are increasingly using digital intelligence methods to fight these threats. Intelligence services' capabilities include collection, interception and analysis of communications and metadata, hacking and computer network exploitation, as well as data mining of databases containing personal information. Such methods have implications for the fundamental rights of European citizens – such as privacy and freedom of expression – and their use must always be justified in a way that respect to those rights is ensured. Strong safeguards are necessary to ensure that they are used in accordance with law, and that interference with some rights to protect others, such as the right to life, only takes place when justified as necessary and proportionate, as allowed for by the ECHR.

The 2013 Snowden revelations showed that the United States (US) and some EU Member States were involved in what is colloquially referred to as 'mass surveillance' activities. This prompted discussions at several institutions, especially national parliaments. The inquiry committee of the German parliament published a particularly encompassing report in June 2017.[1] The EU also reacted strongly. At the time, the European Commission, the Council of the EU and the European Parliament all reported on the revelations. They expressed concern about mass surveillance programmes, sought clarification from US authorities, and worked on "rebuilding trust" in transatlantic relations.[2] The Snowden revelations also damaged the trust of EU citizens towards public authorities, intelligence services and technological companies providing communication software and hardware.

"The culture in the secret services is one of secrecy, and the present culture in society is to be as open as possible. The key element for the existence of the secret services today is what is called trust. Trust in society that they act between the borders of the law. For that you need to become more transparent than you were before."

(FRA interview with expert body, 2016)

(In)effectiveness of mass surveillance

"More generally, [...] it was found that massive eavesdropping measures, besides raising compatibility issues with fundamental rights and compliance with necessity and proportionality principles, as at various time delineated by European case law, prove to be inefficient.

The equation that a greater volume of available data and information would automatically result in better results in terms of security and prevention was not demonstrated."

Italy, COPASIR (2017), p. 12

"The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower."

Anderson, A. (2016), p. 1

On 12 March 2014, the EP adopted a resolution on the US National Security Agency (NSA) surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights, and transatlantic cooperation in Justice and Home Affairs.[3] The resolution drew on the in-depth inquiry that the EP tasked the Civil Liberties, Justice and Home Affairs Committee (LIBE) with conducting during the second half of 2013, shortly after the revelations on mass surveillance were published in the press.[4]

The wide-reaching resolution launched a "European Digital Habeas Corpus – Protecting fundamental rights in a digital age" focusing on eight key actions. The resolution also called on the EU Agency for Fundamental Rights (FRA) "to undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices".[5]

In 2015, FRA published the report *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (hereinafter the '2015 FRA report').[6] The 2015 FRA report presents the legal safeguards that the 28 EU Member States had for ensuring that surveillance measures do not violate fundamental rights. Since then, EU Member States have suffered serious terrorist attacks, triggering a state of emergency in France; have

1 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b).
2 FRA (2014a), p. 81 and following; FRA (2015a).
3 European Parliament (2014), hereafter: the resolution.
4 See FRA (2014a).
5 European Parliament (2014), paras. 132 and 35.
6 FRA (2015a).

faced migration pressures across the Mediterranean, prompting suspension of Schengen area free movement arrangements; and have been confronted with a rising tide of cyber-attacks, intensifying concern about this threat. Several Member States have introduced legislation to strengthen intelligence gathering in response to public pressure over these developments, while expanding the scope of their laws to explicitly cover more of their intelligence services' digital activity and improving oversight and other safeguards against abuse in light of the 2015 FRA report.

Methodology

The present report builds on the 2015 FRA report by providing a socio-legal analysis. Specifically, it:

- updates the 2015 FRA report's legal findings; and
- analyses findings from fieldwork interviews with key actors in the area, such as expert bodies, parliamentary committees, the judiciary, data protection authorities, national human rights institutions, as well as civil society organisations, academia, and media representatives.

FRA staff carried out the fieldwork in 2016, conducting over 70 interviews in seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom. The interviews addressed how intelligence legal frameworks are being implemented in practice and whether they comply with fundamental rights. For a thorough presentation of the methodology, see Annex 1.

The draft report was reviewed by a number of experts. They include Prof. Nico van Eijk, Director of the Institute for Information Law, University of Amsterdam; Prof. Ian Leigh, Durham Law School , Durham University; Prof. Sir David Omand, Visiting Professor, Department of War Studies, King's College, London; and Thorsten Wetzling, Project Director at the Stiftung Neue Verantwortung.

FRA expresses its gratitude for their valuable contributions. The opinions and conclusions outlined in the report do not necessarily represent the views of the organisations or individuals who helped to develop the report.

Five of the seven EU Member States – France, Germany, the Netherlands Sweden and the United Kingdom – were selected because they have detailed legislation on general surveillance of communications. They illustrate fundamental rights safeguards Member States introduce, particularly the oversight of intelligence services, when collecting large quantities of data. Italy and Belgium do not have as detailed legislation on the general surveillance of communications by civil intelligence services. However, the structures of their oversight systems are good examples of two different approaches to overseeing the surveillance measures at the services' disposal. In contrast to the 2015 FRA report, the present report also covers international cooperation between intelligence services.

This FRA project encountered several challenges. The intelligence field involves sensitive topics, resulting in secrecy, little knowledge about European intelligence services' data collection, and different organisational and professional cultures among the main actors, such as intelligence services and oversight bodies, within and across Member States. Recent reforms of intelligence legislation in many Member States have brought further changes to working practices; the comparative tried to capture the changes up to the time of publication. Moreover, the number of experts in the area is limited – in some cases concentrated on a single person (or a few) who represents a specific function in the system. This made access to potential respondents more difficult and made necessary intensive preparatory work in building up trustful and cooperative relationships in each Member State and institution. Finally, in some instances, Member States' interpretation of the applicability of EU law and FRA's mandate posed additional challenges to accessing national expertise – in particular that of active intelligence service representatives, who did not take part in any of the interviews.

Scope of analysis

This report, together with the 2015 FRA report, constitutes the agency's response to the EP's request to study the impact of 'surveillance' on fundamental rights. However, given the context in which the resolution was drafted, so-called 'mass surveillance' is the main focus of the parliament's work. During the data collection phase for FRA's first report in 2014, FRA used the parliament's definition of 'mass surveillance' to delineate the research's scope.

> The EP resolution refers to: *"[F]ar-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner."* European Parliament (2014), para. 1

The European Parliament's definition – highlighted as an excerpt – encompasses two essential aspects: first, a reference to technical collection of intelligence, and second, emphasis on untargeted collection. The distinction between targeted and untargeted collection remains disputed when it comes to techniques enabling general surveillance of communications.

> *"Even though the inquiry committee's investigations have neither found systematic fundamental rights violations nor evidence of 'mass surveillance' or uncontrolled data accumulation or transmission by the BND, the opposition has continually fuelled such fears: with incorrect claims on the consequences of the law and unfounded equating of the BND and the NSA. "*
>
> *Germany, Federal Parliament* (Deutscher Bundestag) *(2017b), p. 1316*

Formulating a precise definition also constituted a methodological challenge for FRA. The methods used by intelligence services have evolved since 2015, and so has the corresponding terminology. This report uses the term 'general surveillance of communications' to refer to what the 2015 FRA report called 'signals intelligence' (SIGINT), since the latter is no longer fully accurate in light of the range of methods currently used by intelligence services.

This report focuses on the work of intelligence services. It does not address the work of law enforcement authorities. Nor does it cover the obligations of commercial entities which are, by law, required to provide intelligence services with raw data – obligations which amount to general surveillance of communications – and are otherwise involved in surveillance programmes. The private sector's role in surveillance requires a separate study. Some commercial entities – especially telecommunication service providers – produce regular 'transparency reports', which outline the requests they receive from public authorities to access data related to users of their commercial services.[7]

> *"A right is only worth as much as its delimitations and enforcement mechanisms allow it to be. This is crucial in the area of governmental surveillance, since we need safeguards without borders as well as remedies across borders."*
>
> *UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci, p. 12*

Given that the secret monitoring of communications – as the ECtHR refers to such activity[8] – interferes with the fundamental right to privacy, this report focuses on analysing the safeguards included in EU Member States' legal frameworks, and on the different ways states safeguard fundamental rights in practice.

Fundamental rights safeguards

Given the scope of the EP's request, the report focuses on privacy and data protection. Other fundamental rights – such as freedom of expression, freedom of religion and freedom of association – are also affected but are not the primary object of the analysis.[9] A fundamental right must be properly safeguarded to be effectively exercised. This report also analyses, as per the EP's request, effective remedies that individuals can pursue to enforce their rights.

The 2015 FRA report referred to existing international and European standards applicable to surveillance.[10] While updating the analysis to take into account the evolution of United Nations (UN) and European standards, this report refers to the *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* (UN Good practices),[11] of which the Human Rights Council took note in 2012.[12] This set of soft law standards remains, to this date, the only encompassing document in the field at universal level.[13]

The ECtHR has well-developed case law on Article 8 of the ECHR (right to respect for private and family life) – including its procedural aspects[14] – and Article 13 of the

7 For an overview of telecommunications, internet and mobile companies' transparency reports, see Ranking Digital Rights (2017).

8 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 78.

9 See European Parliament (2014), para. T. See also FRA (2015a), p. 9, United Nations (UN) General Assembly (GA) (2016); UN Human Rights Council (2017); UN, Human Rights Council (2016), UN, Human Rights Council (2017), Report of the Special Rapporteur David Kaye; UN, Human Rights council (2017), Report of the Special Rapporteur Joe Cannataci; UN, Human Rights Council (2017), Report of the Special Rapporteur Ben Emmerson; the Organization for Security and Co-operation in Europe (OSCE) (2015); ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, para. 88, in which the ECtHR acknowledges that the surveillance methods interfered with the applicant's freedom of expression; Council of Europe Commissioner for Human Rights (2015); Raab, C. *et al.* (2015); Mills, A. and Sarikakis, K. (2017).

10 FRA (2015a), p. 9.

11 UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin.

12 UN, Human Rights Council (2012), Resolution on the protection of human rights and fundamental freedoms while countering terrorism, 23 March 2012.

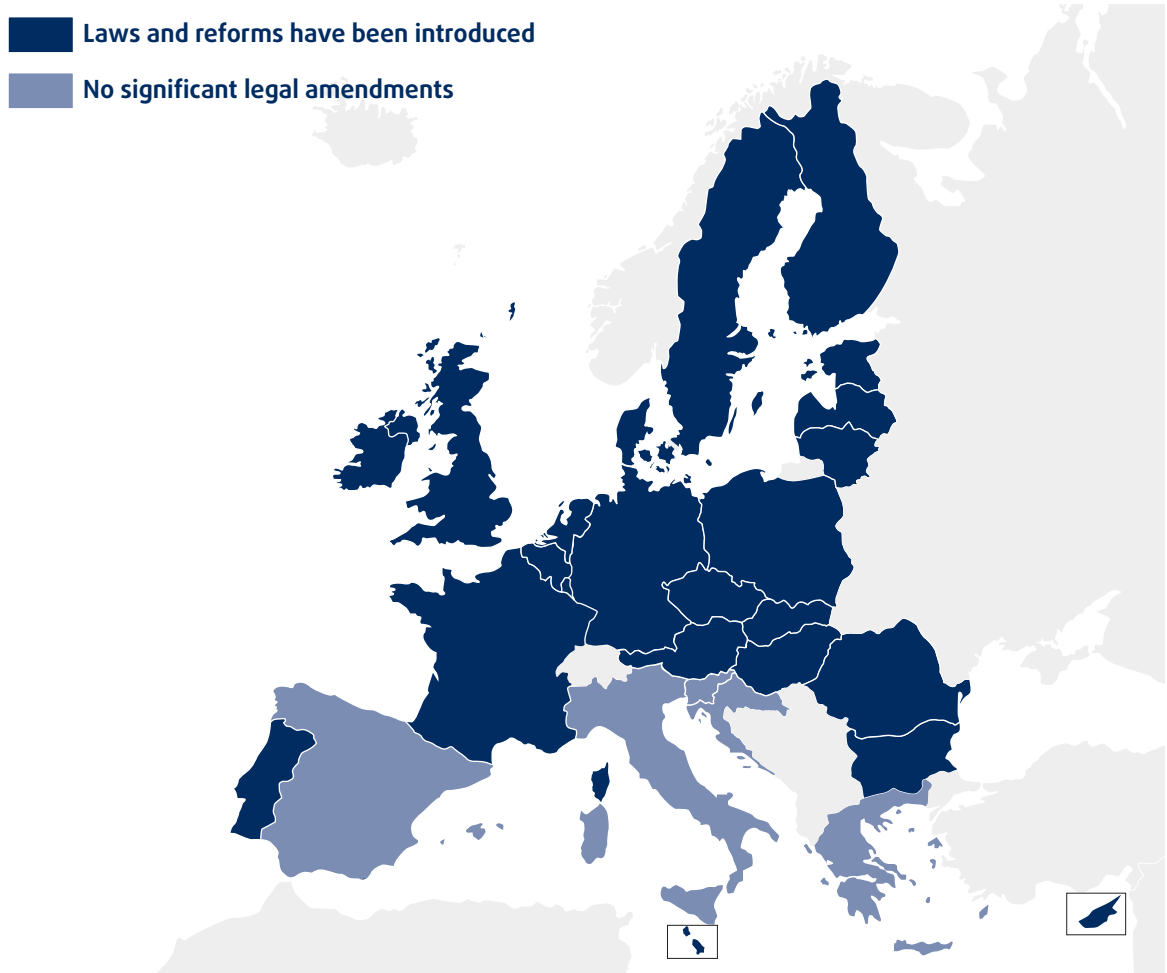
13 See UN, GA (2014a); UN, GA (2016c); UN, Human Rights Council (2009), Report of the Special Rapporteur Martin Scheinin; UN, Office of the High Commissioner for Human Rights (OHCHR) (2014); UN, Human Rights Council (2014), Report of the Special Rapporteur Ben Emmerson; UN, Human Rights Committee (2014); UN, Human Rights Committee (2015); UN, Human Rights Council (2016), Report of the Special Rapporteur Joe Cannataci; UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci.

14 ECtHR, *M.N. and Others v. San Marino*, No. 28005/12, 7 July 2015, para. 83.

ECHR (right to an effective remedy).[15] Nonetheless, cases on general surveillance of communications still need to be adjudicated.[16] Since publication of the 2015 FRA report, the ECtHR handed down a seminal judgment in *Roman Zakharov v. Russia*.[17] In this judgment, the court's Grand Chamber summarised and clarified past case law, while finding that the Russian legal framework was not compatible with human rights standards.

As stated in the 2015 FRA report, the ECtHR's human rights standards – which should be considered minimum standards – have served as a benchmark for Member States' legislative reforms. Figure 1 presents an overview of reforms of legal frameworks on surveillance that have taken place in the EU-28 since the 2015 FRA report. In light of heightened security pressures, an overwhelming majority of EU Member States have reformed or are in the process of reforming their legal frameworks.

Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015



Source: FRA, 2017

15 For a discussion of the ECtHR case law, see Council of Europe (2016), pp. 55-93. See also von Bernstorff, J. and Asche, J., Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 79 and following.

16 See the pending cases: ECtHR, *Centrum För Rättvisa v. Sweden*, No. 35252/08; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, No. 58170/13; ECtHR, *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, No. 62322/14; ECtHR, *10 Human Rights Organisations and Others v. the United Kingdom*, No. 24960/15; ECtHR, *Association confraternelle de la presse judiciaire v. France*, No. 49526/15.

17 ECtHR, *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015.

Surveillance activities and national security: applicability of EU Law

"National security remains the sole responsibility of each Member State: but subject to that, any UK legislation governing interception or communications data is likely to have to comply with the EU Charter because it would constitute a derogation from the EU directives in the field."

Anderson, D. (2015), p. 71

The 2015 FRA report gave an overview of privacy and personal data protection in primary and secondary EU law. It also referred to the 'national security' exemption, which limits the applicability of EU legal instruments.[18] The EU Data Protection Reform adopted in 2016[19] maintains this exemption in Article 2 (2) of the General Data Protection Regulation (GDPR) and in Article 2 (3) of the Data Protection Directive for Police and Criminal Justice Authorities, which excludes the "processing of personal data in the course of an activity which falls outside the scope of Union law" from its scope. This provision should be read in conjunction with Recital 14 in the *Data Protection Directive* for Police and Criminal Justice Authorities, which explains that Article 2 (3) means that "activities concerning national security, activities of agencies or units dealing with national security issues [...] should not be considered to be activities falling within the scope of this Directive."

The 2015 FRA report demonstrated that the debate regarding the limits of the 'national security' exemption, particularly in relation to counter-terrorism measures, involves both intelligence services and law enforcement authorities.[20] Since 2015, following several terrorist attacks in Europe, the EU has created a Security Union to counter terrorism efficiently.[21] In that context, the Council of the EU appointed a Commissioner for Security Union in 2016. The commissioner's task is to create an effective and sustainable Security Union, placing fundamental rights at the centre of the framework.[22]

Recent EU-level initiatives with national security relevance

Several initiatives have been introduced at EU level since 2015 as part of a broad effort to bolster Member States' national security. These include:

- **Policies/policy proposals**: European Agenda on Security (2015); European Commission's suggestion to open Counter Terrorism Group to 'interaction' with law enforcement authorities through Europol (2016)
- **Specialised bodies**: appointment of Commissioner for Security Union (2016); creation of European Parliament special committee to tackle deficiencies in the fight against terrorism (2017)
- **EU agencies**: EU Intelligence and Situation Centre (INTCEN); EU Satellite Centre (SatCen)
- **Legislation**: adoption of Passenger Names Record Directive 2016/681 (2016)

Source: FRA, 2017

The exchange of existing intelligence among Member States for counter-terrorism purposes and access to such data by law enforcement authorities are challenging issues for the Security Union. Data collected by a Member State's intelligence services fall under the exclusive competence of that Member State. The European Commission has stated that solutions to the lack of clarity in the relationship between the law enforcement community and intelligence community should be urgently identified. At present, exchanges of data among national intelligence services take place voluntarily and outside the EU's legal framework, through – for instance – the Club de Berne and the derived Counter Terrorism Group (CTG). The CTG is an intelligence-sharing forum that focuses on counter-terrorism intelligence and encompasses all EU Member States, as well as Norway and Switzerland. The Commission has suggested opening the CTG to 'interaction' with law enforcement authorities, through the existing Europol framework.[23] Meanwhile, in July 2017, the European Parliament created a special committee to tackle deficiencies in the fight against terrorism. The committee is tasked with assessing the extent of terrorist threats on European soil and

18 FRA (2015a), p. 10.

19 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119 (*General Data Protection Regulation, GDPR*); and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119 (*Data Protection Directive for Police and Criminal Justice Authorities*).

20 FRA (2015a), p. 10. For an analysis of the competence of the EU on national security and intelligence services, see also Sule, S. (2017), pp. . 16-20.

21 European Commission, Juncker, J.-C. (2016), 'Juncker after Brussels terror attacks: "We need a Security Union"', Joint Press Conference with French Prime Minister Manuel Valls, 24 March 2016.

22 King J. (2016), 'Introductory remarks by the Commissioner-designate Sir Julian King to the LIBE Committee', Press release, Strasbourg, 12 September 2016.

23 European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council, "Enhancing Security in a world of mobility; improved information exchange in the fight against terrorism and stronger external border", COM(2016)602, Brussels, 14 September 2016, p. 15.

examining the factors that led to recent terrorist attacks in Europe. The committee will look into various aspects, such as deficiencies in intelligence information sharing among Member States and the impact of such sharing on fundamental rights.[24]

At legislative level, the creation of the Security Union led to the adoption of the Passenger Name Records (PNR) Directive.[25] PNR data are collected by airlines from passengers during check-in and reservation procedures. Intelligence services can subsequently access PNR data collected by airlines and use them for intelligence purposes. The PNR Directive establishes at EU level a common legal framework for exchanging PNR data among Member States, as well as sharing PNR data with Europol. The PNR data may then be used for the fight against terrorism and serious crime under certain conditions set by the directive.

National security was also at issue in a 2016 Court of Justice of the European Union (CJEU) judgment. In joined cases *Tele2 Sverige* and *Home Secretary v. Watson*,[26] the CJEU found that requiring telecommunication companies to retain all electronic communications data, meaning data about telephone calls, emails and websites visited by their clients, was not in conformity with the *e-Privacy Directive*[27] and the EU Charter of Fundamental Rights, violating the right to respect for private life and protection of personal data. The court stated that, in the case of serious crime, Member States can impose a general obligation on providers of electronic telecommunications services to retain data only if deployed against specific targets. Retention measures must be necessary and proportionate regarding the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention. Furthermore, national authorities' access to the retained data must be conditional and meet certain data protection safeguards. The court explicitly distinguished cases where the data are retained to protect 'national security' from other types of 'serious crime'.[28] Where 'national security' is at stake, the court concluded that access may also be granted to data of persons other than the specific targets; however, as a safeguard, there must be objective evidence of these data's effective contribution to the fight against a specific 'national security' threat.

'National security' is also relevant to the transfer of personal data to a third country on the basis of a decision that the third country provides an adequate level of protection of personal data (adequacy decision). Under the GDPR, to assess the level of protection of personal data, the European Commission must take into account any relevant legislation concerning national security as well as the implementation of such legislation. In particular, the Commission looks at whether the third country guarantees effective and enforceable data subject rights, and effective and judicial redress for the data subjects whose personal data are being transferred.[29] The *EU-US Privacy Shield* is an example of such an adequacy decision. This decision allows for free flow of data for commercial purposes between the EU and the US.[30] The *EU-US Privacy Shield* was the result of the annulment of the *Safe Harbour* Adequacy Decision by the CJEU in *Schrems*.[31] The CJEU looked into personal data transfers to the US on the basis of the *Safe Harbour* Adequacy Decision and subsequent access to the data by national intelligence services for reasons of national security. The CJEU held that legislation must provide effective oversight and redress mechanisms. Failing to provide an effective remedy violates Article 47 of the Charter.

The 'national security' exemption thus cannot be seen as entirely excluding the applicability of EU law. Individuals' records of calls, text messages, e-mails and any other forms of electronic communication that are retained by their telecommunications providers and subsequently transferred to intelligence services for national security purposes could enjoy the standards of protection offered by the GDPR.

24 European Parliament (2017), European Parliament Decision of 6 July 2017 on setting up a special committee on terrorism, its responsibilities, numerical strength and term of office, P8_TA-PROV(2017) 0307, Strasbourg, 6 July 2017.

25 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016 (*PNR Directive*).

26 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016.

27 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002 (*Directive on privacy and electronic communications*).

28 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 119.

29 GDPR, Art. 45.

30 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L207, 1 August 2016.

31 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015.

As explained in the 2015 FRA report, if EU law is not applicable, Council of Europe conventions might be.[32] These include the ECHR and the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108),[33] and its 2001 Additional Protocol related to transborder data flows to non-parties to Convention 108 and the mandatory establishment of national data protection supervisory authorities.[34] Convention 108 is currently being amended to, on the one hand, better address challenges resulting from the use of new information and communication technologies and, on the other hand, to strengthen its implementation.[35] The reform maintains the general and technologically neutral nature of the convention's provisions; it does not impose or discriminate in favour of the use of a particular type of technology. At the same time, it aims to be coherent with other legal frameworks, such as the EU's. In line with the GDPR, the reformed Convention 108 will include an exception to the protection of personal data for the processing activities for national security.[36] However, such an exception must be provided for by law, respect the essence of fundamental rights and freedoms, and constitute a necessary and proportionate measure in a democratic society. The reformed Convention 108 will also require processing activities for national security purposes to be subject to independent and effective review and supervision. Convention 108 is of great importance to the EU legal order given that all EU Member States ratified it following a 1999 amendment, and that the EU could become a party thereto.[37]

Report structure

The report is structured as follows:

- **Part 1** provides an overview of intelligence services and surveillance laws in all EU Member States. Highlighted findings from fieldwork interviews conducted at national level in selected EU Member States offer insights into how experts view legal frameworks in terms of their compliance with human rights standards.

- **Part 2** presents existing statutory safeguards, focusing on oversight of intelligence services. Most fieldwork findings are presented in this part. While the 2015 FRA report treated oversight mechanisms according to the type of institution involved, this report presents oversight mechanisms according to their role in oversight.

- **Part 3** analyses the available remedies for an individual in cases of alleged unlawful surveillance. The fieldwork findings on the availability and effectiveness of remedial avenues provide empirical evidence.

The report's annexes present the research data collection methodology (Annex 1), the intelligence services in the EU-28 (Annex 2), and key features of expert oversight bodies' and parliamentary oversight committees' annual reports (Annex 3 and Annex 4).

32 FRA (2015a), p. 11.
33 Council of Europe, Convention for the protection of individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981 (*Convention 108*); CJEU, C-387/05, *European Commission v. Italian Republic*, 15 December 2009, para. 45.
34 Council of Europe, Convention 108, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001.
35 Council of Europe, Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (*Draft Modernised Convention 108*).
36 *Ibid*. Art. 9.
37 Council of Europe, Amendments to the Convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form.

PART I: THE LEGAL FRAMEWORK FOR INTELLIGENCE

KEY FINDINGS

Intelligence services' legal frameworks

- All EU Member States regulate by law the organisation of their intelligence services to comply with rule of law and human rights standards.
- The organisation of intelligence services varies significantly in the EU Member States. In some, two intelligence services carry out the work, while in others, five, six or more bodies may apply surveillance measures.
- International human rights standards require that intelligence services' mandate and powers be defined in legislation. The law has to be clear, foreseeable and accessible. Interviewees raised concerns relating to the complexity, as well as the lack of clarity and comprehensiveness, of some legal frameworks.
- The mere existence of a law allowing for surveillance measures – either targeted (with prior suspicion) or untargeted (without prior suspicion) – constitutes an interference with the fundamental rights to privacy and data protection.
- Under EU data protection law, the collection of data by intelligence services in itself constitutes an interference.
- Almost all EU Member States have a legal framework on targeted surveillance.
- France, Germany, the Netherlands, Sweden and the United Kingdom have detailed legislation on general surveillance of communications.
- Legal safeguards are more extensive for domestic surveillance than for foreign-focused surveillance.
- France, Germany, the Netherlands and the United Kingdom have reformed their legislation extensively since 2015. Several other Member States have started significant reforms. These aim, among others, to adapt to new technological developments and respond to new threats. Reforms increased transparency on surveillance powers granted to intelligence services. Interviewed experts acknowledged that legal reforms have brought improvements. However, interviewees believe that lack of clarity – and hence the need for quality legal rules governing the work of intelligence services – remains an issue.
- The concept of national security is not harmoniously defined across EU Member States. The scope of national security is rarely defined, and sometimes other, similar terms are used. Interviewed experts confirmed the need for clearer definitions of – among other terms – national security, including at EU level.

International cooperation frameworks

- Almost all EU Member States' laws allow for international intelligence cooperation. Only few detail in their legislation the procedures intelligence services must follow to establish international cooperation.
- Before establishing cooperation agreements, intelligence services from eight Member States have to follow confidential internal rules. A small number of EU Member States' laws prescribe a review of international cooperation agreements by independent bodies.

1 Intelligence services in the EU-28: a diverse landscape



UN good practices on mandate of intelligence services

Practice 1. Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.

Practice 5. Intelligence services are explicitly prohibited from undertaking any action that contravenes the constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The organisation of intelligence communities within the EU-28 has not fundamentally changed since publication of the 2015 FRA report, and FRA's subsequent fieldwork research did not address this topic. This chapter therefore reiterates some of the earlier report's main findings, and provides updates where warranted.

This report uses generic terminology, referring to 'intelligence services' for both 'intelligence services' that focus on foreign threats and 'security services' that focus on domestic threats.[38] The report focuses only on these entities' intelligence collection, analysis and dissemination functions, and not on any other activities involved in directly countering and disrupting threats.[39]

Annex 2 lists the existing intelligence services in the EU Member States. The table does not list Member State assessment and coordination bodies, such as the United Kingdom Joint Intelligence Committee; the Department for Security Information (DIS) in Italy; or the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*) in France, who is a part of the French intelligence community.[40]

By law, all EU Member States regulate the organisation of their country's intelligence services. Almost all have established at least two different bodies for conducting civil and military intelligence. In practice, the line separating the mandates of civil and military services is increasingly blurred;[41] many digital techniques – such as the geolocation of mobile devices – are used by both. Since this report is concerned with surveillance and not with wider national security intelligence gathering, it focuses – to the extent possible – on civil intelligence services. It does not cover the latter's work on military targets or the work of purely military intelligence services, given that they fall outside the scope of the EP resolution that sparked this research.

In some Member States, civil intelligence services are further divided into separate services – often with a domestic or foreign mandate. In some cases, these separate services have access to common platforms for technical and digital intelligence gathering operations. Moreover, some Member States grant the power to conduct intelligence operations to units that are not part of the civil intelligence services and that specialise

38 See Cousseran, J.-C. and Hayez, P. (2015), p. 41 and UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin, p. 4.
39 Born, H. and Wills, A. (eds.) 2012.

40 France, Defence Code (*Code de la Défense*), Art. D 1122-8-1. See also France, CNCTR (2016), p. 33 and France, DPR & CNCTR (2017), p. 13.
41 See Council of Europe (2016), p. 61; Cousseran, J.-C. and Hayez, P. (2015), p. 30.

in countering defined threats, such as organised crime, corruption or the fight against terrorism.

In France, for example, implementing regulations of the 2015 intelligence law established two intelligence 'circles'. The 'first circle' (*premier cercle*) is composed of six so-called specialised intelligence services (*services spécialisés de renseignement*), such as the *Direction générale de la sécurité interieure (DGSI)* and the *Direction générale de la sécurité exterieure (DGSE)*.[42] The six services have access to most intelligence techniques prescribed by the Interior Security Code.[43] The 'second circle' (*second cercle*) services have access to a number of intelligence techniques depending on their mandate.[44] These are police,*gendarmerie* and security services that are not part of the French intelligence community. Since 2017, the 'second circle' has been widened to include two offices placed under the authority of the director of prison administration (*directeur de l'administration pénitentiaire*), under the minister of justice. These can be authorised to use certain intelligence techniques to prevent terrorism, crime and organised crime in prisons.[45]

A state's constitutional organisation also plays a role in the organisation of the services. In Germany, for example, aside from the federal services, each regional state (*Land*) has an intelligence service.

Another key element is the extent of the relationship between security services and law enforcement. Indeed, an organisational separation between intelligence services and law enforcement authorities is commonly considered a safeguard against the concentration of powers in one service and the risk of arbitrary use of information obtained in secrecy.

Maintaining a separation between police and intelligence services

"[I]nternal security services should not be authorised to carry out law enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law enforcement agencies."

PACE (1999), p. 2

42 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 811-1. See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 40.
43 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 811-2.
44 *Ibid.* See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 51.
45 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 811-2 III. See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 54. See for critical views on this widening of the intelligence circles: France, DPR & CNCTR (2017), p. 49 and 60 and following.

The majority of intelligence services in the EU Member States have their own structure, organisation and accountability, independent of the police and other law enforcement authorities. Calls for enhanced cooperation between police and intelligence services in the fight against terrorism sometimes make it difficult to see the dividing lines between the two entities. The wave of terrorist attacks across Europe in the past few years has brought law enforcement and intelligence services closer together, with security professionals widely regarding joint investigations of terrorist networks and suspects as constituting best practice.

Differences between surveillance by police and by intelligence services

"[Surveillance by intelligence services] differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lay both the value it can have for security operations, and the risk it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights."

Council of Europe (2016), p. 64

Since publication of the 2015 FRA report, Cyprus has established its intelligence services in law. The law provides for strict organisational separation between the police and the intelligence services.[46] Few Member States make exceptions to this rule. Those that do include Austria, Denmark, Finland and Ireland, where the body responsible for conducting intelligence activities is officially part of the police and/or law enforcement authorities.

Organisational separation in law does not necessarily mean that the exchange of information and personal data between law enforcement and intelligence services is prohibited by law, given increasingly common fields of competence, such as the fight against terrorism. Indeed, national legislation may provide for data transfers between these authorities, in accordance with the rights to private life and personal data protection.[47] In Germany, for instance, the police and intelligence services have used shared databases frequently since 2004.[48]

46 Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*) N. 75(I)/2016, Art. 3.
47 Sule, S. (2006), pp. 128 and 236.
48 Töpfer, E. (2013), pp. 5 and following.

2

Surveillance measures in the digital age



The 2015 FRA report presented the key features of the surveillance measures that were at the core of the Snowden revelations.[49] When referring to large-scale technical collection of intelligence, it used the term 'signals intelligence'. This report instead uses the term 'general surveillance of communications' to refer to such activity.

Signals intelligence is a traditional term originally used for the interception and analysis of radio signals – but is still widely used, even where the signals in question are transmitted by other means, such as fibre optic cables. The term is mentioned in some Member States' legislation – for example, Sweden, which refers to '*signalspaning*' – literally, 'signal reconnaissance'. When 'signals intelligence' is not used, institutions and commentators use various terms to refer to these surveillance techniques. The UN refers to 'mass digital surveillance',[50] 'online surveillance',[51] 'bulk interception',[52] or 'bulk telephone metadata collection'.[53] The UN Special Rapporteur on privacy uses the terms 'mass surveillance' and 'bulk hacking' when discussing, for example, the powers included in the United Kingdom's Investigatory Powers Act.[54] The Special Rapporteur also refers to 'bulk processing'.[55] The Committee of Ministers of the Council of Europe refers to 'broad surveillance of citizens';[56] the specialised ministers of the Council of Europe refer to 'the question of gathering vast amounts of electronic communications data on individuals by security agencies';[57] and the Parliamentary Assembly of the Council of Europe entitled its report 'mass surveillance'.[58] The European Parliament refers to 'mass surveillance' in its 2014 resolution on the topic,[59] and Bigo *et al.* in their commissioned report for the European Parliament refer to large-scale surveillance and 'cyber-mass surveillance'.[60] The ECtHR refers to 'exploratory or general surveillance'[61] and 'strategic monitoring' to identify risks (as opposed to individual monitoring of specific persons, with suspicion).[62]

The Venice Commission uses the concept of 'strategic surveillance' to emphasise that "signals intelligence can now involve monitoring of 'ordinary communications' ".[63] In doing so, it builds on the concept used in German law – strategic restriction (*strategische Beschränkung*) – adding that 'strategic surveillance' also includes "signals intelligence to collect information on identified individuals and groups",[64] therefore covering initially untargeted surveillance that becomes more targeted. The word 'strategic' denotes a process involving a selection by way of automated tools. The data go through selectors or discriminants applied by algorithms. This touches on the second key aspect of the European Parliament's definition in its 2014 resolution, which requires an explanation of the

49 FRA (2015a), p. 15-16.
50 UN, Human Rights Council (2017), Report of the Special Rapporteur Ben Emmerson, p. 10.
51 *Ibid.*
52 *Ibid.*
53 *Ibid.* p. 11.
54 UN, GA (2016a), Report of the Special Rapporteur Joe Cannataci, paras. 28-29.
55 *Ibid.* para. 29.
56 Council of Europe, Committee of Ministers (2013).
57 Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), para. 13 (v).
58 Council of Europe (2016).
59 European Parliament (2014), Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014) 0230, Strasbourg, 12 March 2014.
60 Bigo, D. *et al.* (2013), p. 14.
61 ECtHR, *Klass and others v. Germany,* No. 5029/71, 6 September 1978, para. 51.
62 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 4.
63 Council of Europe (2016), p. 61.
64 *Ibid.* p. 61, fn. 4.

distinction between targeted and untargeted collection. The UK Independent Reviewer of Terrorism Legislation Anderson highlighted the difference between the concept of bulk powers, as prescribed by the United Kingdom's legal framework, and 'mass surveillance', in a 2016 report (see excerpted quote).

Bulk powers versus mass surveillance

"[T]he exercise of a bulk power implies the collection and retention of large quantities of data which can subsequently be accessed by the authorities. On this broad definition, the characterisation of a power as a bulk power does not depend on whether data is collected and stored by the Government or by a private company. […]

But the [Investigatory Powers Bill] proceeds on a narrower definition of bulk powers, limited to those powers which provide for data in bulk to be acquired by the Government itself.

Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "*mass surveillance*". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers [CSPs]) is not given on an indiscriminate or unjustified basis."

Anderson QC, D. (2016), Report of the bulk powers review, p. 3-4

Technological developments and the need to respond to new national security threats, particularly in the context of counter-terrorism, prompted intelligence gathering techniques to evolve. Intelligence services now focus more on network traffic – the data moving across a network at a given point in time.

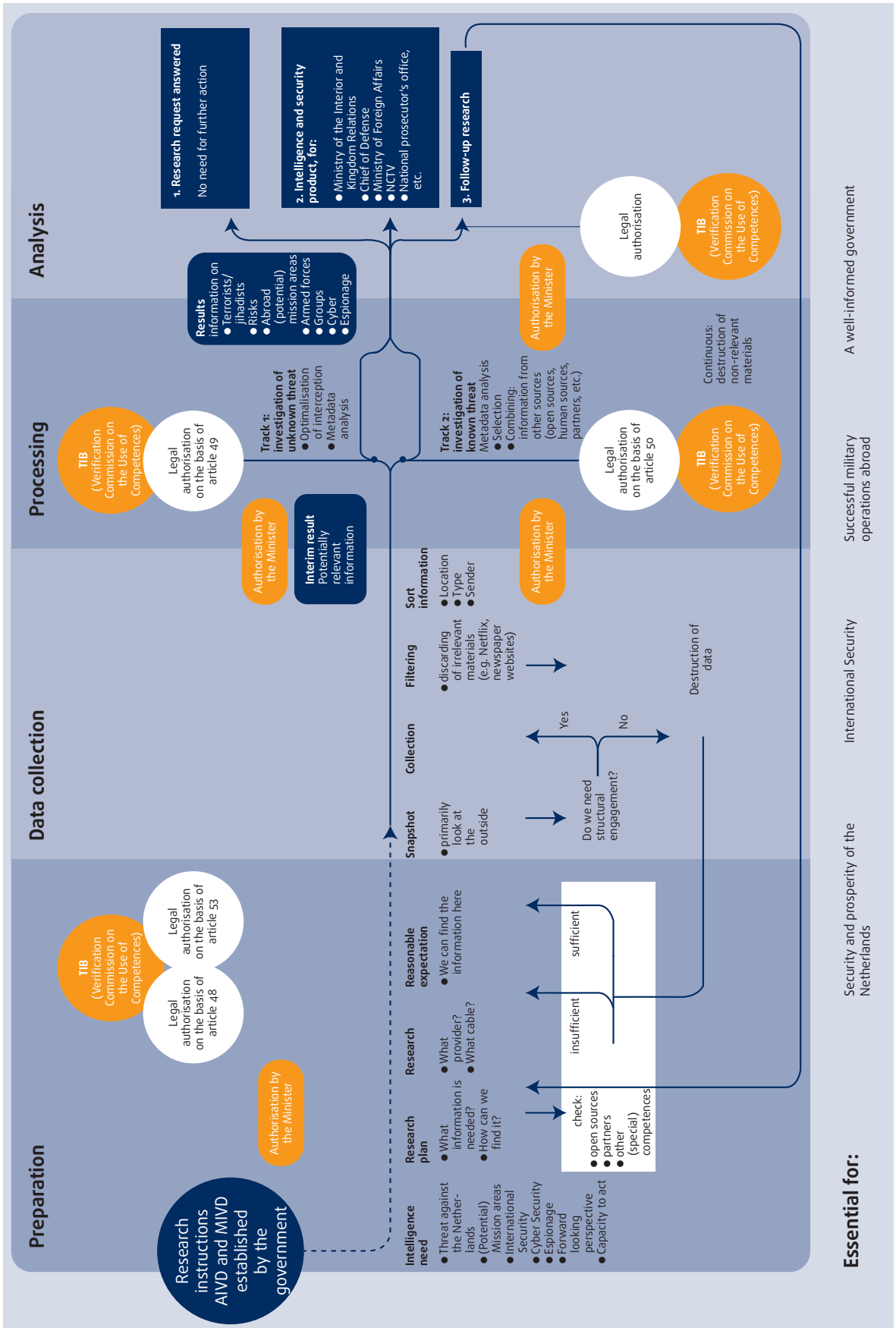
The 2015 FRA report referred to a publication of the US National Research Council to illustrate the conceptual model of signals intelligence.[65] Meanwhile, the Dutch government published an alternative figure when it submitted the Dutch draft intelligence bill, reflecting the Dutch process of cable communications interception after the Intelligence and Security Services Act 2017 enters into force (see Figure 2).[66] It shows that the Dutch intelligence services will intercept communications transmitted via cables when they will not have sufficient information from other sources. Figure 2 also shows that the collected data are filtered before they are stored, to disregard irrelevant materials for the fulfilment of the intelligence services' mandate. The final stage before storage consists of sorting the data according to the information they provide (for example, location or identity). Concerning the processing of the stored data, Figure 2 shows that selection is conducted to identify the possibly relevant information for a particular investigation. Once the final analysis of the gathered intelligence is completed, intelligence services continue with 'follow-up research'.

In 2015 and 2016, the CJEU delivered judgments in the *Schrems*[67] and *Tele2*[68] cases, respectively. In *Schrems*, the CJEU examined the interference with EU citizens' right to private life and protection of personal data resulting from surveillance activities by US authorities – specifically, the collection of and access to data of EU citizens transferred to the US pursuant to the Safe Harbour Decision.[69] The CJEU used the terms 'storage of data on a generalised basis'[70] and 'access to data on a generalised basis'[71] to describe the bulk collection of data and unrestricted access to the data by public authorities, respectively. In *Tele2*, the CJEU used the terms 'general and indiscriminate retention of electronic communications data',[72] *'generalised retention'*[73] and 'access not restricted genuinely and strictly to one of the [specified] objectives'.[74] Korff *et al.* used the term 'generic access to communication data' for the purposes of their article, based on the CJEU's terminology in *Schrems*.[75]

The great variety of terms used highlights that what one deems appropriate terminology depends on one's point of view. The differences in terminology reflect the varying objectives and perspectives regarding the same or overlapping phenomena. From the intelligence services' point of view, 'signals intelligence' refers to a type of technology used to collect data. This technology is used for a specific ('strategic') purpose, at a given scale (mass/bulk), and within legal boundaries. In this report, FRA uses, to the extent possible, the terminology adopted in national laws, while having

65 FRA (2015a), p. 16.
66 The Netherlands, National Government (*Rijksoverheid*) (2016), Infographic about AIVD and MIVD's method of interception of information (*'Gemoderniseerde Wet op de inlichtingen- en veiligheidsdiensten: extra bescherming veiligheid én privacy'*), Press Release 28 October 2016.
67 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015.
68 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016.
69 European Commission (2000), Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215 (*Safe Harbour Decision*).
70 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 93.
71 *Ibid.* para. 94.
72 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 62.
73 *Ibid.* para. 113.
74 *Ibid.* para. 114.
75 Korff, D. et al (2017), p. 14.

Figure 2: Intelligence cycle in the Netherlands



Source: *National government (Rijksoverheid) of the Netherlands, 2016 (original figure available on their website)*

in mind the 'systems' referred to by the European Parliament in its 2014 resolution.[76]

While the FRA 2015 report describes the distinction between targeted and untargeted surveillance in detail,[77] this report covers both types of surveillance by intelligence services.

In the context of general surveillance of communications, distinguishing between targeted and untargeted surveillance can be problematic, given that a target can be defined after collecting and filtering certain data. This in turn raises the question of when an interference with fundamental rights can be established.

Notes on terminology

General surveillance of communications

Intelligence can be collected with technical means and at large scale. This surveillance technique is referred to in different ways, including 'signals intelligence', 'strategic surveillance', 'bulk investigatory powers', 'mass digital surveillance' and 'storage of data on a generalised basis'. Whenever possible, FRA uses the national laws' terminology, but also uses – as a generic encompassing term – 'general surveillance of communications'.

Targeted and untargeted surveillance

Based on whether or not a target exists, surveillance measures can be divided into targeted and untargeted surveillance. 'Targeted surveillance' presupposes the existence of prior suspicion of a targeted individual or organisation. 'Untargeted surveillance' starts without prior suspicion or a specific target.

76 European Parliament (2014), para. 1.
77 FRA (2015a), p. 17-18.

3

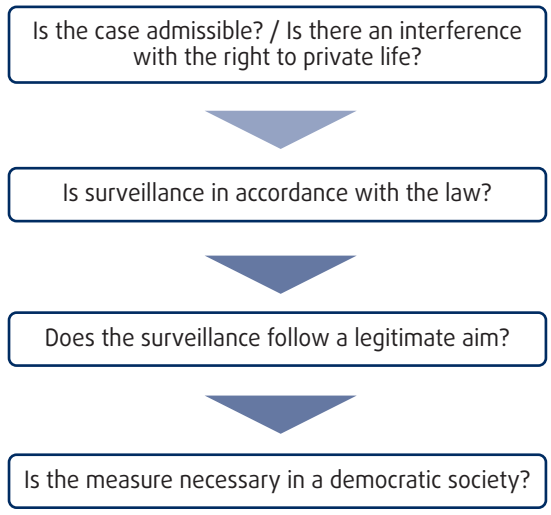
Interference with the right to respect for private life

Surveillance measures and surveillance legal frameworks can ultimately be subjected to the control of the ECtHR. Once domestic remedies have been exhausted, individuals can bring a case before the ECtHR, alleging that surveillance measures are violating their human rights. Before considering whether a particular surveillance measure is justified under the ECHR, the ECtHR will assess whether the applicant can be considered a 'victim' under the ECHR to determine whether their case is admissible.

Due to the necessarily secret character of surveillance measures, applicants always struggle to demonstrate that they were under surveillance. The court often joins the question of whether an applicant can be considered a "victim" (i.e., has victim's status) with the question of the existence of an interference with the right to private life. Figure 3 presents the different stages of the ECtHR's review. This chapter focuses on the definition of the interference with the right to respect for private life.

The ECtHR has held, in the context of examining *in abstracto* claims,[78] that the mere existence of a law permitting surveillance in itself constitutes interference. The ECtHR sets two conditions for deeming legislation that permits surveillance measures an interference

Figure 3: Stages of control by ECtHR in the context of surveillance



Source: *FRA, 2017*

78 ECtHR, *Roman Zakharov v. Russia* [GC], No. 47143/06, 5 December 2015 (Grand Chamber), paras. 229-231; ECtHR, *Kennedy v. United Kingdom*, No. 26839/05, paras. 118-129 and the judgments cited therein.

with a right. First, the scope of the legislation must be such that the applicant can possibly be affected by it. Second, the ECtHR looks at the availability of effective remedies at the national level. If there are no effective remedies, the ECtHR considers interference with the right to private life to occur with the mere existence of legislation permitting surveillance. In practice, once intelligence services intercept a signal and start collecting data, they interfere with the right to private life. The CJEU has followed the same point of view.[79]

ECtHR case law: interference with the right to private life

"[T]he Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. [...] [W]here the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified [...]. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto*, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 4 December 2015, para. 171*

Under the GDPR, any processing of personal data – including collection of data – amounts to interference. Intelligence services sometimes collect data by requesting telecommunications providers to transfer their customers' data to them. Under EU data protection law, such data collection constitutes an interference.

At the same time, a question arises as to the definition of 'collection' of data. Figure 2 indicates that, in the Netherlands, the collection of data includes the stage when intelligence services extract data from an intercepted signal, filter and, eventually, store it.

Among EU Member States, the general understanding is that the interception of a signal is a form of data collection. This is reflected, for example, in the respective laws of France, Germany and the United Kingdom regarding interception of interception of electronic communications. In France, after foreign electronic communications are gathered from an intercepted signal, their exploitation is subject to authorisation by the prime minister.[80] If communications using connections based on subscriptions from the French territory are identified, these are immediately deleted.[81] Finally, the collected, transcribed or extracted data must be destroyed within a time period specified by law.[82] In Germany, the intelligence services capture telecommunications data and store them without any other prior processing.[83] They must then, within a certain time period, identify the data and delete those not relevant to the purposes for which the surveillance measure was implemented. In the United Kingdom, the intelligence services intercept electronic communications in the course of their transmission.[84] Subsequently, they select certain intercepted data for examination. The selected data are then disclosed to authorised persons.

However, the mere collection of data by intelligence services is not universally accepted as the starting point of an interference with the right to private life. As previously noted, intelligence services store the data they have collected and, when needed, later access them for analysis. Some suggest that an interference begins only when intelligence services actually access and analyse the previously collected data. For example, the governments of the United Kingdom and Ireland argued before the CJEU – in a case concerning

79 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, 8 April 2014; CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson v. Home Secretary*, 21 December 2016, para. 100.

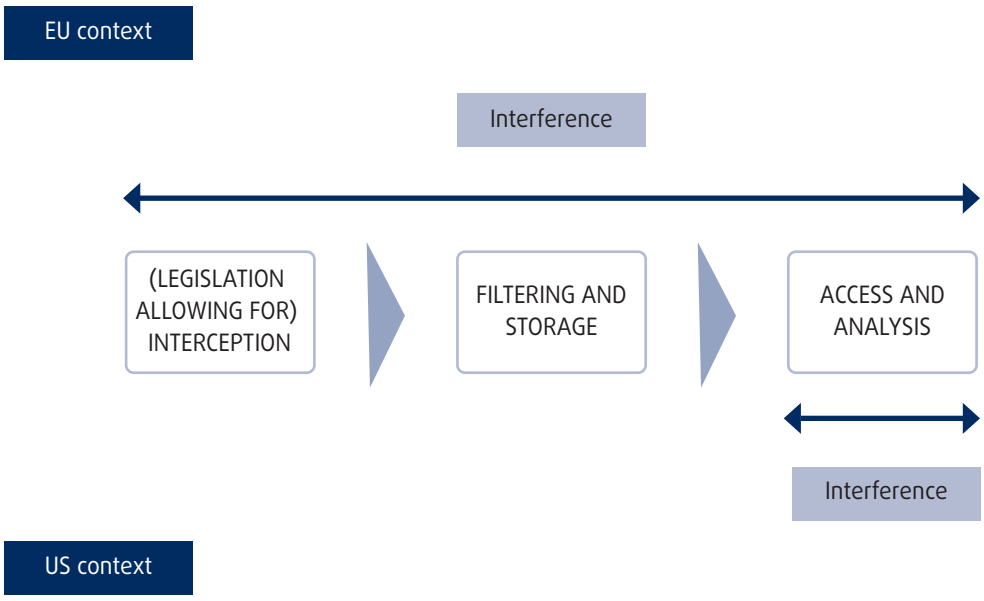
80 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-2.
81 *Ibid.* Art. L. 854-1.
82 *Ibid.* Art. L. 854-5.
83 Germany, Federal Intelligence Act (*Gesetz über den Bundesnachrichtendienst*) (BNDG), s. 2.
84 United Kingdom, Investigatory Powers Act 2016, Part 6, Chapter 1.

the EU-Canada PNR Agreement[85] – that there is no interference until intelligence services start using collected data. The CJEU reaffirmed the position that communication of personal data to a third party, such as a public authority, constitutes an interference with the right to respect for private life, regardless of the subsequent use of the information communicated.[86]

Figure 4 shows the difference in the perception of the notion of an interference in the EU and US contexts. In the United States, an interference is considered to occur when intelligence services use the data, and not when they collect them.[87] In practice, this means that an interference with the right to private life is established when intelligence services access and analyse the previously collected data.

The differences in the understanding of the notion of an interference are important when European courts assess surveillance measures. According to both ECHR and EU law, an interference with the right to private life is established with the existence of legislation allowing for surveillance measures, and this opens the way to a control on the merits of the case. Therefore, European courts consider the mere collection of data by intelligence services to constitute an interference.

Figure 4: Different understandings of 'interference' (EU and US)



Source: FRA, 2017

85 CJEU, *Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, Opinion of the Advocate General, 8 September 2016, paras. 171-172.

86 CJEU, *Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, Opinion of the Court (Grand Chamber), 26 July 2017, paras. 124-125.

87 United States, National Research Council (2015), p. 36.

4

Surveillance "in accordance with the law"



UN good practices on mandate and legal basis

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.

Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorising, overseeing and reviewing the use of intelligence-collection measures.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The establishment of an interference with the right to private life opens the way for the ECtHR to assess whether it can be justified under the ECHR (see Figure 3). When it does so, the court examines whether the interference:

- is in accordance with the law;
- pursues a legitimate aim; and
- is necessary in a democratic society to achieve that aim.

Given the seriousness of the interference in cases of surveillance, the ECtHR has developed a set of minimum safeguards for interferences to be deemed in accordance with the law. These criteria have been established in the context of targeted surveillance, but they also apply to general surveillance of communications. The court summarised them in *Roman Zhakarov v. Russia*. The CJEU has embraced a similar approach.

ECtHR case law: quality of the law

"[A]ny interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim [...].

The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects [...].

The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...].

Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference [...].

In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed [...]."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015, paras. 227-231

CJEU on quality of the law

"[N]ational legislation must, first, lay down clear and precise rules governing the scope and application of [...] a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary."

CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson v. Home Secretary, 21 December 2016, para. 109

Given the complexity of the issue, it can be difficult for a lay person to understand surveillance legal frameworks. In light of this reality, the ECtHR has not excluded the possibility for a law to be considered sufficiently clear if individuals can obtain the necessary understanding of the law by seeking legal advice.[88]

FRA's fieldwork[89] in seven EU Member States confirmed that expectations for lay persons to understand surveillance legislation – even with legal advice – are unrealistic. Most actors working in the field agree that such legislation hardly meets the standards of clarity and foreseeability. Officials interviewed also deemed such pieces of legislation as particularly complex compared to legislation encountered in other areas of their professional expertise and experience.

"The law governing the intelligence services is difficult to understand, inconsistent and has no regulatory concept."

(Academia)

Interviewees tended to be critical of current legislation. The views most differed by the type of institution represented: the further removed respondents were from the respective oversight system, the more critical they were. In this regard, civil society organisations (mainly represented by legal professionals or lawyers involved in law suits), academics and practicing lawyers were more critical than representatives of oversight bodies or executive control.

Representatives of the aforementioned public institutions tended to be less critical. The data collected provide possible explanations for this perspective. First,

88 ECtHR, *Kafkaris v. Cyprus* [GC], No. 21906/04, 12 February 2008, para. 140 and *Del Rio Prada v. Spain* [GC], No. 42750/09, 21 October 2013, para. 79.

89 Annex 1, section on 'Social fieldwork methodology', presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

representatives of the public administration work with the direct implementation of the laws, which equips them with a better understanding, the ability to provide more explanations, and examples of everyday practices. Also, they work in a specific institutional context and have built up working relationships or cooperation with others in the field. This also helps develop mutual trust with the actors in the field, including intelligence services. They are therefore in a better position to ensure compliance with standards and implementation of best practices.

"But if we put it this way, an ordinary well-educated non-lawyer looking at the legislation would not be able to understand from this that there is such a broad signal intelligence capability and they certainly wouldn't without the benefit of detailed legal advice be able to understand the ramification of what is proposed." (Lawyer)

Respondents nearly unanimously deemed the current legal framework complex – with regard to a variety of characteristics. Some noted that it is difficult to legislate simply in the area of intelligence collection. As a result, legislation is kept 'general', 'vague' or 'obscure'. Some referred to the complexity in terms of recent developments, recent changes (legislative reforms) or the need for changes in the area.

Respondents mentioned that a number of different pieces of legislation regulate the field and oversight, and that legislation sometimes contains cross-references to other legislation or to codes of conduct. As one lawyer put it: 'in terms of different pieces of legislation and institutions, it is quite a jungle out there'. Several respondents mentioned the length of the legislation, particularly the most recent legislation.

Others referred to the need for better definitions of concepts (e.g. related to 'national security'), and fewer vague terms ('it is full of very vague terms, [there is] very little in terms of thresholds') and other inconsistencies or imprecise areas. According to one lawyer, the vague wording leaves a lot of provisions open to interpretation – which is linked to the tendency to 'expand the scope of' the laws.

Adding to the complexity is the lack of cooperation between oversight bodies and inconsistencies across powers for the number of actors involved in the area. For example, some Data Protection Authorities (DPAs) mentioned ongoing discussions on how to reduce the complexity of legislation and suggested that DPAs could shoulder more work, if the necessary powers were attributed to them. According to respondents, the legal framework is also complex because the laws are incomplete (e.g. they do not address technical arrangements for oversight, although they define surveillance techniques).

"[The law] has failed numerous tests in terms of clarity and foreseeability." (Expert body)

The different actors were asked about the clarity of their respective national legal frameworks in terms of the effectiveness of the day-to-day oversight of the work of intelligence services. In relation to the content of the legislation, opinions diverge. More respondents felt that the legal framework lacks clarity than considered it sufficiently clear.

"The main aspects that characterise the law's lack of clarity are the imprecision with which the law on the intelligence services deals with a certain number of issues and the excessively vast scale of the surveillance." (Lawyer)

Respondents who stated that the legal framework lacks clarity noted the vagueness of the laws, e.g. broad definitions of terms, mandates of institutions, and many different ambitions. They considered the laws to be incomplete and in certain cases non-compliant with European case law standards. A lack of consistency and transparency was also mentioned. The definitions provided by the legal text of both the powers and mandate of the intelligence services were considered insufficiently clear. Some believe the [current] lack of clarity is intentional – to ensure the greatest possible freedom to manoeuvre. These respondents called for an improvement of current legal frameworks. Lawyers, civil society representatives and academics tended to be most critical, and more often stated that legislation lacks clarity.

"You read the text and you do not really understand what it means. You read it again, you get a bit of a glimpse, but the cascades of cross-references to other laws hinder your understanding. The terms are vague." (Civil society organisation)

Nonetheless, a significant share of respondents considered the legal framework to be clear. They tended to be representatives of parliamentary committees, expert bodies, and executive control. They noted that certain parts or aspects of the legislation are clearer than others, e.g. no clear division of competences between specific bodies, or some forms of surveillance under the legislation being slightly clearer than others. Institutions with specific mandates tended to find the legislation clear in terms of their own work. For example, data protection authorities, ombuds institutions and expert bodies suggested that the legislation is clear as far as it is related to their specific – and, in most cases, limited – function.

"That legal framework is clear for those who work for the [ombuds institution]. The framework is perhaps less clear to members of the public. There is frequent consultation between institutions to determine which institution is competent to deal with a particular matter." (Ombuds institution)

"Talking about data protection, and not violations of fundamental rights in general, the text of the law, albeit complex, is clear and comprehensible overall."

(Data protection authority)

"The general framework is sufficiently clear and it requires no further adjustments." (Judiciary)

Even though interviewed experts from oversight and executive control institutions from different Member States – e.g. Belgium, France, the Netherlands and Sweden – view the current legislation and oversight setting positively, they acknowledged several problems. Many of these echo the complaints voiced by individuals with overall more critical views. They referred to their respective system as 'quite sophisticated', 'quite unique' and 'very credible', noting that 'the construction is well-thought through'.

However, some stated that, even if clear, the legislation was outdated and needed to be updated (or was in the process of discussion). Some said it was still not able to respond to current situation while implementation of recent legislative reforms which is not yet clear. Respondents often referred to the problem of general inconsistency, fragmentation of the legal framework, and the need to improve current practices in terms of coordination among different institutions. This includes clarifying the division of competences and avoiding overlapping functions. Some respondents also stated that the legislation regulating the oversight of intelligence services lacks clarity.

4.1. Member States' laws on surveillance

In some Member States, the legal basis that frames the intelligence services' mandate and powers consists of one unique legal act governing their organisation and means – Cyprus is a recent example.[90] In others, complex frameworks consisting of several laws and regulations stipulate specific aspects of the services' mandate, organisation, competences or means (e.g. the United Kingdom). However, most Member States organise the work of their intelligence services in two laws: one on their mandate and organisation, the other on means of action and the conditions for using them. For instance, the Act on the Security Services of the Czech Republic sets out the general legal framework for the intelligence services in that Member State. The powers of each intelligence service are further detailed in two separate acts.[91]

A review of legal frameworks regulating surveillance methods used by intelligence services shows that 27 of 28 Member States have codified their use; Cyprus is the exception. In Cyprus, a recently adopted law codifies the existence of operations conducted by intelligence services. However, it does not regulate the surveillance methods used by the intelligence services, nor does it explicitly sanction or prohibit surveillance.[92] In Portugal, a law adopted in July 2017 lays down the conditions for intelligence services to access metadata of an existing target.[93]

As far as general surveillance of communications is concerned, the 2015 FRA report showed that France, Germany,[94] the Netherlands, Sweden and the United Kingdom have detailed legislation governing the use of measures aiming at general surveillance of communications.[95] France, Germany and the United Kingdom have significantly reformed their intelligence laws since 2015. Several other EU Member States have started wide-reaching reform processes – such as Finland, which will be the sixth Member State with detailed legislation on general surveillance of communications if the proposed reform is adopted.

"The reform of the legal framework has been very positive. It has brought clarity and changed the world of intelligence services, changed the approach and the methodology. No more deviated secret services." (Parliamentary committee)

"The [new] legislation is positive to the extent that it makes explicit things which were previously implicit." (Lawyer)

The reforms in the Member States were triggered by various factors. The intelligence services needed to adapt to

90 Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*) N. 75(I)/2016.

91 Czech Republic, Act on the Security Information Service (*Zákon o bezpečnostní informační službě*), No. 154/1994, 7 July 1994; and Czech Republic, Act on Military Intelligence (*Zákon o Vojenském zpravodajství*), No. 289/2005, 16 June 2005.

92 Cyprus, Cypriot Intelligence Services Act 2016 (*Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών Νόμος του 2016*).

93 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Lei Orgânica n.º 4/2017 de 25 de agosto *Aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de Agosto* (Lei da Organização do Sistema Judiciário).

94 The NSA inquiry committee's report provides additional explanation on the legal framework and its implementation before the 2016 reform: Germany, Federal Parliament (2017a), p. 687 and following.

95 FRA (2015a), p. 20.

new technologies to better respond to new threats (particularly in a counter-terrorism context). Public authorities reacted to the Snowden revelations with enhanced transparency on the intelligence services' powers in an effort to regain the population's trust which had been undermined by the revelations. In the case of Germany, discussions on the legal framework's shortcomings in the NSA inquiry committee prompted legal reform in 2016, even before completion of the committee's report in June 2017. Overall, the reforms contributed significantly to enhanced clarity in the respective laws. Fieldwork participants from the Member States at issue acknowledged that the reforms brought improvements. However, they stated that the lack of clarity – and hence the need for quality legal rules governing the work of intelligence services – remains an issue.

4.2. Targeted surveillance regulated by almost all Member States

Targeted surveillance, as regulated in the Member States' laws, refers to concrete targets (individuals, group of individuals or legal entities) upon suspicion that an act falling within the remit of the intelligence services' tasks could be committed before a surveillance measure can be initiated. In some Member States (e.g. the United Kingdom), a single targeted surveillance measure can cover a considerably wide scope of targets.

In Belgium, the State Security (*Sûreté de l'Etat*) can research, analyse and treat intelligence that is connected with the activities of an individual or a group of individuals who "threaten or could threaten", among others, the state's internal or external security.[96] Such activities are explicitly identified in the Intelligence Services Act: espionage; intrusion; terrorism; extremism; proliferation; harmful sectarian organisations; and criminal organisations.[97]

The definitions of each of these activities are also set out in the law.[98] The Belgian Standing Committee I confirms, via its oversight activities, that the intelligence services have been complying with the requirement to focus their activities on an individual or a group of individuals.[99]

The Belgian law envisages the use of ordinary, specific and/or exceptional methods of surveillance. Within the context of ordinary surveillance measures, intelligence services can request from public authorities the relevant information they need for their missions. They can also access the databases of the public sector.[100] Specific measures are comparatively more intrusive into individuals' private life. They include identification or localisation, by technical means, of the services and electronic communication methods to which an individual is subscribed. The intelligence services may request this information from telecommunications providers. The collection of electronic communications data, such as the location of the recipient of a call, is also considered a specific measure.[101] The most intrusive targeted surveillance methods in Belgium are exceptional measures. These permit intelligence services to interfere with a computer system or listen to and record electronic communications.[102]

In Italy, the law does not explicitly distinguish among the methods of surveillance depending on the threat. The Agency for information and external security (*Agenzia informazioni e sicurezza esterna*, AISE) and the Agency for information and internal security (*Agenzia informazioni e sicurezza interna*, AISI) may carry out tapping activities and preventive controls on communications – such as interception of phone calls and e-mails – "when these are deemed essential for performing the tasks assigned to them".[103] The surveillance methods are similar to those used in judicial proceedings. The tasks assigned to AISE and AISI are set out in legislation.[104] The intelligence services may use surveillance methods only to ensure the defence of the independence, integrity and security of the Republic from foreign threats or the defence of the internal security of the Republic and its democratic institutions from all kinds of threats, subversive activity and forms of criminal or terrorist aggressions. Nevertheless, the use of surveillance measures is allowed only where applied to a single target or a group of targets previously specified by the intelligence services.[105]

In the United Kingdom, a targeted interception warrant is not necessarily related only to a single person or set of premises. The target can be "a group of persons who

96 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 8 (1).
97 *Ibid.*
98 *Ibid.* Art. 8 (1) (a) – (g).
99 Belgium, Standing Committee I (2015), pp. 20-21.
100 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 14.
101 *Ibid.* Art. 18 (2) and (3).
102 *Ibid.* Art. 18 (10).
103 Italy, Implementing provisions of the Code of Criminal Procedure *(Disposizioni di attuazione del codice di procedura penale)*, Art. 226 read in conjunction with Italy, Legislative Decree no. 144 of 27 July 2005, Art. 4 converted into Law no. 155 of 31 July 2005, as amended.
104 Italy, Law no. 124 of 3 August 2007 on "Information System for the security of the Republic and new rules on State secrets" (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*), Arts. 6-7.
105 Italy, Implementing provisions of the Code of Criminal Procedure *(Disposizioni di attuazione del codice di procedura penale)*, Art. 226.

share a common purpose or who carry on, or may carry on, a particular activity" or "more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation".[106] This type of targeted interception warrant can be called 'thematic'.[107] The potential scope of thematic interception warrants can be quite broad given that the "[d]escriptions of persons, organisations or sets of premises [in the warrant] must be as granular as *reasonably practicable* in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interception."[108]

In Portugal, a recently adopted law grants powers to the intelligence services to conduct targeted surveillance. It allows for the intelligence services to access source and equipment location data retained by telecommunication providers for the purposes of ensuring national defence, internal security and prevention of acts of sabotage, espionage, terrorism, proliferation of weapons of mass destruction and highly organised criminality. Such measures cannot exceed the duration of three months and can be deployed exclusively in relation to a concrete operation, involving specific targets. The law explicitly bans real-time network traffic surveillance.[109]

4.3. Member States reform legislation on general surveillance of communications

The 2015 FRA report showed that five Member States – France, Germany, the Netherlands, Sweden and the United Kingdom – detail the conditions that permit the use of both targeted and untargeted surveillance.[110] This report focuses on these same five Member States when discussing detailed legislation on general surveillance of communications. FRA's selection is based on the fact that this type of collection is prescribed, in detail, in the law. The list of five Member States is in no way exhaustive, in the sense that other Member States' laws might allow for general surveillance of communications – but they do not regulate it in detail.

In Italy, for example, a Decree-Law of 2015 gives AISE authority to perform its tasks also by electronic means (*assetti di ricerca elettronica*). The law does not provide more details about these surveillance means; it only states that it should be exclusively directed abroad.[111]

In some cases, a lack of clarity on a provision's scope can prompt courts to deem it unconstitutional. The French constitutional court reached this conclusion when assessing a clause on surveillance and control of radio transmissions (Article L. 811-5 of the Interior Security Code).[112] A June 2017 bill tries to address this issue, clarifying the scope of the surveillance technique and its oversight.[113]

Other Member States do not explicitly permit civil intelligence services to engage in general surveillance of communications. For example, in Belgium, the law grants no general surveillance of communications' powers to the civil intelligence service (State Security – *Sûreté de l'Etat*). Only the military intelligence service (General Intelligence and Security Service – *Service Général du Renseignement et de la Sécurité*) – not covered by this report – has these powers.[114]

In the United Kingdom, the Investigatory Powers Act (IPA) received royal assent in November 2016, and its various provisions have started entering into force since 30 December 2016. At the time of writing, not all provisions of the IPA were fully in force; these will be brought into force in due course by means of regulations implemented by the Secretary of State. The IPA largely – but not entirely – replaces the Regulation of Investigatory Powers Act 2000 (RIPA). Therefore,

106 United Kingdom, Investigatory Powers Act 2016, s. 17 (2).
107 Anderson, D. (2016), p. 21.
108 United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', 23 February 2017, para. 5.13.
109 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Art. 2-5.
110 FRA (2015a), p. 20 and following.
111 Italy, Legislative Decree No. 7 of 18 February 2015 converted, with amendments by law of 17 April 2015, No. 43, Art. 8. See also Italy, COPASIR (2017), p. 11 and 18. For Poland, see Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Art. 5.1 which mentions "electronic surveillance" (prowadzenie wywiadu elektronicznego) as a task of the Internal Security Agency. This task is not further regulated in the law, making it difficult to describe the nature of such type of surveillance. The same law prescribes that "the Agency is competent to access metadata (telecommunication and internet data) in order to complete its tasks". Moreover, another task of the Internal Security Agency is to investigate, prevent and detect crimes "harming the economic foundations of the state". In 2014, the Constitutional Tribunal ruled that such task is not precise enough and violates the Constitution. See Poland, Constitutional Tribunal, case no. K 23/11, 30 July 2014.
112 France, Constitutional Court (*Conseil constitutionnel*), La Quadrature du Net and Others, Decision 2016-590 QPC, 21 October 2016. See also France, CNCTR (2016), p. 48 and following and France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 72 and following.
113 France, Bill reinforcing internal security and the fight against terrorism (*Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*), 22 June 2017.
114 Belgium, Organic law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), Arts. 44 and 44/1 to 44/5.

two pieces of legislation on surveillance powers are currently in force.[115]

> *"RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable."* Anderson, D. (2015), para. 35

A legislative reform proposal in its very early stages in Finland aims to introduce a detailed legal framework on general surveillance of communications, which would make it the sixth Member State with such legislation if the proposal is adopted. In its current form, the proposal grants powers to the Finnish intelligence services to conduct 'electronic surveillance of network communications' both in Finland and abroad. Such collection of intelligence can only be carried out to counter certain outlined activities that threaten national security and by using specific search criteria, subject to judicial authorisation. The proposal also creates a new independent and autonomous authority, the Intelligence Ombudsman. The Intelligence Ombudsman would be responsible for overseeing the legality of the use of intelligence collection methods and the observance of fundamental rights in surveillance activities. The Intelligence Ombudsman would have an extensive right to access information and necessary documents as well as to conduct inspections on the premises of the intelligence services. The Intelligence Ombudsman would also have the competence to order the suspension or termination of the use of a certain surveillance technique due to illegality. In such a situation, the court that authorised the initiation of the surveillance measure would issue the final decision on whether the measure could be continued.[116]

FRA's analysis further shows that general surveillance of communications of suspects can take place both within and outside the Member State. The safeguards established in the legislation differ for domestic- and foreign-focused surveillance measures. When intelligence services conduct surveillance domestically, the applicable legal safeguards are enhanced comparing to those in place for foreign surveillance.

Enhanced safeguards in place for domestic surveillance

An analysis of the detailed legal frameworks allowing for domestic general surveillance of communications reveals that legislators have decided to adopt enhanced safeguards for this type of surveillance. Among the five Member States having detailed legislation on general surveillance of communications, three allow for domestic surveillance: France, Germany and the United Kingdom. Restrictions on the permitted techniques for domestic surveillance differ among the countries based on citizenship criteria (Germany) or territorial criteria (United Kingdom and France). Additionally, the intelligence services must obtain warrants approved by the judiciary or expert bodies.

In Germany, the Basic Law (*Grundgesetz*) permits, in select circumstances, restrictions of the inviolability of the privacy of correspondence, post and telecommunications: "Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."[117]

The 'strategic restrictions' prescribed by the *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (G 10 Act) enable the Federal Intelligence Service (*Bundesnachrichtendienst,* BND) to wiretap international communications to and from Germany. They are called 'strategic' because of their original military purpose. The BND is authorised to proceed only with the aid of selectors (*Suchbegriffe*), which serve and are suitable for the investigation of one of the threats listed in the law. The BND sets a list of either format-related selectors (e.g. telephone number or email) or content-related selectors (e.g. holy war).[118] The BND needs to specify the region and the percentage of the communication channel it wants to monitor. This percentage cannot exceed 20 % of the full telecommunication channel capacity.[119] In 2015, for example, the BND established a list of 1,762 selectors in the context of international terrorism to be applied on 1,132 telecommunication channels (email, voice recognition (*Spracherfassung*), data sets of metadata (*Verkehrsdatensätze*), and SMS); of these, only 41 turned out to be useful from an intelligence point of view.[120] The selectors should not contain any distinguishing features leading to a targeted telecommunication connection nor affect the core area of the private sphere. Different restrictions apply to communications outside Germany, unless they involve German citizens.[121] The list of selectors and the overall request for surveillance is controlled *ex ante* by

115 United Kingdom, Investigatory Powers Act 2016, Explanatory memorandum.
116 Finland, Ministry of Interior (2017), pp. 301-303.
117 Germany, Basic Law (*Grundgezetz*), Art. 10 (2).
118 See Huber, B. (2013), p. 2573.
119 Germany, G 10 Act, s. 10 (4).
120 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 8.
121 Germany, G 10 Act, S. 5 (2). See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1236 and following. Academia has questioned whether this nationality-based legislation is compatible with the German constitution and with EU Law. See Schenke, W.-R. *et al.* (2014), p. 1402.

the G 10 Commission, which decides whether the measures are permissible and necessary.[122] The surveillance order is valid for a renewable three-month period.

In 2015, the G 10 Act was further amended to increase the surveillance powers of the intelligence services: surveillance may now also be launched against individuals suspected of having planned or committed cybercrimes. The same amendment also provides that the BND may monitor international telecommunication to and from Germany to detect and respond to international cybercrime.[123]

In the United Kingdom, the Investigatory Powers Act 2016 provides an updated framework for the use of 'bulk' investigatory powers to obtain communications and communications data by the intelligence and security services.

Promising practice

Requesting independent reviewer to scrutinise surveillance powers

In the United Kingdom, while the Investigatory Powers Act was debated in parliament, the Home Office requested the Independent Reviewer of Terrorism Legislation, then David Anderson QC, to review the operational case for bulk powers. With a point of view independent from government and the ability to access secret national security information, the Independent Reviewer explained how bulk powers are currently used by the intelligence services; their importance to national security; the safeguards in place; potential changes the Investigatory Powers Bill brings; and recommendations for better adaptation of the intelligence collection techniques to the new threats and technologies.

For further information, see Anderson, D. (2016)

The powers that can be used domestically cover the retention and acquisition of electronic communications data,[124] and the retention and examination of bulk personal datasets.[125] For the purposes of this research, obtaining communications should be understood as 'obtaining the content of the communications' whereas obtaining of communications data should be understood as 'obtaining metadata' within the meaning of the definition included in the proposal for an e-Privacy Regulation (see box on EU legal terminology).

Note on terminology: EU law

'Electronic communications metadata'

"'[E]lectronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication."

'Electronic communications content'

"'[E]lectronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound."

European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), *COM (2017) 10 final, Brussels, 10 January 2017, Art 4 (3) (c) and Art. 4 (3) (b).*

'Bulk acquisition' refers to the power of the intelligence services to require a telecommunications operator to retain communications data and disclose these to the intelligence services, as well as to select for examination the acquired communications data, as specified in the warrant.[126] Essentially, the telecommunications providers transfer the "who", "where", "when", "how" and "with whom" of communications, but not what was written or said. It includes information such as the identity of a subscriber to a telephone service or a detailed telephone bill. The bulk acquisition technique can be applied domestically, but the intelligence services may only collect communications data and not the content of the communications.[127] The bulk acquisition power originally derives from section 94 of the Telecommunications Act 1984.[128] The NGO Privacy International challenged the bulk acquisition powers under this provision before the Investigatory Powers Tribunal (IPT) – the specialist court of the United Kingdom for surveillance matters. The IPT ruled that until 4 November 2015 – when stricter safeguards were introduced – the intelligence services were violating the

122 Germany, G 10 Act, s. 15 (5).
123 *Ibid.* s. 5 (8).
124 United Kingdom, Investigatory Powers Act 2016, ss 158 – 175. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
125 *Ibid.* ss. 199 – 226. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
126 *Ibid.* s. 158 (6). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
127 *Ibid.* s. 158(6). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
128 For a description and assessment of the original bulk acquisition powers, see United Kingdom, IOCCO (2016b). See also United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 8 September 2017, paras 14-17.

right to private life (Article 8 of the ECHR).[129] Anderson provides an example of the use of bulk acquisition powers by the Security Service MI5: a threat was made by telephone against an overseas embassy in London. The Security Service used bulk acquisition data to identify the user of the telephone as a known hoaxer.[130]

Bulk personal datasets are sets of "information that includes personal data relating to a number of individuals"[131] and "the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions".[132] In simple terms, bulk personal datasets are sets of information about a large number of individuals, the majority of whom will not be of any interest to the intelligence services. However, the intelligence services will only look at the data relating to the minority who are of intelligence interest.[133] The use of bulk personal datasets by the intelligence services was disclosed for the first time in a 2015 report by the Intelligence and Security Committee of Parliament.[134] Privacy International challenged them before the IPT and, as for the bulk acquisition powers, the IPT found that the intelligence services violated the right to private life until 12 March 2015, when stricter safeguards were introduced.[135] Anderson provides an example of the use of bulk personal datasets following the attacks in Paris and Brussels: the Secret Intelligence Service (SIS) worked in partnership with MI5 and the Government Communications Headquarters (GCHQ) to identify individuals in so-called Islamic State of Iraq and the Levant networks who posed a threat to the United Kingdom. SIS used bulk personal datasets to identify a number of such individuals.

The United Kingdom's intelligence services, before exercising one of the 'bulk' powers, must obtain a warrant authorised by the Secretary of State and approved by a Judicial Commissioner. The warrants must specify the operational purposes for which any communications data obtained under the warrant may be selected for examination. The acceptable purposes for a warrant to be obtained are: national security; prevention or detection of serious crime; and the economic well-being of the United Kingdom, provided that this is related to the interests of national security.[136]

Promising practice

Explaining surveillance laws in codes of practice and on intelligence services' websites

In the **United Kingdom**, the government presented publicly to Parliament plain language draft codes of practice to explain each of the different forms of investigatory powers. Following a consultation process, they will be published in final form. In addition, the Secret Intelligence Service (SIS), the Security Service MI5 and GCHQprovide an easy-to-read explanation of the intelligence techniques' legal framework on their respective websites. They provide simple definitions of bulk investigatory powers, allowing individuals to better understand the law. This effort aims to increase transparency on the work of the intelligence services.

For further information, see the websites of the SIS, MI5 and GCHQ

The 2015 FRA report presented the domestic general surveillance of communications technique introduced in 2015 in France.[137] The law envisaged a potential obligation on telecommunications providers to detect terrorist threats with the use of 'algorithms' on their customers' connection data.[138] The CNCTR adopted a detailed opinion specifying what should be understood by 'connection data'.[139] For the purposes of this research, it should be understood as 'metadata'. In July 2016, the CNCTR gave a classified opinion to the prime minister on the planned general architecture of the algorithm.[140] By March 2017, the intelligence services had yet to ask the CNCTR to give an opinion on their use of this surveillance technique, meaning this surveillance technique had not yet been used by that point.[141]

French law also provides for the use of 'IMSI catchers' by intelligence services. These are a type of technical equipment that allows data to be collected, potentially identifying users of mobile phones and the location of devices via their SIM card numbers. The maximum

129 United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 17 October 2016.
130 Anderson, D. (2016), p. 170.
131 United Kingdom, Investigatory Powers Act 2016, s 199 (1) (a). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
132 *Ibid.* s. 199 (1)(b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
133 *Ibid.* s. 212. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
134 United Kingdom, Intelligence and Security Committee of Parliament (2015), Chapter 7.
135 United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 17 October 2016.
136 United Kingdom, Investigatory Powers Act, Chapters 1 -3.
137 FRA (2015a), pp. 23-24.
138 France, Interior Security Code (*Code de la sécurité interieure*), Art. L. 851-3.
139 France, CNCTR (2016), p. 120 and following. See also France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 851-5.
140 France, CNCTR (2016), p. 40.
141 France, DPR & CNCTR (2017), p. 51.

number of IMSI catchers that can be used simultaneously is set by the prime minister, following an opinion on the matter by the CNCTR.[142]

Safeguards in case of foreign surveillance

In all five Member States that have detailed legislation on general surveillance of communications, their respective laws provide for lower safeguards for foreign-focused general surveillance of communications than for domestic surveillance. All five permit their intelligence services to perform foreign surveillance. As noted, for Germany, the citizenship criterion is crucial; however, the prior authorisation procedure applicable to foreign surveillance requires the intelligence services to disclose less information to the approving body than for domestic surveillance. In the United Kingdom and France, compared to domestic surveillance, there is no such safeguard banning the collection and access to communications content.

In Germany, since 2016, the law on the federal intelligence service (BNDG) regulates the federal intelligence service's (BND) surveillance of foreign-foreign telecommunication. The reform adapted the legal framework to take into account technological evolution. The relevant sections were incorporated into the BND Law to highlight that German constitutional protection (Article 10 of the Basic Law) does not extend to these type of data.[143] The data can be intercepted outside Germany, through cooperation with foreign services or at German communication hubs and via satellite interceptions.[144] However, the law imposes the safeguard that only a foreigner's telecommunications may be intercepted. In practice, the BND is authorised to collect and process any foreign telecommunication content data (as well as metadata) from telecommunication networks if such data are deemed necessary to detect and pre-empt, among others, "threats against internal or external security".[145] Section 6 (4) of the BNDG prohibits the BND from collecting and processing data on German citizens outside Germany. Communications of EU institutions, public institutions in the EU Member States, and EU citizens can be intercepted in the counter-terrorism and non-proliferation context or if they provide important information on third countries.[146]

The telecommunication networks to be targeted must be ordered by the Federal Chancellery in advance, with effect for no more than nine months, and approved by a newly established oversight body, the Independent Committee (*Unabhängiges Gremium*).[147] The selectors established by the head of the BND to search the flow of telecommunication data must be aligned with the interests of German foreign and security policy. The Federal Chancellery needs to be informed.[148]

In the United Kingdom, the 'bulk' powers that require a foreign-focus under the Investigatory Powers Act are bulk interception of telecommunications data[149] and bulk equipment interference.[150]

'Bulk interception' is the power of "interception of overseas-related communications"[151] and "obtaining secondary data from such communications".[152] Essentially, the intelligence services tap undersea fibre optic cables landing in the United Kingdom to intercept their traffic. Anderson provides the following example of the use of bulk interception powers: after the disruption of a United Kingdom-based terrorist cell, GCHQ and MI5 continued to investigate its potential overseas links. GCHQ had been analysing data obtained through bulk interception warrants to look for patterns of behaviour indicative of operational planning. They identified an email address that was in contact with a United Kingdom-based individual. Analysis of the communications data and content of these emails revealed more members of the United Kingdom network and details of the attack plot.[153]

'Bulk equipment interference' covers a range of techniques involving interference with electronic equipment. This includes computers, electronic storage devices and smartphones for the purpose of obtaining communications or other information. The bulk equipment interference techniques are colloquially referred to as "hacking or the implantation of software into endpoint devices or network infrastructure

142 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 851-6. See also France, CNCTR (2016), p. 41.
143 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1245 and following.
144 See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1236 and following, Wetzling, T. (2017), p. 2 and 16.
145 Germany, BNDG, S. 6.
146 *Ibid.* S. 6 (3) and (7).
147 *Ibid.* S. 9 (4).
148 *Ibid.* S. 9 (2).
149 United Kingdom, Investigatory Powers Act 2016, Part 6 Chapter 1. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
150 *Ibid.* Part 7. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
151 *Ibid.* s. 136 (2)(a). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
152 *Ibid.* s. 136 (2)(b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
153 Anderson, D. (2016), p. 159.

to retrieve intelligence, but may also include, for example, copying data directly from a computer".[154] Bulk equipment interference requires a foreign focus.[155] MI5 suggests that bulk equipment interference "can be sometimes the only method by which [they] can acquire the data" and "plays an important role in making up for the loss of intelligence that may no longer be obtained through other techniques, such as interception." Prior to the IPA's entry into force, the bulk powers interference technique was never used in the United Kingdom.[156]

The French parliament adopted the Law on international surveillance in November 2015.[157] The Constitutional Court reviewed the bill and confirmed its constitutionality.[158] The law entered into force on 2 December 2015, amending the Interior Security Code. International surveillance shall pursue the same aims as national surveillance, as defined in Article L. 811-3 of the Interior Security Code.

However, the procedure is different. Article L. 854-2 prescribes three scenarios.[159] First, the prime minister can authorise the surveillance of international communication networks, without time limitations. Second, based on a request by a minister, the prime minister can authorise the exploitation of untargeted metadata collected on international communication networks. According to Warusfel, this type of measure is similar to those done via algorithms at the national level and amounts to 'mass surveillance'.[160] Third, the prime minister can authorise the exploitation of targeted content data and metadata. The law provides for the prime minister to issue authorisations without a prior opinion by the CNCTR. The French oversight body only performs *ex post* controls over the implemented measures.[161] Interestingly though, since May 2016, pursuant to a request by the prime minister, the CNCTR agreed to deliver *ex ante* opinions on requests for the exploitation of collected data.[162] After a one-year trial phase, this informal temporary agreement was extended in March 2017.[163]

The French legal framework defines international communications as communications sent or received from abroad. They should transit on French soil.[164] As soon as a communication can be linked to a French identifier (such as a French telephone number), the data are immediately destroyed, unless the person is already under surveillance or represents a threat to the nation.[165] Furthermore, MPs, lawyers, judges and media professionals working in France cannot be placed under surveillance when travelling abroad.

In the Netherlands, the new Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) extends the powers of the intelligence services to intercept network traffic, email and phone communications. The new legislation permits the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst*, AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst,* MIVD) to use several surveillance techniques; however, this report does not deal with military intelligence services. Most importantly, the law enables the services to perform "investigation-mandated interception" of data.[166] For the purposes of this law, "interception" means tapping, receiving, recording and monitoring in a targeted manner any form of telecommunication or data transfer through automated means, irrespective of where this takes place.[167] This includes the power to undo the encryption of conversations, telecommunications or data transfers. An explanatory memorandum states that investigation-mandated interception of data targets certain geographical areas and certain data streams.[168] Essentially, the investigation-mandate interception of data is a form of general surveillance of communications to the extent that it does not provide any limits to the amount of data that can be intercepted or the size of the targeted geographical area. Within the power of the investigation-mandated interception of data, AIVD can demand telecommunications service providers to transfer their customers' data to AIVD.[169] The providers do not have any discretion. To exercise these powers,

154 *Ibid.* p. 34.
155 United Kingdom, Investigatory Powers Act 2016, s 176(1)(c). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
156 Anderson, D. (2016), p. 184.
157 France, Law No. 2015–1556 on international surveillance (Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales), 30 November 2015.
158 France, Constitutional Court (*Conseil constitutionnel*), No. 2015-722 DC, 26 November 2015.
159 France, DPR & CNCTR (2017), p. 53 and following.
160 See Warusfel, B., *in* Gohin, O. and Latour, X. (eds.) (2016), p. 353.
161 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-9.
162 *Ibid.* Art. L. 854-2 (III).
163 France, CNCTR (2016), p. 45 and 47. See also France, DPR & CNCTR (2017), p. 54.
164 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 71.
165 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-1.
166 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 48.
167 *Ibid.*
168 The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (*Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie*) (2016), Draft Act on the Intelligence and Security Services 20... (Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..), Explanatory Memorandum.
169 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 53.

the intelligence services need prior ministerial authorisation. The prior authorisation must also be examined by the Assessment Committee on the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden*).

The 2015 FRA report presented the foreign general surveillance of communications techniques available to the National Defence Radio Establishment (*Försvarets Radioanstalt*) in Sweden, which have not been subject to legislative reform since 2015.[170] The law provides for the interception of signals from cables crossing Swedish territory, at the request of specific public authorities, following judicial approval.

170 FRA (2015a), p. 23.

5 Legality in case of international intelligence cooperation



With the globalisation of conflicts and the common transnational feature of threats such as terrorism, the benefits of international cooperation are well established. To achieve their goals, intelligence services may need specialist resources or access they do not have nationally, such as to acquire data that neither their domestic nor foreign intelligence operations can provide. To this end, EU Member States may establish partnerships with each other and with non-EU intelligence services through international intelligence cooperation. International intelligence cooperation is a very sensitive, complex and secretive field, as it touches closely on states' sovereignty, and leaks or miscommunication can result in serious diplomatic crises. Very few countries disclose information on international cooperation, its processes, and existing safeguards intelligence services are expected to follow. However, recent scandals, growing media interest, academic and civil society publications as well as the explosion of the use of big data techniques have hastened a global trend of increased transparency in this area as well.[171] This section analyses the legality and transparency principles currently in force in EU Member States.

The necessity of international cooperation

"International cooperation between intelligence services is indispensable in view of the diverse global security policy challenges. If intelligence services' exchange of personal data were prohibited, intelligence services would be incapable of acting in many areas."

Germany, Federal Parliament (Deutscher Bundestag) *(2017b), p. 1236 [FRA translation]*

All EU Member States have established such arrangements to greater or lesser degree. A number of EU Member States belong to communication networks for purposes of intelligence cooperation, which link them among themselves or with non-European countries (such as, for instance, the SIGINT Seniors Europe, SSEUR).[172] International intelligence cooperation – be it bilateral or multilateral – is normally based on international and/or bilateral agreements delimiting the scope of the collaboration. These agreements may focus on a thematic aspect of the data and techniques on which the operational cooperation will take place, such as joint operations, technical support or exchange of classified information, coordinating the fight against terrorism, or cooperation on criminal matters.[173] An important addition in recent years is intelligence cooperation for the purpose of cyber security.[174] The following section details how, and to which extent, international intelligence cooperation is legally grounded in EU Member States' legal frameworks.

UN good practices on intelligence sharing laws

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

171 See Kojm, C. in Goldman, Z. and Rascof, S. eds (2016), p. 118 and following.

172 The SSEUR is composed of the Five Eyes (the U.S., the United Kingdom, Australia, Canada and New Zealand), and France, Germany, Spain, Italy, Belgium, the Netherlands, Denmark, Norway and Sweden. See Germany, Federal Parliament (2017a), p. 197.

173 Born, H., Leigh, I. and Wills, A. (2015), pp. 29-30.

174 Omand, D. (2014), in Duyvesteyn, I., de Jong, B., van Reijn, J. eds, pp. 14 and following.

Almost all Member States (27 out of 28) have established international intelligence cooperation in their national legal frameworks, defining and thereby regulating competences of intelligence services – either by granting them the authority to establish international cooperation or instructing them to enter into international partnerships. Examples of Member States with laws imposing a duty on intelligence services to cooperate with foreign partners include Belgium,[175] Latvia,[176] Luxembourg,[177] the Netherlands[178] and Portugal.[179] It is not apparent from the Maltese legal framework whether international intelligence service cooperation is prescribed by law: international exchange of data is indirectly referred to as being 'sensitive information', in cases where disclosure has not been consented to by the foreign government and cannot, consequently, be disclosed to the Security Committee.[180]

Very few Member States have explicitly articulated the modalities for both establishing and implementing international cooperation within the enabling laws. For instance, Article 59 of the Act on the Security Intelligence System of the Republic of Croatia provides that "the National Security Council shall approve the establishment and termination of cooperation with individual foreign agencies, on the basis of a proposal from the heads of security and intelligence agencies, and after obtaining the opinion of the Council for Coordination of Security and Intelligence Agencies."[181]

Few Member States have detailed laws describing the procedure intelligence services must follow to implement international cooperation. Germany, for instance, does have such laws.[182] Several Member States – Belgium,[183] Denmark,[184] Germany,[185] Latvia,[186] Lithuania,[187] the Netherlands,[188] Portugal,[189] and the United Kingdom[190] – have provided for the establishment of internal rules to be followed when exchanging information internationally. These internal procedural documents are drafted either by the services (Belgium, the Netherlands and Portugal) or by the executive (Latvia, Lithuania, and Poland). None of these internal guidelines are publicly available.

However, in a few Member States, parts of these internal rules are publicly available. In the Netherlands, for instance, where internal guidelines are classified, the Dutch oversight body (CTIVD) published its first in-depth assessment of these procedures in 2009.[191] In 2016, an updated and revised version of this report also included a detailed presentation of the most recent internal guidelines adopted by the AIVD in 2013 and 2014.[192] In the United Kingdom, general guidelines are also classified, but specific guidelines – on international intelligence cooperation where there is a risk of torture, for instance – are publicly available.[193]

Internal guidance applied by intelligence services might take different forms. In Denmark and Latvia, exchanges of intelligence may take place under specific rules and regulations, drafted by the services in the case of Denmark[194] and the cabinet of ministers in

175 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 20 (1).
176 Latvia, Law on Constitution Protection Bureau (*Satversmes aizsardzības biroja likums*), 5 May 1994, Art. 5 para. 5(3).
177 Luxembourg, Act of 15 June 2004, Art. 3(1).
178 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 88.
179 Poland, Act on the Internal Security Agency and the Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), 24 May 2002, Art. 8.
180 Malta, Security Service Act, Art. 14(3).
181 Croatia, Act on the Security Intelligence System of the Republic of Croatia, 30 June 2006, Art. 59.
182 Germany, BNDG, S. 13 and following and Germany, G10 Act, S. 7a. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1274 and following and See Siems, T. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1479 and following.
183 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 20.
184 Denmark, Danish Security and Intelligence Service (PET), Legal Matters – Legislation.
185 See description in Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 504 and p. 509 and following.
186 Latvia, Law on the State Secrets (*Par valsts noslēpumu*), 17 October 1997, Art. 9, para. 7.
187 Lithuania, the State Defence Council (*Valstybės gynimo taryba*), establishes guidelines for international cooperation of intelligence institutions with intelligence and security institutions of foreign states, international organisations and institutions, which are not publicly available.
188 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 88.
189 Portugal, Law 50/2014, 1st amendment to law 9/2007 of 19 February that lays down the Organic law of the Secretary-General of the Intelligence Services of the Portuguese Republic, the Strategic Defence Intelligence Service and the Security Intelligence Service, 13 August 2014.
190 United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 42.
191 The Netherlands, CTIVD (2009), pp. 78-80.
192 The Netherlands, CTIVD (2016a), pp. 14-17.
193 See Born, H., Leigh, I. and Wills, A. (2015), p. 127, and United Kingdom, Cabinet Office (2010), Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees, Cabinet Office, July 2010.
194 Denmark, Danish Security and Intelligence Service (PET), Legal Matters – Legislation.

Latvia.[195] Three Member States – Austria,[196] Bulgaria[197] and Hungary[198] – apply the rules of police international collaboration to the procedures for establishing intelligence international cooperation. But, interestingly, not all Member States in which intelligence services are part of law enforcement authorities use police cooperation procedures. In Finland and Ireland, intelligence services legislation does not specify the procedures to be followed.

The scope of the collaboration is also not clearly detailed in law. For most Member States, international cooperation explicitly refers to both the transfer and the receipt of data, and no distinction is drawn between the two in the laws. Few Member States make an exception to this rule. In the United Kingdom, in a landmark decision, the Investigatory Powers Tribunal held, among others, that the law must specify the conditions for the receipt of data: "any request for, or receipt of, intercept or communications data pursuant [to international intelligence sharing arrangements] is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly"[199] by the government. In Germany, reforms of the intelligence services acts in 2015 and 2016 introduced detailed conditions for Germany's participation in shared databases and the transmission of intelligence data to foreign partners.[200]

UN good practices on external review of international intelligence cooperation agreements

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Very few Member States allow expert bodies to assess international agreements and/or cooperation criteria establishing international intelligence collaboration, either *a priori* or *a posteriori*. Belgium,[201] Luxembourg[202] and the Netherlands do so.[203] In Germany, the Parliamentary Control Panel (PKGr) is informed about the declaration of intent (*Absichtserklärung*) drafted by the services before conducting international cooperation. This declaration of intent, which clearly identifies the objectives, scope, duration and specific guarantees of the cooperation, must be approved by the Federal Chancellery before the cooperation begins.[204] The DPA must also be heard before the establishment of any new databases that share intelligence data with foreign partners.[205]

"There is an accountability gap. You know that all oversight bodies are looking at their national services, no one is looking at how the cooperation of secret services as a whole works out. When our services send the information we look at the ways they apply the rules, we do not know what the other intelligence service will do with it, we always follow one end of the string and the other end is not known."

(Expert body)

Some interviewees critically noted the absence of regulation of international cooperation between intelligence services, both on national and international levels, and its impact on oversight. The exclusion of international cooperation from national legislation was also deemed an 'abnormal situation', an example of under-regulation, and as lacking a legal basis (e.g. 'the [national] framework is satisfactory but lacking an international dimension'). Respondents noted that it also prevents individuals from seeking remedies and reinforces an 'accountability gap' with regard to the use of collection techniques, purposes and use of data. Even when international cooperation is mentioned in national legislation, procedures governing international cooperation and the exchange of intelligence remains vague and unclear. Some respondents stated that international cooperation currently mostly involves bilateral agreements, and that such agreements are the most efficient option.

"It is not at all normal that international cooperation on intelligence is not included in the law. This cooperation not only exists but is desired by the executive. The law should therefore include this in order to enable political control and proportionality, including for reasons of national sovereignty, as this cooperation could lead to a transfer of sovereignty."

(Academia)

195 Latvia, Law on the State Secrets (*Par valsts noslēpumu*), 17 October 1997, Art. 9, para. 7.
196 Austria, International Police Cooperation Act (*Bundesgesetz über die internationale polizeiliche Kooperation, Polizeikooperationsgesetz - PolKG*), BGBl. I Nr. 104/1997, and, Austria, EU Police Cooperation Act (*Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), EU – Polizeikooperationsgesetz, EU-PolKG*), BGBl. I Nr. 132/2009.
197 Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*), 21 October 1997, Art. 34м.
198 Hungary, Act LIV of 2002 on the international cooperation of law enforcement bodies (*2002. évi LIV. törvény a bűnöldöző szervek nemzetközi együttműködéséről*), 1 April 2003.
199 United Kingdom, IPT, *Liberty & Others vs. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, para 53.
200 Germany, BNDG, S. 26-30. See Kutschbach, G. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1415 and following.
201 Belgium, Standing Committee I (2015), p. 24.
202 Luxembourg, CNPD, *Rapport Annuel 2015, pp.* 36-37.
203 Netherlands, CTIVD (2016a).
204 Germany, BNDG, S. 13 (5) and Germany, G10 Act, S. 7a (1).
205 Germany, BNDG, S. 28.

Oversight bodies have in academic publications[206] and at international conferences and public events raised the question of how to regulate international cooperation. For example, a representative of the Dutch oversight body addressed the absence of an international legal framework for international cooperation.

Regulating international cooperation

"And also on a national level [international cooperation] tends to be underregulated. Cooperation criteria are often unclear and there is no independent body involved in authorizing e.g. the exchange of personal data. Yet possible consequences can be far-reaching. Once data is exchanged, it is out of your hands. Foreign partners use your data for purposes you disagree of, e.g. illegal detention or targeting. The last years, secret services have intensified their international cooperation. The exchange of personal data takes place not only in bilateral contacts but increasingly also within a multilateral network, leading to databases and operational platforms. [...] Hence it is very important to start by setting national standards. And to allow national oversight bodies to assess this cooperation. [...] [R]elations between national oversight bodies are very important. Not only to exchange experience and views, but also to identify cross border issues and discuss findings in similar investigations. All within the existing legal mandates."

Bos-Ollermann, H. (2016)

206 Born, H., Leigh, I. and Wills, A. (2015).

6

Surveillance for a legitimate aim: need for 'national security' definition(s)



Article 8 (2) of the ECHR states that all interferences with the right to privacy should pursue a legitimate aim. It refers in particular to "national security, public safety or the economic wellbeing of the country". Article 52 (1) of the EU Charter of Fundamental Rights does not refer to specific aims, but states that "any limitation of the exercise of the rights and freedoms recognised by this Charter must [...] respect the essence of those rights and freedoms [...] and genuinely meet objectives of general interest recognised by the Union or protect the rights and freedom of others".

Well established ECtHR case law acknowledges that secret surveillance measures pursue the legitimate aims mentioned in Article 8 (2) of the ECHR, in particular 'national security'. As illustrated in *Roman Zakharov v. Russia*, the legitimate aim test does not create a major issue in the court's case law.

ECtHR case law: a legitimate aim

"[T]he Court considers it clear that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015, para. 237

Whether the measures at issue pursue a legitimate aim is rarely questioned by the ECtHR. According to the court, notions like national security – the protection of which is a primary aim of intelligence services – must therefore comply with the 'quality of law' requirements, in particular foreseeability/clarity of the law.

The ECtHR has held that it is difficult to precisely define the concept of national security. Yet, even broadly defined, and leaving a large margin of appreciation to Council of Europe Member States, in its case law, the court assigns to the notion of national security various concepts that need to have a factual basis.

It is clear from the examples listed in the box on ECtHR case law on national security that the latter goes beyond the protection of the territorial integrity of a state and protection of its democratic institutions – extending to major threats to public safety and including cyber-attacks on critical infrastructures. In some EU secondary legislation, 'national security' is explained as state security – for instance, in Article 15(1)

ECtHR case law: national security

Throughout its jurisprudence, the ECtHR has accepted, among others, as threats to national security:

- espionage (*Roman Zakharov v. Russia*, *Klass v. Germany*)
- terrorism (*Klass v. Germany*, *Weber v. Saravia*)
- incitement to/approval of terrorism (*Zana v. Turkey*)
- subversion of parliamentary democracy (*Leander v. Sweden*)
- separatist extremist organisations that threaten the unity or security of a state by violent or undemocratic means (*United Communist Party of Turkey v. Turkey*)
- inciting disaffection of military personnel (*Arrowsmith v. United Kingdom*)

Source: Born H. and Leigh I. (2005), p. 30; ECtHR (2013); updated by FRA, 2017

of the *e-Privacy Directive* 2002/58/EC. In other EU secondary legislation – for example, in Article 6(1)(d) of the *Admission of Third-Country Nationals for the Purposes of Studies Directive*[207] – 'national security' is referred to as 'public security'. The CJEU in *Fahimian v. Germany* stated that the concept of 'public security' covers both the internal security of a Member State and its external security.[208] Moreover, in *ZZ v. Secretary for the Home Department*, the CJEU implicitly held that the notion of state security as used in EU secondary legislation is equivalent to the notion of 'national security' as used in national law.[209]

The 2015 FRA report noted that the concept of national security is not used harmoniously across EU Member States.[210] In Luxembourg, the notion of 'national security' was inserted into the law reforming the intelligence services in 2016, to clarify the difference in the scope of missions of the police and intelligence services.[211]

"National security: all topics of fundamental interest for the stability of the country, unity of the country and safety of its citizens." (Parliamentary committee)

"It is not only military and political security, it is also increasingly infrastructure and economic and financial security. Threats can have a plurality of aspects. […] It includes security of technological infrastructures, cybercrime." (Parliamentary committee)

"The services do not have a monopoly on national security. Other services such as police, customs, etc., also have an essential role to play." (Expert body)

Respondents were asked how national security is defined in their respective legal framework or how it is understood in the context of intelligence. The responses reflected the legal terminology in each Member State and mainly referred to very broad concepts, as examples provided in the cited quotes show. Links were also made to international terrorism, organised crime and anti-democracy groups. Several respondents from expert bodies referred to their mandate as 'seeking the balance between national security and fundamental rights, privacy in particular'. Some of the respondents maintained that clearer definitions would help ('if not positive, at least negative'), including at EU level.

Defining national security: Luxembourg

"[W]e consider as activity which threatens or could threaten the national security or the above-mentioned interests, every activity, individual or collective, deployed domestically or from abroad,

a) which can be related to espionage, interference, terrorism, violent propensity extremism, proliferation of arms of mass destruction or of products linked to defence and technology related to defence, organised crime or cyber-threat to the extent that the latter two are linked to previously-mentioned activities, and

b) which is likely to endanger the independence and sovereignty of the State, the security and functioning of institutions, fundamental rights and civil liberties, the security of individuals and goods, the scientific and technical potential or the economic interests of the Grand Duchy of Luxembourg."

Luxembourg, Law of 5 July 2016, Art. 3(2) [FRA translation]

207 Council Directive 2004/114/EC of 13 December 2004 on the conditions of admission of third-country nationals for the purposes of studies, pupil exchange, unremunerated training or voluntary service, OJ 2004 L 375.

208 CJEU, C-544/15, *Sahar Fahimian v. Bundesrepublik Deutschland*, 4 April 2017, para. 39, C-145/09 *Tsakouridis*, 23 November 2010, paras. 43 and following and *C-601/15, N*, 15 February 2016, para. 66.

209 CJEU, C-300/11, *ZZ v. Secretary of the State of Home Department*, 4 June 2013, paras. 5, 11, 35, 38 and 54.

210 FRA (2015a), p. 24 and following. See also *ECtHR, Regner v. The Czech Republic [GC], No. 35289/11, 19 September 2017*, para. 67.

211 Luxembourg, Law of 5 July 2016 1. reorganising the State Intelligence Service; 2. modifying the Code of Criminal Procedure, the Law of 15 June 2004 regarding the classification of documents and security clearances and the Law of 25 March 2015 setting the regime for the compensation and the conditions for promotion of the State civil servants (Loi du 5 juillet 2016 1. portant réorganisation du Service de renseignement de l'État; 2. modifiant le Code d'instruction criminelle, la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, et- la loi du 25 mars 2015 fixant le régime des traitements et les conditions d'avancement des fonctionnaires de l'État), Art. 3.

PART II: ACCOUNTABILITY

KEY FINDINGS

A diverse oversight framework

- Oversight bodies have diverse roles, including overseeing the legality of the intelligence services' functioning, their efficiency, policies, and their finances.
- Oversight of surveillance measures is normally undertaken either by the judiciary or an expert body. In 16 Member States, expert bodies are involved in the oversight system, and in 17 Member States, judicial bodies are involved in oversight, generally at the stage of authorising targeted surveillance measures.
- Fieldwork interviews suggest that oversight by expert bodies contributes to the development and improvement of internal safeguards in intelligence services.
- In most Member States, parliaments are to some extent involved in all of these roles. In 21 Member States, one or two specialised parliamentary committees are involved in overseeing the intelligence services.
- In seven Member States, DPAs have the same powers over intelligence services as over all other data controllers. In 11 Member States, DPAs have no powers over intelligence services. In 10 Member States, their powers are limited.

Independence, sufficient resources and powers and public scrutiny

- **Independence:** all 28 Member States include at least one independent body in the oversight of intelligence services. Almost all respondents from oversight bodies confirmed that their institutions are independent, impartial, and resistant to any external influence, including by politicians and the intelligence services. However, some interviewees from civil society and academia questioned the oversight bodies' actual independence.
- **Resources and powers:** oversight bodies in all Member States that have detailed legal provisions on general surveillance of communications can initiate controls on their own initiative. All Member States also provide at least one of their oversight bodies with full access to all relevant data and information. The interviewed experts believe that full access to intelligence information is key to empowering oversight bodies and ensuring effective oversight. However, of the five Member States that have detailed provisions on general surveillance of communications, oversight bodies have some form of binding powers in only three. Representatives of different oversight bodies stated that lack of technical expertise remains one of the biggest challenges in oversight. In all seven Member States covered by FRA's fieldwork, oversight bodies may either include technical experts or can engage them on an ad hoc basis. The fieldwork findings show that the latter is rarely done in practice.
- **Public scrutiny:** in all the five Member States that have detailed provisions on general surveillance of communications, the oversight bodies issue annual reports. Interviewed experts indicated that enhanced transparency is vital.
- The respondents view public scrutiny and transparency as being closely linked with the accountability of oversight bodies. Civil society and academia representatives called for more transparency, deeming the content of issued reports uninformative.
- Respondents emphasised the importance of cooperation among the different national actors and across the different purposes of oversight, regardless of its nature (e.g. prescribed by law or informal exchanges). According to the interviewees, cooperation is vital for effective oversight; it strengthens its transparency and helps overcome possible fragmentation of oversight by contributing to its continuity. The respondents also expressed a great need for both national and international cooperation among oversight bodies.

Whistleblower protection

- Provisions on whistleblower protection are prescribed in the legislation of four of the seven Member States covered by FRA's fieldwork. Interviewees tended to agree that efficient whistleblower protection within the intelligence services requires a specific regime, different than those designed for other governmental institutions.

Continuous oversight

- Twenty-two Member States include an independent authority – judicial or expert – in the authorisation of the use of at least one type of targeted surveillance measure. In six Member States, all types of targeted surveillance measures may be implemented without ex ante oversight by an independent body.
- In the five Member States that have detailed provisions on general surveillance of communications, only three provide for the binding involvement of an independent body in the authorisation of these measures. In the two Member States that do not do so, the oversight bodies also do not have the power to make binding interventions.
- In all five Member States that have detailed provisions on general surveillance of communications, an independent body is tasked with providing for ongoing oversight (oversight of the implementation) of these measures.

Oversight of international intelligence cooperation

- A majority of Member States – 17 out of 28 – do not prescribe oversight of international cooperation among intelligence services. Of the 11 EU Member States that do provide for oversight of such international cooperation in law, three have excluded information originating from foreign services from the scope of oversight; four do not differentiate between the oversight regime for international sharing of data and for domestic sharing of data; and four have limited the scope of the control over information obtained through such cooperation.
- The specific characteristics of international intelligence sharing require Member States to establish safeguards tailored thereto, notably:
  - prior approval of any agreement by the executive (currently in force in 27 Member States),
  - complementary approval by either the executive or the head of the services before the exchange may take place (currently in force in 4 Member States),
  - an assessment of fundamental rights anchorage (currently required in the laws of 3 Member States) or of the existence of equivalent data protection legislation (currently conducted in 2 Member States), and
  - data reliability assessments and the obligation to keep records (currently mandatory in 4 Member States).
- The dominant principle in international cooperation – the 'third party rule' – states that a foreign agency to which intelligence has been transmitted can neither share this information with a third party nor use the data for an objective different from the one for which the exchange was established in the first place. When considered to be third parties, expert bodies are not authorised to access – and therefore, oversee – intelligence data obtained via international cooperation. In some Member States, oversight bodies are increasingly not considered to be 'third parties'.

7 An imperative: control from within



Control v. Oversight

"Oversight should be distinguished from control because the latter term (like management) implies the power to direct an organization's policies and activities. Thus, control is typically associated with the executive branch of government and specifically with the senior management of intelligence services. An example of control, as opposed to oversight, would be the issuance of an executive order requiring an intelligence service to adopt a new priority in international intelligence cooperation, such as counterterrorism."

Born, H., Leigh, I. and Wills, A. (2015), pp. 6-7

The following section describes how controls within the services and by the executive contribute to the services' accountability.

7.1. Control by the services

UN good practices on intelligence services management of personal data

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

As the UN Special Rapporteur on the right to privacy has highlighted, a mechanism enforcing accountability "needs to be embedded first and foremost within the authorities carrying out surveillance and it needs to be clear who is accountable for compliance".[212] Internal controls within the services may be undertaken by a designated officer or sector, who may be appointed by the services or the executive, and report to them as well. The 2015 FRA report described the situation in various Member States.[213]

In Germany, the NSA inquiry committee's report provides a detailed description of the powers of the data protection officer within the BND. The report highlights the impact of the Snowden revelations on her work. Interestingly, given the lack of awareness on data protection in the technical intelligence department of the BND, the data protection officer launched a project to raise awareness among the staff.[214] The 2016 amendments to the BND Law prescribe specific data protection rules on when collected foreign data need to be destroyed and how long they can be kept.[215] Similarly, in the United Kingdom, GCHQ's staff are continuously instructed and trained in the legal and other requirements of the surveillance legislation, with particular emphasis on human rights requirements. Additionally, there are computerised systems for checking and searching for potentially non-compliant uses of GCHQ's systems and premises.[216] For example, when an authorised person selects a particular communication for examination, this person must demonstrate that the selection is necessary and proportionate; this process is subject to internal audit.[217]

212 UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci, para. 35.

213 See FRA (2015a), p. 30 and following.
214 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 526 and following.
215 Germany, BNDG, S. 10 and 12. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1271 and following.
216 United Kingdom, IOCCO (2016a), p. 26.
217 United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', February 2017, s. 6.14.

FRA was not able to interview any intelligence service representatives during its fieldwork.[218] However, other research participants – mostly representatives of oversight bodies, but also from the executive – discussed examples of control practices implemented by intelligence services. They mainly argued that expert body oversight contributes to the development or improvement of internal safeguards within the intelligence services to act lawfully. The relationships with the services were described as 'cooperative and not adversarial'. For example, intelligence services ask oversight bodies to be present in certain situations, such as to witness data destruction. The services also sometimes share material that might not be directly related to the specific oversight function but could still be relevant for the oversight bodies. Respondents also noted that oversight helps 'to ensure the greater legitimacy of the records held', and emphasised the importance of internal controls through 'a strong legal department within the services'. They viewed the abovementioned practices as contributing to the clarity and, thus, the legitimacy of the intelligence services.

"We also say how important it is for services to have a strong legal department within the services. It is not only for the outsider to be critical, but for inside." (Expert body)

"Also, 'behind the scene' we are doing a lot for fundamental rights, and 'behind the scene' we are helping the agencies to improve their practices, pointing to the issues that we consider disproportionate, unnecessary etc." (Expert body)

7.2. Control by the executive

Strictly speaking, control by the executive is not part of the oversight system because it is not independent. However, the nature of the involvement of the superintending governmental department concerned – whether Chancellery, Foreign, Interior or Defence Ministry – contributes greatly to the effectiveness of intelligence services' accountability systems. The intelligence services are part of the public administration and, as for every administration and public service, effective control stems from the government itself.

The relevant governmental departments can supervise intelligence services in a variety of ways: by establishing their policies, priorities or guidelines; by nominating and/or appointing the service's senior management; by formulating the budget that parliament will ultimately vote on; by authorising or approving specific surveillance measures; or by approving cooperation with other services. As a former director of the French intelligence service (DGSE) puts it: "political control is, first of all, [...] hierarchical control because the services do not work in vacuum but under the authority of the executive".[219]

In the United Kingdom, the intelligence agencies operate by law under the authority of the Secretary of State (for Foreign Affairs for the Secret Intelligence Service and GCHQ, and for Home Affairs for the Security Service), supported by dedicated teams of policy officials with full access to the work of the agencies. In the Cabinet Office, the National Security Secretariat coordinates policies – for example, towards overseas liaisons – and prepares and scrutinises budgets; the Joint Intelligence Committee provides strategic intelligence assessments and recommends intelligence priorities.

In France, a June 2017 reform changed intelligence coordination within the executive. The National Intelligence Council (*Conseil national du renseignement*) has the specific mandate of setting strategies and priorities for the services. It includes the president and the prime minister, ministers, the heads of specialised services if required by the agenda, and the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*). The coordinator is responsible for coordinating the actions of the intelligence services and ensuring efficient cooperation among them. The coordinator also transmits and checks the implementation of the president's instructions to the relevant ministers. Additionally, the coordinator coordinates and develops the initiatives taken by France concerning European and international cooperation in the fields of intelligence and the fight against terrorism. The coordinator proposes to the president the intelligence priorities in the fight against terrorism.[220]

In Germany, the reform of 2016 did not change the Federal Chancellery's supervising role over the work of the federal intelligence service (BND) or the coordinating role over the work of the federal intelligence services.[221] The NSA inquiry committee assessed the Federal Chancellery's capacities when controlling the BND. It supported the views of the PKGr calling for adjusting the Federal Chancellery's supervisory control to allow it to properly perform its controlling tasks.[222] In the meantime, the Federal Chancellery staff has significantly increased to take into account the request adjustments. Still the following quote by a Federal

218 The section on social fieldwork methodology in Annex 1 presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

219 France, DPR & CNCTR (2017), p. 14 [FRA translation].

220 France, Defence Code (*Code de la défense*), Art. R.* 1122-7, Art. R.* 1122-8 and Art R.* 1122-8-1.

221 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 536 and following.

222 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1243.

Chancellery staff member nicely illustrates the issues faced by all controllers.

The need to be selective when controlling

"We certainly often also became proactive. But we are, of course, as you rightly point out, as an entity that conducts legality reviews with relatively few employees at the Federal Chancellery trying to accompany a huge authority in terms of administrative and specialised control, not in a position to follow all processes in all departments down to the last detail. We always need and needed to concentrate on key areas."

Germany, Federal Parliament (Deutscher Bundestag) *(2017b), p. 1243 [FRA translation]*

In the Netherlands, the Minister of the Interior, the Minister of Defence and the Minister of General Affairs (the prime minister) are in charge of appointing the coordinator for the intelligence services. The prime minister instructs the coordinator, in agreement with the Minister of the Interior and the Minister of Defence.[223] The coordinator chairs a special committee on the intelligence services composed of representatives of relevant ministries.[224] The heads of the services are under obligation to cooperate with the coordinator.[225] The Minister of Interior reports to parliament annually regarding the work of the AIVD.[226]

In Belgium, the Minister of Justice appoints the head of the service, officers to certain posts, and the internal administrative control. The minister is also in charge of the expenses and discipline of the services.[227]

The 2015 FRA report highlighted the executive's crucial role in authorising/approving surveillance measures in most Member States.[228] In the United Kingdom, officials in the Home Office and Foreign Office scrutinise applications for warrants from their agencies and obtain their own legal advice before submitting advice on the applications to their Secretary of State. In France, members of the executive other than the president of the republic or prime minister may also exercise control over the intelligence services. Furthermore, a 2017 decree specifies that the heads of the intelligence services communicate to the national intelligence and fight against terrorism coordinator the intelligence to be brought to the attention of the prime minister and the president of the republic.[229] The prime minister may hold the services accountable via the Inspectorate of Intelligence Services, whose members the prime minister may appoint from among the personnel of existing inspectorates. This body is in charge of monitoring, auditing, researching, consulting, and assessing the intelligence services, and reports back to the prime minister.[230] While the inspectorate's powers were extended recently, the French parliamentary oversight committee is calling for its further strengthening.[231]

FRA's fieldwork included interviews with representatives of executive control bodies in three Member States (France, Germany, and Sweden). The interviewees described their roles as involving 'internal control in the services' – for example, that procedures and provisions are implemented properly; supervisory functions; acting as advisory to the government; and coordinating the services – for example, facilitating sharing of information between agencies and between government and the services. The experts said that, alongside their main supervisory role, they performed audit or advisory functions. Some said that they supplemented the general oversight system. They noted that they addressed matters as directed by the government, but also exercised their power to take up specific matters on their own initiative.

"The strength of the [national] system is having an independent person who says what is doable and what is not, and the government which decides in fine." (Expert body)

While executive control plays an intrinsic role and should always be informed about the work of the services, it may not have a strong interest in revealing failures that occur due to the potential political costs.[232] Therefore, for accountability mechanisms to provide public reassurance, they must include independent oversight, as well. Control led by the executive is in fact a pre-condition for setting up efficient oversight frameworks – as described in the following section.

223 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) Art. 4.
224 *Ibid.* Art. 5.
225 *Ibid.* Art. 7.
226 *Ibid.* Art. 12
227 Belgium, Organic Law on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, Arts. 4 and 5.
228 FRA (2015a), p. 32.
229 France, Defence Code (*Code de la défense*), Article R.* 1122-8-1.
230 France, Decree No. 2014-833 on the Inspectorate of intelligence services (*Décret n°2014-833 relatif à l'inspection des services de renseignement*), 24 July 2014. See also France, DPR & CNCTR (2017), p. 24.
231 See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 24.
232 Born, H. and Wills, A. (eds.) (2012), p. 10.

8 Oversight framework of intelligence services



UN good practices on oversight institutions

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

To fulfil their mandate, intelligence services need to act in secret and often to use methods that will involve access to personal data and intrude upon personal privacy. In democratic states, this also means the protection of an *open society* through the use of *secret tools*. "It is because of this paradox [...], that the security and intelligence services should be the object of democratic accountability and civilian control".[233] Oversight of intelligence services is one of the conditions of the services' legitimacy.[234]

The oversight on intelligence services is organised in extremely diverse ways in EU Member States. A single model would be an impossible objective because national oversight frameworks have to directly link to the political institutions and administrative and judicial organisation of each Member State.[235] Table 1 is based on a model developed by Cousseran and Hayez and adapted by FRA for comparative analysis purposes. It highlights that effective oversight requires a multiplicity of actors assessing a variety of aspects. However, the essential requirement of an effective oversight framework is that it is comprehensive. Comprehensive oversight requires the oversight of all aspects of the services' work, of which surveillance operations are but one element.

233 Born, H. and Leigh, I. (2005), p. 16. See also France, DPR & CNCTR (2017), p. 2.
234 Cousseran, J.-C. and Hayez, P. (2015), p. 288.
235 See Cousseran, J.-C. and Hayez, P. (2015), p. 291.

Table 1: Oversight framework: main actors and scope of control

Who?/What?	Efficiency	Legality	Policy / specific threats	Fundamental rights protection	Financial integrity and rigour
Parliament	Oversight committee	Oversight committee	Oversight committee & Inquiry commission	Inquiry commission	Financial Commission
Judge	-	Yes	-	Yes	Supreme Court of Auditors
Independent bodies	Expert bodies and State Secrets control body	Expert bodies	Expert bodies	Expert bodies, DPA, ombuds institutions	Special bodies
Watchdogs	Yes		Yes	Yes	Yes

Notes: *The red line indicates the focus of FRA's research.*

Source: *Cousseran, J.-C. and Hayez, P. (2015), p. 292; adapted by FRA, 2017*

8.1. Diversity of oversight mandates

Table 1 shows that the different oversight bodies within an oversight framework have varying purposes, with individual actors focusing on different aspects of the services' functioning. Actors with specifically limited mandates, such as supreme audit institutions, focus on a single task. Others' mandate requires them to undertake broader oversight and assess different aspects. Coordination is therefore needed.

FRA's research focused on two main aspects: legality – a core task of expert bodies – and fundamental rights protection. The review of intelligence policies is indirectly covered, as well. This report does not address the supervision of intelligence services' efficiency, given that this is only indirectly related to fundamental rights safeguards and would require data on surveillance techniques that are confidential. Similarly, this report does not analyse the role of supreme audit institutions, although these are very important for ensuring the financial integrity of, and rigour regarding, public money expenditures.[236]

Scrutinising intelligence services' finances

The Swedish National Audit Office (*Riksrevisionen*), mandated by parliament to audit all state finances, issued a report in 2015 on 'the control of the defence intelligence operations'. The 64-page document addresses four overarching questions: 1) has the government created preconditions for effective control?; 2) is the control conducted effectively?; 3) are the findings of the control reported to the controlled entities and the government?; and 4) are issues raised by the controlling authorities acted upon?

While the assessment is generally positive, it also calls for some improvements. For instance, the report states that the State Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) should be more explicit in its communications with controlled agencies on needed changes and also better document its control methodologies.

Swedish National Audit Office (2015), 'The control of the defence intelligence operations'

In terms of financial supervision over intelligence services, for example, in Germany and France, parliaments adopted original solutions to supervise the services' expenditures in addition to the specialised budget commissions and the Federal Court of Auditors (*Bundesrechnungshof*) and the French Court of Auditors (*Cour des comptes*), respectively.

236 For more information on SAIs, see, for example: Born, H. and Wills, A. (eds.) (2012), pp. 166-175.

The vast majority of specialised parliamentary committees have an ex post say on the effectiveness of budget allocations. Germany, exceptionally, has a separate parliamentary committee in charge of the budget – the Trust Panel (*Vertrauensgremium*), which decides intelligence services' budget and on investment in surveillance technologies. Three Trust Panel members participate in the meetings of the PKGr and three of the members of the PKGr participate in the deliberations of the Trust Panel.[237] The French parliamentary oversight body DPR oversees the expenses of the intelligence services through an annual report prepared by the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*)[238] and through the annual report by the Audit Commission on special funds (*Commission de vérification des fonds spéciaux*), which is composed of four members of the DPR.[239]

8.2. Diversity of actors

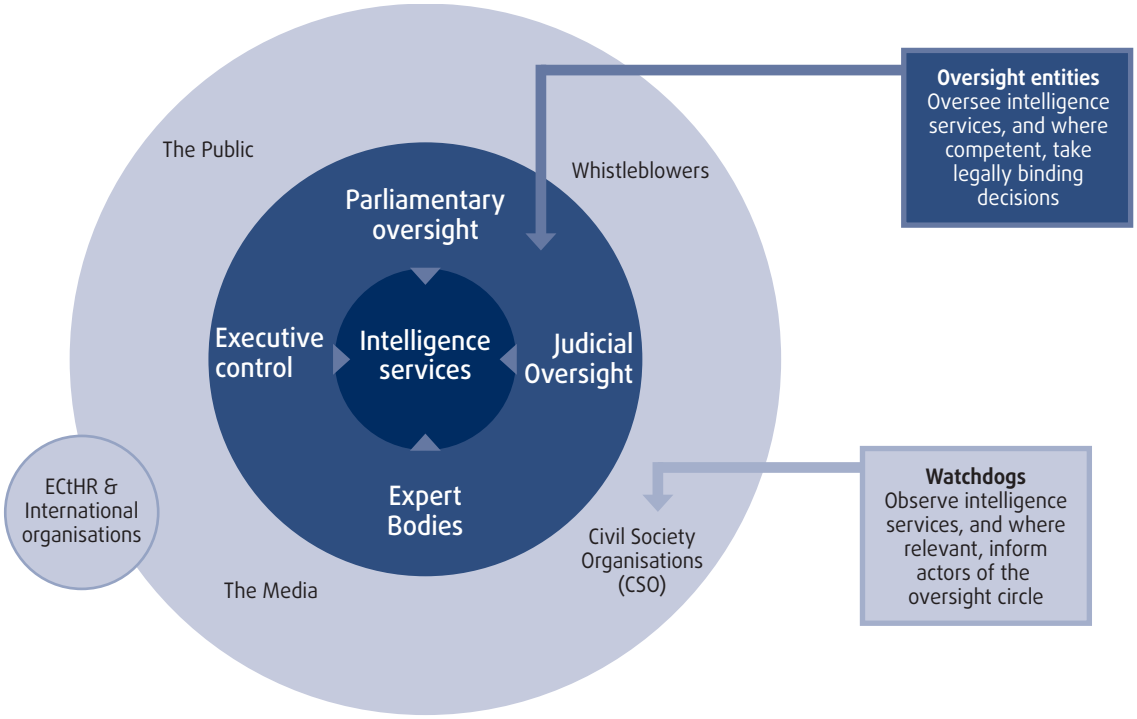
UN standards for oversight bodies

"(E)stablish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."

UN, GA (2016a), Resolutions on the right to privacy in the digital age, *21 November 2016, para. 5(d)*

The following sections introduce the main actors who contribute to the oversight of intelligence services and their accountability (Figure 5): parliaments; expert bodies; and several actors that perform important watchdog functions in democratic societies: media, ombuds institutions, national human rights institutions, civil society organisations and whistleblowers. (Data protection authorities, which are treated as a type of expert body for purposes of this report, are discussed in Section 9.2.)

Figure 5: Intelligence services' accountability scheme



Source: FRA, 2017

237 Germany, Federal Budget Order (Bundeshaushaltsordnung), 19 August 1969, as amended, s. 10 (a); and Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, s. 9. See also de With, H. and Kathmann, E., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 225.

238 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 22.

239 *Ibid.* p. 83.

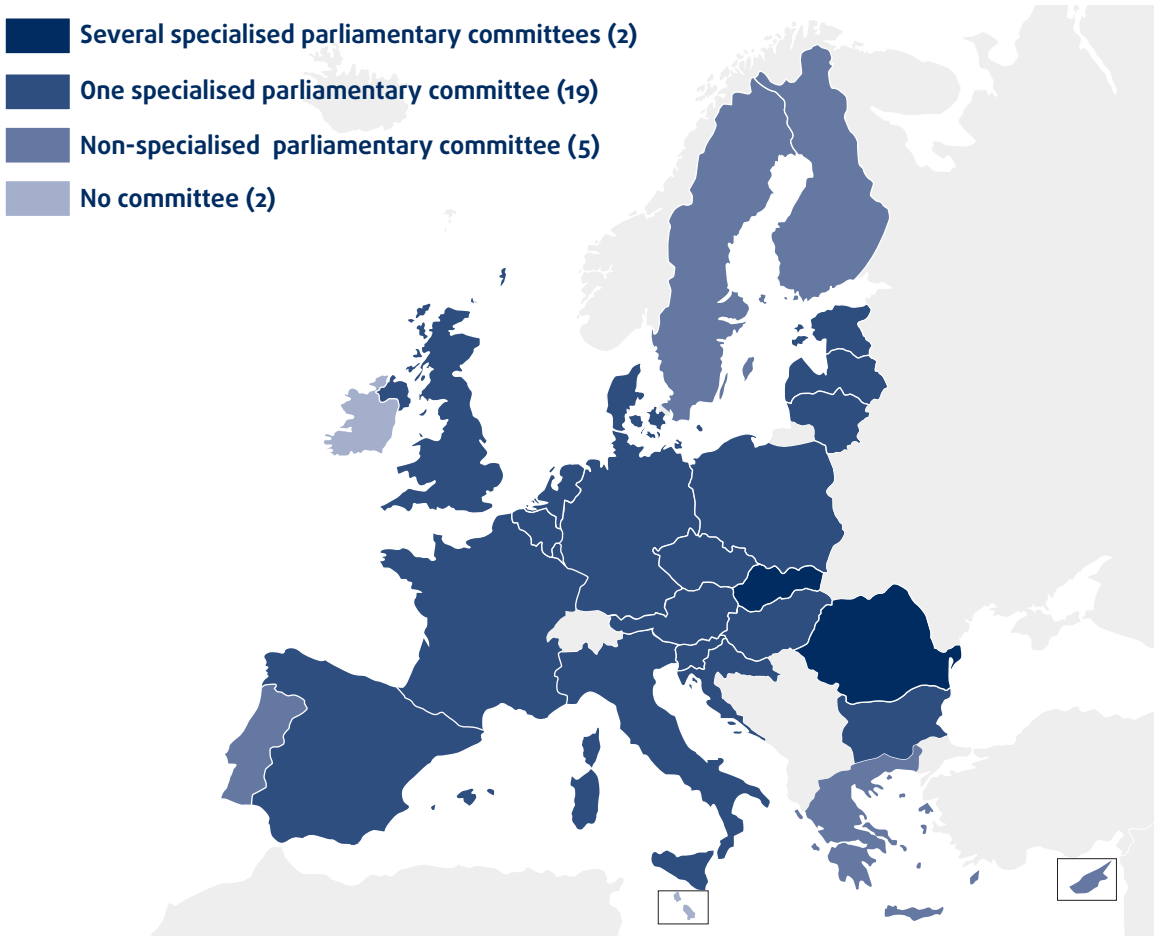
8.3. Parliaments

Parliament has the "supreme responsibility to hold the government accountable".[240] As lawmaker, it is responsible for enacting clear, accessible legislation and establishing the intelligence services and their organisation, special powers and limitations. It also approves the intelligence services' budget and plays a strong role in scrutinising whether their operations are in line with the laws they set out.

As illustrated in Figure 6, 26 EU Member States – all except for Ireland and Malta – provide for parliamentary oversight.[241] In 21 of these, special parliamentary committees oversee the intelligence services. The Venice Commission recommends setting up one parliamentary committee to deal with the various security and intelligence services, since this allows the committee to carry out more far-reaching oversight and to "cross agency boundaries".[242]

In Germany, on 7 December 2016, the Act on the Further Development of Parliamentary Oversight of the Federal Intelligence Services (*Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes*) came into force, amending the Parliamentary Control Panel Act (*Kontrollgremiumgesetz,* PKGrG). It established the office of the Permanent Representative (*Ständiger Bevollmächtigter*), with the task of supporting the regular work and specific investigations of the Control Panel and the Trust Panel.[243] The Permanent

Figure 6: Parliamentary oversight of intelligence services in EU Member States



Source: FRA, 2017

240 Born, H. (2003), p. 36.

241 In Malta, the law establishes a Security Committee, which consists of the Prime Minister, the Minister, the Minister responsible for Foreign Affairs and the leader of the opposition. While introducing a parliamentary aspect, this body seems closer to an executive body. See Malta, Security Service Act 1996, Art. 14 and Schedule 2.

242 Venice Commission (2007), p. 33.

243 Germany, PKGrG, S. 5a. See Bartodziej, P. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1583 and following.

Representative participates in all meetings of the Control Panel, Trust Panel and G10 Commission. These provide the office with a source of information that the member of these bodies do not have. The Permanent Representative supervises the staff working for the Control Panel and the G10 Commission.

"Oversight is not lack of trust, but willingness to clarify."

(Parliamentary committee)

Sweden does not have a specialised parliamentary committee to oversee its intelligence services. The work of the intelligence services does, however, fall within the remit of two standing committees within the parliament: the Committee on Justice and the Committee on Defence. The government must present annual reports to the parliament on the protection of individual persons' integrity in relation to defence signals intelligence activities. These annual reports are reviewed by the Parliamentary Committee of Defence *(Försvarsutskottet)* before it is accepted by parliament.[244] The Committee on the Constitution is also relevant in this context as it is responsible for the areas of fundamental rights, data protection and privacy.[245]

8.4. Expert bodies

Table 2 lists the various expert oversight bodies established in the Member States. It does not include DPAs, but only the bodies specialised in intelligence matters. Across the EU, 16 Member States have set up one or more expert bodies exclusively dedicated to intelligence service oversight.

All five Member States with detailed laws on general surveillance of communications have established one or more expert bodies to oversee this capacity of the intelligence services. However, their mandates are not always comparable. The 2015 FRA report describes their powers.[246] The following paragraph focuses on changes since 2015.

In the Netherlands, the 2017 reform splits the existing CTIVD into two sub-committees: one performing general oversight by conducting investigations and another handling complaints lodged by individuals. The general oversight sub-committee consists of three members, including the chair (also chair of the entire CTIVD), nominated by the responsible ministers for 6 years with once-renewable mandate. The complaints-handling sub-committee consists of a chair and two additional members. At least two of the members of CTIVD the general sub-committee and all members of the complaints sub-committee of the must hold a master's or doctoral degree in law.[247] Currently, the CTIVD is assisted in its work by a staff of 12 persons: the secretary to the Committee, eight review officers, one IT expert and two secretaries,[248] but the Committee will receive an increased budget to be able to implement the new legislation.[249]

In the United Kingdom, the Investigatory Powers Commissioner and the Judicial Commissioners must hold or have held a high judicial office.[250] The number of staff provided to the Judicial Commissioners is subject to the approval of the Treasury, and is provided by the Secretary of State.[251] The Investigatory Powers Commissioner's Office will consist of around 70 staff. This will be made up of around 15 Judicial Commissioners, current and recently retired High Court, Court of Appeal and Supreme Court Judges; a Technical Advisory Panel, of scientific experts; and almost 50 official staff, including inspectors, lawyers and communications experts.[252]

The Investigatory Powers Commissioner has already secured access to in-house legal advice and identified independent standing counsel to facilitate performing his functions, in line with an agreement made with the UK government when the body was set up. The commissioner will have the flexibility to 'buy in' whatever advice he needs at any given time.[253]

In Germany, the G10 Commission carries out expert oversight for matters relating to targeted surveillance and strategic surveillance under the G10 Law. The G10 Commission is supported by the same secretariat (13 persons in 2016) that works for the Parliamentary Control Panel. With the reform of the PKGrG in 2016, the secretariat, under the management of the Permanent Representative, will be strengthened.[254] The reform of the BND Law on foreign-foreign surveillance established a new body in charge of approving such surveillance measures: the Independent Committee (*Unabhängiges Gremium*).[255] At the time of writing, the Independent Committee was not yet operational, although its members have been appointed, five supporting staff

244 Sweden, Parliamentary communication (Riksdagsskrivelse 2007/08:266) on the Government Bill "Adaptation of Defence Intelligence Activities" (Proposition 2006/07:63, En anpassad försvarsunderrättelseverkamhet), 8 March 2007.
245 Sweden, Parliament, The 15 parliamentary committees.
246 FRA (2015a), p. 41 and following.
247 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97-99.
248 The Netherlands, CTIVD (2017), p. 35, and CTIVD, webpage on members and staff.
249 The Netherlands, General States (*Staten-Generaal*) (2017), Parliamentary Document 34588, Nr. 67, 2 May 2017.
250 United Kingdom, Investigatory Powers Act, s. 227 (2).
251 *Ibid.* s. 238 (2).
252 United Kingdom, IPCO website.
253 United Kingdom, House of Lords (2016), Transcripts of debate on Investigatory Powers Bill, 17 October 2016, Volume 774, Column 2170.
254 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1319.
255 Germany, BNDG, S. 16.

Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU

EU Member State	Expert Bodies
AT	Legal Protection Commissioner (*Rechtsschutzbeauftragter)*
BE	Standing Intelligence Agencies Review Committee (*Vast Comité van Toezicht op de inlichtingen - en veiligheidsdiensten/Comité permanent de Contrôle des services de renseignement et de sécurité*) Administrative Commission (*Bestuurlijke Commissie/Commission Administrative*)
BG	National Bureau for Control over Special Intelligence Means (*Национално бюро за контрол на специалните разузнавателни средства*)
CY	Three-Member Committee (*Τριμελής Επιτροπή*) [Not yet in place]
CZ	N.A.
DE	G 10 Commission (*G 10-Kommission*) Independent Committee (*Unabhängiges Gremium*)
DK	The Danish Intelligence Oversight Board (*Tilsynet med Efterretningstjenesterne*)
EE	N.A.
EL	Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*)
ES	N.A.
FI	N.A.
FR	National Commission for Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*) Council of State special formation
HR	Council for Civilian Oversight of Security and Intelligence Services *(Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*)
HU	N.A.
IE	Complaints Referee
IT	N.A.
LT	N.A.
LU	Supervisory committee (*autorité de contrôle*) of Act of 2 August 2002 Commission (*commission*) of the Criminal Investigation Code (*Code d'Instruction Criminelle*)
LV	N.A.
MT	Commissioner of the Security Service *(Kummissarju tas-Servizz ta' Sigurtà)*
NL	The Review Committee on the Intelligence and Security Services *(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)*
PL	N.A.
PT	Council for the Oversight of the Intelligence System of the Portuguese Republic (*Conselho de Fiscalização do Sistema de Informações da República Portuguesa*)
RO	N.A.
SE	Swedish Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten*) Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden*) Defence Intelligence Court (*Försvarsunderrättelsedomstolen*)
SI	N.A.
SK	N.A.
UK *	Investigatory Powers Commissioner

Notes: *N.A. = not applicable (no expert body exists)*

** On September 1 2017, the Investigatory Powers Commissioner took over from the former Intelligence Service Commissioner and Interceptions of Communications Commissioner..*

Source: *FRA, 2017*

members have been hired and trained for the secretariat, rules of procedure prepared and secure facilities set up.[256]

For the purpose of this report, DPAs are considered to be oversight expert bodies. They are specialised bodies that have been specifically tasked with safeguarding privacy and data protection in EU Member States. The Court of Justice of the European Union (CJEU) has held in a series of judgments that supervision by DPAs is an essential

256 Lorenz, P. (2017), 'BND-Kontrolle am BHG: Unabhängiges Gremium nimmt Arbeit auf', *Legal Tribune Online*, 9 March 2017; and Dreusicke, L. (2017), 'Präsidentin des BGH in Osnabrück: Wer das Ausspähen des BND kontrollieren soll', *Osnabrücker Zeitung*, 27 April 2017.

component of the right to personal data protection.[257] Their powers and competences are analysed in Section 9.2.

8.5. Watchdogs

Other actors also substantially contribute to ensuring the effectiveness of existing safeguards. These include national human rights institutions, civil society actors – including the media, academia[258] and NGOs – and whistleblowers.

NGOs have launched lawsuits in various EU Member States, promoted reforms,[259] developed international principles applicable to oversight of intelligence services,[260] and have acted as watchdogs of legislative processes.[261] Consequently, it is important to support and respect their roles so that they can contribute to improving the oversight of intelligence matters. The same is true about national human rights institutions (NHRIs).[262] In France, for example, the French NHRI in 2015 contributed to the legislative reform regarding surveillance measures and their oversight by providing parliament with various opinions on different laws relating to intelligence and counter-terrorism.[263] The German NHRI submitted written opinions on relevant issues for parliamentary hearings, including the one on the BND reform in 2016.[264] However, NHRIs' opinions are not sought systematically in this area.[265]

257 See in particular CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014, para. 68; CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 41 and 66. See also Working Group on Data Protection in Telecommunications (2017).

258 University of Amsterdam (2015), *Ten standards for oversight and transparency of national intelligence services*, IViR (Institute for Information Law, University of Amsterdam). See also the various projects funded by the European Union under the FP7 and now the Horizon 2020 programme.

259 See, for example, Löning, M. (2015); Brown, I. *et al.* (2015). See also the strategic litigation, advocacy, capacity building and reporting undertaken by Privacy International.

260 See Forcese, C. and LaViolette, N. (2006), Ottawa Principles on Anti-terrorism and Human Rights; Open Society Justice Initiative (2013), Global Principles on National Security and the Right to Information (Tshwane Principles); and Access *et al.* (2014), International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles).

261 See, for example, ECtHR, *Youth initiative for human rights v. Serbia*, No. 48135/06, 25 June 2013. The Serbian intelligence agency denied the applicant NGO information on the number of people subjected to electronic surveillance by the agency, despite an Information Commissioner order supporting the NGO's request. The ECtHR found a violation of freedom of expression, acknowledging the NGO's role in a debate of public interest (para. 24); Bits of Freedom, a NGO, a digital rights organisation in the Netherlands closely follows the legal reforms.

262 Council of Europe, Commissioner for Human Rights (2016).

263 See France, Commission Nationale Consultative des Droits de l'Homme (2015); France, Commission Nationale Consultative des Droits de l'Homme (2016); France, Commission Nationale Consultative des Droits de l'Homme (2017a); France, Commission Nationale Consultative des Droits de l'Homme (2017b). See also France, Défenseur des Droits (2017).

264 Germany, Deutsches Institut für Menschenrechte (2016)

265 France, Le Monde (2017).

Protecting fundamental rights via strategic litigation

In **France**, in 2017, the NGOs *La Quadrature du Net*, French Data Network and *Fédération des fournisseurs d'accès à internet associatifs* filed a 'priority preliminary ruling on constitutionality' (*Question Prioritaire de Constitutionalité,* QPC) with the Council of State related to the access of intelligence services to metadata retained by telecommunication providers. The Council of State referred the case to the Constitutional Court. The Constitutional Court decided on 4 August 2017 that the four-month authorisation the intelligence services can obtain to access metadata of a targeted suspect complies with the constitution. However, the Constitutional Court declared unconstitutional the extension of the same authorisation to access metadata of the suspect's entourage.

France, Constitutional Court, Decision n. 2017-648 QPC, 4 August 2017

In **France**, in 2016, four associations – *La Quadrature du Net*, *FDN*, *Fédération des fournisseurs d'accès à Internet associatifs* and *igwan.net* – filed a QPC with the Council of State, on the grounds that radio surveillance was not subject to any procedural safeguards. The Council of State referred the matter to the Constitutional Court, which held – in October 2016 – that the legal provision allowing for radio surveillance was contrary to the French constitution. As a result, Article L.811-5 of the Internal Security Code was repealed; this will take effect on 31 December 2017.

France, Constitutional Court, Decision n. 2016-590 QPC, 21 October 2016

In 2015, **United Kingdom**-based Privacy International started a legal challenge in the Investigatory Powers Tribunal (IPT), about whether the acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets (BPD) and Bulk Communications Data (BCD) is in accordance with the law or necessary and proportionate. In 2016, the IPT ruled that obtaining BPD and BCD, before doing so was publicly acknowledged, violated the right to private life, by virtue of the lack of foreseeability to the public and the lack of adequate oversight. However, the IPT accepted that, following public acknowledgment of the use of these powers, the changes made to oversight powers and the publication of the relevant procedures, the powers were compatible with the right to private life. The case was referred to the CJEU for matters relating to EU law.

United Kingdom, Investigatory Powers Tribunal, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, *IPT/15/110/CH, 17 October 2016 and 8 September 2017*

In 2014, Privacy International brought an action before the IPT, challenging the compliance of GCHQ's Computer Network Exploitation (CNE) – colloquially, 'hacking' – with domestic law and the right to private life (Article 8 of the ECHR) and freedom of expression (Article 10 of the ECHR). In 2016, the IPT ruled that CNE activities can in principle be lawful. The tribunal considered and gave guidance on how a warrant allowing for CNE activity would have to describe the potentially intercepted equipment. The IPT concluded that warrants compliant with such guidance would be lawful both under domestic law and the ECHR.

United Kingdom, Investigatory Powers Tribunal, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, *IPT/14/85/CH 14/120-126/CH, 12 February 2016*

In 2013, the **German** branch of Reporters without Borders (RWB) brought an action against BND's strategic surveillance of international communications. RWB argued that both the interception of communications itself and the collection, storage and analysis of metadata violated their privacy. In 2016, the Federal Administrative Court decided that there was no privacy violation because, even if the NGO's communications had been under surveillance, BND deleted them immediately and such act could not be traced. In 2017, the case was brought before the Federal Constitutional Court challenging, among others, the lack of remedies in case of strategic surveillance.

Germany, Federal Administrative Court (Bundesverwaltungsgericht), *BVerwG 6 A 7.14, 15 June 2016*

During fieldwork interviews, all respondents were asked to describe cooperation efforts between their institutions and the other main actors in their country, including civil society organisations. The findings show that cooperation is least developed with civil society organisations (in comparison with other institutional bodies) and mainly takes the form of ad hoc exchanges or consultations. Few entities within the Member States researched have established contacts with civil society organisations or take advantage of certain networks operating domestically – such as the Belgian Human Rights Platform, established in January 2015, which brings together all institutions with human rights protection mandates, including the Standing Committee I. In Croatia, civil society participates in the Council for Civilian Oversight of Security and Intelligence Services, which exercises part of the oversight of the operations of intelligence services and their legality.[266] However, in the remaining Member States, many respondents suggested there was room for future developments and closer cooperation. The work of civil society is most appreciated by national human rights institutions, ombuds institutions, lawyers and academics for their professionalism, strategic litigation, provision of amicus curiae briefs, opinions on draft laws, participation in public consultations and provision of legal advice for individuals who seek remedies in case of violations.

The media unquestionably play a substantial role in generating or steering public debate during legal reforms. They also played a crucial role in publishing some of the US National Security Agency material exposed by Edward Snowden, informing the broader public about the existence and some of the functioning programmes of general surveillance of communications. Interviewed oversight body representatives in Italy, the Netherlands and Sweden noted that some of their investigations were triggered by media attention to certain issues. At the same time, in relation to trust-based cooperation, expert body representatives tended to cite reports or leaks of information, e.g. to the media, as undermining their relationship with the intelligence services.

As further analysed in Section 10.3, media professionals might be less willing to conduct in-depth investigative reporting on intelligence services if the confidentiality of their sources is not assured by enhanced safeguards against surveillance.

ECtHR case law: whistleblowers

"[A] civil servant, in the course of his work, may become aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest. The Court thus considers that the signalling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. [...] In the light of the duty of discretion referred to above, disclosure should be made in the first place to the person's superior or other competent authority or body. It is only where this is clearly impracticable that the information could, as a last resort, be disclosed to the public [...]."

ECtHR, Guja v. Moldova [GC], No. 14277/04, 12 February 2008, paras. 72-73

The 2015 FRA report highlighted the importance of whistleblowers.[267] Staff within intelligence services may want to raise concerns about the legality of activities witnessed within their agency. This can be achieved by means of internal controls such as ethics commissioners or staff counsellors, to whom staff can turn in confidence if they have anxieties relating to the work of their service; and through whistleblower provisions, which allow staff to feel secure when reporting wrongdoing. Ethics counsellors, journalists and whistleblowers thus can also play an essential 'intermediary' role in alerting executive and oversight bodies to issues that require investigation. The Snowden revelations provide a good example of this since they led to both national and international litigation.[268]

266 Croatia, Act on the Security Intelligence System of the Republic of Croatia 2006 (*Zakon o Sigurnosno-Obavještajnom Sustavu Republike Hrvatske 2006*), Art. 110.

267 FRA (2015a), pp. 33 and 68.

268 See also the concept of 'insider' complaints in Forcese, C. (2012), p. 182. See also PACE, Committee on Legal Affairs and Human Rights (2015a).

Protecting whistleblowers

"Whistle-blowers should be strongly protected and whistleblowing mechanisms should be strongly encouraged. Reports on internal and external whistleblowing should be sent to an independent supervisory body. The press and their sources should be protected in their reporting on the activities of the intelligence and law enforcement agencies."

Korff, D. et al. *(2017), p. 12*

"The law should require public authorities to establish internal procedures and designate persons to receive protected disclosures.

States should also establish or identify independent bodies to receive and investigate protected disclosures. Such bodies should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch."

Tshwane Principle 39 A and B(i)

The ECtHR addressed matters relating to whistleblowing by civil servants in *Guja v. Moldova*[269] and *Bucur and Toma v. Romania*.[270] The latter relates specifically to whistleblowing by a member of an intelligence service regarding the unlawful interception of communications. In deciding whether a sanction against a whistleblower is a justified interference with their freedom of expression, the ECtHR considers the following matters:

- whether the whistleblower had alternative channels for the disclosure,
- the public interest in the disclosed information,
- the authenticity of the disclosed information,
- the detriment to the affected institution,
- whether the whistleblower acted in good faith, and
- the severity of the sanction.

The French law on intelligence protects whistleblowers. If confronted with suspected wrongdoing, a staff member of the intelligence service can contact the CNCTR, which can then bring the case before the Council of State and inform the prime minister.[271] As of March 2017, the procedure has not yet been used.[272] In Germany, a whistleblower mechanism provides for the possibility for intelligence service staff to approach the Parliamentary Control Panel.[273] In the Netherlands, the new Act on the Intelligence and Security Services 2017 assigns the competence to investigate reported wrongdoing to the CTIVD.[274] In Belgium, when dealing with denunciations made by whistleblowers wishing to complain about their own administration, the Standing Committee I handles the individual complaint but focuses on the improvement of the efficiency of the intelligence services. Upon receiving a denunciation, it launches an investigation. The results of the investigation are shared with the whistleblower in general terms. They are also reported to the head of the relevant service, the competent minister and parliament. Finally, the general findings are made public.[275]

FRA asked different actors about possible provisions regarding whistleblower protection within the intelligence services. Provisions for such protection are prescribed in the legislation of four of the seven Member States researched. The respondents generally did not express specific or clear opinions regarding whistleblower protection provisions, and indicated that they lacked knowledge about the respective national context.

The interviewees did tend to agree on one aspect: that efficient whistleblower protection in the intelligence services requires a specific regime, different from those for other governmental institutions. In some Member States, recent legislative reform efforts included discussions of this issue, but they are not necessarily reflected in the enacted legislation. Otherwise, however, opinions on the issue of whistleblower protection generally varied, and also differed among respondents from the same Member State.

"It is not regarded as being very effective. For this reason, the political demand has been made time and time again that comprehensive protection for whistleblowers is needed." (Expert body)

"Well, we have no whistleblower protection. In general, there is no such protection and this is a real problem."

(Data protection authority)

"There are always calls for a whistleblower law in [country]. I do not consider this to be necessary. We do not need such a law." (Academia)

269 ECtHR, *Guja v. Moldova* [GC], No. 14277/04, 12 February 2008, paras. 70-78.
270 ECtHR, *Bucur v. Romania*, No. 40238/02, 8 January 2013, paras. 94-119.
271 France, Interior Security Code, Art. L. 861–3. See also Foegle, J.-P. (2015).
272 France, DPR &CNCTR (2017).
273 Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, s. 8 (1).
274 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97 and Arts. 125-131.
275 In total, the Standing Committee I received 22 complaints or denunciations, see Belgium, Standing Committee I (2016), p. 7.

In one Member State, for example, the opinions of the different actors ranged from a strong call to make whistleblower protection effective and a call for its implementation to questioning the need for such safeguards, even though the national legislation provides such a mechanism. The excerpted quotes illustrate the diverging opinions. These findings suggest that broader discussions are needed to encourage actors to fully consider their approaches to the issue.

9 Features of oversight bodies



ECtHR case law

Qualities required for supervisory control

"It is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...] supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 275

Public scrutiny

"The Court must also examine whether the supervisory body's activities are open to public scrutiny (see, for example, *L. v. Norway*, cited above, where the supervision was performed by the Control Committee, which reported annually to the Government and whose reports were published and discussed by Parliament; *Kennedy*, cited above, § 166, where the supervision of interceptions was performed by the Interception of Communications Commissioner, who reported annually to the Prime Minister, his report being a public document laid before Parliament; and, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 88, where the Court found fault with the system where neither the Minister of Internal Affairs nor any other official was required to report regularly to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases)."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para 283

The ECtHR favours oversight settings involving judges. The 2015 FRA report highlighted that a majority of EU Member States provide for such oversight.[276]

However, 'non-judicial bodies' – which this report refers to as oversight bodies in an encompassing manner or as expert bodies in a narrower sense – can be ECHR compliant. They should however have two essential qualities: be independent and have enough powers and competence to carry out continuous control that is subject to public scrutiny.

The interviewed oversight body experts were asked to identify what they consider to be the main features of effective oversight. Effective oversight was associated with the following five interrelated features: (1) cooperation among key actors in the area; (2) full access to intelligence information; (3) sufficient resources; (4) transparency (specifically through reporting), and (5) independence. These elements are listed based on the frequency with which they were mentioned during the interviews; however, this varied among respondents.

The respondents' views regarding what the most important elements of effective oversight are largely overlap with the main features of effective oversight identified in European case law. This is directly reflected with regard to independence, and partly with regard to public scrutiny, which is mainly considered through the issue of transparency. In this regard, reporting – mainly via reports produced, preferably published on a regular basis – plays an important role. The issues raised while discussing resources of oversight bodies, full access to intelligence information, and cooperation among key actors fall under the label of powers and competences. Table 3 presents the overlap between interviewed experts' views regarding features that make for effective oversight and the main features identified in ECtHR case law.

276 FRA (2015a), p. 51 and following.

Table 3: Effective oversight: legal standards and views of key actors

ECtHR standards	FRA fieldwork findings
Independence	Independence
Powers and competence	Full access
	Sufficient resources and expertise
	Cooperation of key actors
Public scrutiny	Transparency

Source: FRA, 2017

The following sections describe oversight bodies' features in detail, as formulated by the ECtHR and discussed in relevant fieldwork findings.

9.1. Independence

Basic requirements for independence

"In determining whether a body can be considered to be 'independent' – notably of the executive and of the parties to the case [...], the Court has had regard to the manner of appointment of its members and the duration of their term of office [...], the existence of guarantees against outside pressures [...] and the question whether the body presents an appearance of independence."

ECtHR, Campbell and Fell v. the United Kingdom, No. 7819/77 and 7878/77, 28 June 1984, para. 78

The ECtHR has confirmed that an institution's legal obligation to act independently and impartially is not sufficient to meet the minimum standard of independence; independence from the executive must be ensured both in functioning and institutionally.[277] The ECtHR requirement of independence entails organisational, operational and aspects relating to the members of the institution. Key questions in addressing the independence of an oversight body thus relate to its appointing authority; the body's composition and who chairs the body; rules on conflicts of interest; whether the law foresees its independent functioning and whether the body (in fact) operates without hindrance. Finally, independence is also a matter of perception: the body also needs to appear independent; the way it functions needs to be perceived as independent. In this context, the location of the body's offices may be relevant, for example – such as when an expert body is located within a ministry or in the intelligence service building. This is a particularly problematic matter given the data to which the oversight body has access. The need to be perceived as independent has to be balanced against practical security concerns.

Determining the optimal distance between the controlled and the controllers is a complex exercise, since providing up-to-date expertise requires oversight bodies to work side-by-side with the intelligence services. Therefore, while ties that are too close may lead to a conflict of interest, too much separation might result in oversight bodies that, while independent, are poorly informed.

"The oversight body must be able to work independently, full-time, it must be able to specialise and choose its own staff." (Expert body)

Oversight body representatives were asked about safeguards for their institutions to carry out tasks independently and the measures implemented to sustain their independence. Almost all respondents stated that their institutions were independent, impartial, and resistant to any external influence, including by politicians or the intelligence services. Independence is said to be guaranteed by institutional and operational procedures. The institutional procedures mentioned by the respondents include statutory recruitment procedures, methods of appointment (or the standing of the members), fixed terms of office, seniority of staff, and allocated budgets (independent budgets). The operational procedures that ensure independence in oversight actions were related to security clearance requirements, the staff's duty of absolute secrecy, access to data/information of the intelligence services, and their power to initiate investigations. In addition, some interviewees noted that their independence improved while moving their offices outside the premises of, for example, executive or other governmental bodies. Still, some interviewees pointed to a lack of independence due to being integrated into the hierarchies and structures of the institutions they were meant to monitor.

The oversight representatives attributed less importance to oversight bodies' independence than to other aspects when discussing their effectiveness. This might be related to their view that they currently exercise their functions in full independence.

As with other issues, representatives from civil society organisations and academia were more critical regarding oversight bodies' independence. They emphasised the importance of independent oversight, voicing the opinion that such bodies are currently 'only independent because they call themselves independent'. They noted that staff of oversight bodies lack knowledge on independence. In addition, some operational features make it difficult to sustain

277 ECtHR, *Campbell and Fell v. the United Kingdom*, No. 7819/77 and 7878/77, 28 June 1984, para. 77.

their independence – such as not being able to issue binding decisions, or having overlapping functions (e.g. being independent from the executive while, at the same time, participating in functions closely linked to the executive). They also highlighted the lack of transparency in nomination procedures and budgets being part of general ministerial budgets. These factors were also described as feeding into oversight bodies' lack of transparency and accountability.

ECtHR case law: requirements for independence

"As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the prime minister [...]. In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent [...]. In contrast to the supervisory bodies cited above, in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities [...].This fact may raise doubts as to their independence from the executive. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest [...]. The Court observes that prosecutor's offices do not specialise in supervision of interceptions [...]. Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings [...]. This blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 278*

Regarding parliament, the 2015 FRA report emphasised that the question of independence should be understood in terms of pluralism, which many Member States ensure by including mandatory proportional representation rules on membership.[278] By contrast, the executive appoints the members of some expert bodies. This is the case, for instance, in Sweden and the United Kingdom. In the United Kingdom, the Investigatory Powers Commissioner and the Judicial Commissioners are appointed for three years, by the prime minister, upon joint recommendation by the Lord Chancellor, the Lord Chief Justice of England & Wales, the Lord President of the Court of Session and the Lord Chief Justice of Northern Ireland.[279] In the case of the Judicial Commissioners, recommendation by the Investigatory Powers Commissioner is also necessary.

While some aspects of independence need to be enshrined in law, others can be re-affirmed in codes of ethics at institutional level. The French law on intelligence integrated specific ethical rules into the legal framework, including on CNCTR members' independence, specifying that they should not receive any instructions from any authority, and that members should not have incompatible mandates, links to the intelligence services, or perform any other professions or elective mandates.[280]

The CJEU has emphasised that DPAs shall act in full independence, particularly from government.[281] The same requirement is prescribed by the *General Data Protection Regulation*.[282]

9.2. Powers and competence

The ECtHR's requirements for an oversight body to have 'sufficient powers and competence' to exercise its control continuously is linked not only to a strong mandate but also to the means put at its disposal to perform its oversight role.

UN good practices on sufficient resources

Practice 7. Oversight institutions have the [...] resources and expertise to initiate and conduct their own investigations.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Oversight bodies may wield a variety of powers, a diverse combination of which may allow for adequate oversight of intelligence activity, including surveillance measures. These powers relate, on the one hand, to the appropriate review of the measures and, on the other, to the oversight bodies' ability to ensure that effective action is taken in case they find irregularities. What may be considered sufficient powers depends on a specific oversight body's function.

278 FRA (2015a), p. 41.

279 United Kingdom, Investigatory Powers Act, s. 227 (3)-(4).
280 France, Interior Security Code, Art. L. 832–1 and Art. L. 832–2.
281 CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 9 March 2010, paras. 23 and 30, CJEU, C-614/10, *Commission v. Austria*, 16 October 2012, paras. 36–37; CJEU, C-288/12, *Commission v. Hungary*, 8 April 2014, paras. 47–48; CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, para. 68.
282 GDPR, Art. 52.

Securing sufficient powers and competence for the oversight system, however, may still fall short of securing an overall adequate oversight system, if the bodies involved do not have sufficient human, financial and technical resources to fulfil their functions appropriately.

Review of resources

"The adequacy of such resources should be kept under review and consideration should be given as to whether increases in security service budgets necessitate parallel increases in overseers' budgets."

Council of Europe Commissioner for Human Rights (2015), p. 14.

As the resource needs of oversight bodies may differ substantially according to their functions and their role within a state's oversight system, general standards for sufficient resources cannot be established. Therefore, they should be assessed on a case-by-case basis, taking into account the standard of sufficient powers. The oversight bodies contribute to the framing of the intelligence services' work as well as the specific control of the surveillance measures. DPAs can play an important but specific role in this area depending on their competences.

Parliamentary committees focus their review on the overall legality of the functioning of the services and the intelligence policy, and not of that of their specific operations. In the Netherlands, for example, the Parliamentary Commission for the Intelligence and Security Services (*Commissie voor de Inlichtingen- en Veiligheidsdiensten,* CIVD) is responsible for overseeing the services to the extent that matters remain classified and is regularly informed about the operational activities of the General Intelligence and Security Service.[283] The French parliamentary intelligence delegation (DPR) examines and assesses governmental policy on intelligence; it does not oversee the services directly. This is to preserve the separation of powers.[284] It may conduct hearings and request strategic intelligence reports from the executive.[285] The DPR does not carry out thematic investigations. In its 2017 report, the DPR suggested that two audits be conducted by the Inspectorate of Intelligence Services, one on recruiting intelligence service staff and one on intelligence files.[286]

The different parliamentary committees of Member States have various mandates and powers. These include overseeing the policies, administration, budget and expenditure of the intelligence services; receiving periodical reports from the services themselves or from the members of the executive that oversee them; and inspecting sensitive documents and records and the premises of the intelligence services. Some may also receive complaints from individuals. The 2015 FRA report described the powers and competences of several specialised and non-specialised parliamentary committees in charge of the oversight of intelligence services.[287]

> *"The [United Kingdom's Parliamentary] Committee has been supported in its work by a team of seven core staff and seven Detainee Inquiry staff. These staff have an immensely difficult job to do. They act independently in support of the Committee and this is not always easy or popular with those who do not understand the importance of robust independent oversight."*
>
> *Statement by Chairman of the Intelligence and Security Committee (2017)*

Ad-hoc inquiry commissions or other general commissions can also play an important role in overseeing the services' work. In Belgium, the temporary 'Fight against Terrorism' Commission was established after the Paris attacks of November 2015. Its task was to examine the bills implementing certain measures put forward by the government following the terrorist attacks in Paris.[288] A Parliamentary Investigative Commission was also set up to examine the circumstances that led to the March 2016 attacks in Brussels.[289]

283 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*) (2016), 'Verslag van de commissie voor de Inlichtingen- en Veiligheidsdiensten over haar werkzaamheden in 2015', available at: https://zoek.officielebekendmakingen.nl/kst-34505-1.html

284 France, DPR & CNCTR (2017), p. 9

285 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 12.

286 *Ibid.* p. 57 and following.

287 FRA (2015a), pp. 34 and following.

288 Belgium, House of Representatives (2016), 'Magazine La chambre', *LaChambre.be*, p. 3; House of Representatives, Text adopted by the temporary 'Fight against Terrorism' Commission – Bill concerning complementary measures related to the fight against terrorism (*Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme/Wetsontwerp inzake aanvullende maatregelen ter bestrijding van terrorisme*), 14 April 2016.

289 Belgium, Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, 11 April 2016.

The German federal parliament's NSA inquiry committee

Following the Snowden revelations, the federal parliament established, on 20 March 2014, an inquiry committee (*1. Untersuchungsausschuss „NSA"*). The scope of its work was to investigate among others, these revelations, the operation of the Five Eyes (USA, UK, Canada, New Zealand, Australia) in Germany and the cooperation between the BND and the NSA. The committee published its 1,822 page-report on 23 June 2017, after 134 sessions and more than 90 witnesses (a total of 581 hours and 21 minutes of work). It is by far the most encompassing report published in the EU following the Snowden revelations.

Faced with a lack of cooperation from the services belonging to the Five Eyes, the inquiry committee focused its attention on, among others, the German legal framework, the work of the BND and other services, their surveillance powers, various intelligence programmes carried out by the BND, cooperation between the BND and the NSA, and the oversight system in Germany. The inquiry committee report contributes greatly to a better understanding of the work of the services in Germany, its oversight and international cooperation. In reaction to the Snowden revelations, the inquiry committee highlighted shortcomings, which led to an important reform of the German legal framework at the end of 2016.

The NSA inquiry committee members were not able to reach a consensus on the final report and so a separate opinion drafted by the opposition was added to the report. In particular, while the parties of the ruling coalition stated that no mass surveillance programme was carried out by the NSA and the BND (p. 1243), the opposition parties came to the opposite conclusion in their – partly redacted – separate opinion (p. 1323).

The NSA inquiry committee did agree that past serious grievances and major flaws could be attributed to the BND, necessitating reform.

*Germany, Federal Parliament (*Deutscher Bundestag*) (2017b)*

Members of parliamentary oversight committees tend to have access to classified information.[290] However, the law always qualifies the right of access, and few parliamentary committees have unrestricted access.[291] The laws of most countries grant parliamentary committees the authority to request information from the intelligence services or the executive, but not to demand it. In the United Kingdom, the ISC may request the chiefs of any of the three main intelligence and security services to disclose information, and they must make it available or inform the ISC that disclosure was vetoed by the secretary of state.[292] The French parliamentary committee (DPR) does not have access to information on ongoing operations carried out by the services, governmental instructions given to them, or surveillance methods or exchanges with foreign services.[293] The DPR gets its information through hearings, on-site visits and strategic documents, as well as opinions and reports by the oversight body.[294] The Dutch CIVD has access to the confidential part of the annual report of the General Intelligence and Security Service. The German Parliamentary Control Panel's access to files and information may be limited by the "direct executive responsibility" of the federal government. As underlined in FRA's 2015 report, the flipside of powers to access information also relates to security clearance.[295] In Belgium, the parliamentary committee decided on its own motion not to obtain clearance and thus cannot access confidential information, but it can turn to the Standing Committee I to conduct investigations.[296]

Oversight bodies' contributions to legislative reform vary greatly across Member States. Some contributions, in the form of official mandatory opinions, are prescribed by law – as is the case, for example, with the French expert body CNCTR. [297] The French parliamentary oversight body makes recommendations to the executive based on the analysis of intelligence policy and the functioning of the services. These recommendations are presented in a classified report addressed to the president, the prime minister and the speakers of both houses of parliament.[298] Once officially presented to the president, a non-classified report is also published with the recommendations. In the United Kingdom, the ISC published its views on the draft Investigatory Powers Bill.[299] In other legislative settings, the contribution can be published on a voluntary basis – see, for example, *The CTIVD's Views on the ISS Act 2017*[300] *in the Netherlands, or Interception of Communication Commissioners Office (IOCCO) Points to consider on the Investigatory Powers Bill* in the United Kingdom.[301] Participation in hearings and written evidence can also contribute to the legislative process and enhance transparency.

290 Wills, A. *et al.* (2011), p. 142.
291 See *Ibid.* p. 117; and Council of Europe Commissioner for Human Rights (2015), p. 44.
292 United Kingdom, Justice and Security Act 2013, Schedule 1, S.4. See, United Kingdom, House of Commons (2017), p. 7.
293 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6 nonies, I 4°. See also France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014), p. 13 and following and Urvoas, J.–J (2015), p. 41 and following.
294 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 12 and following.
295 FRA (2015a), p. 42.
296 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union for Threat Assessment (*Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*), 18 July 1991, Arts. 32, 33 and 35 (2).
297 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 811-4 and L. 833-11.
298 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 7 and 91.
299 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2016).
300 The Netherlands, CTIVD (2016b).
301 United Kingdom, IOCCO (2016b).

UN good practices on oversight institutions

Practice 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

One of the most important powers of oversight bodies is their ability to initiate investigations on their own. The Belgian Standing Committee I can start investigations on its own initiative, on the request of the Chamber of Representatives or the competent minister or authority,[302] or on the request of a citizen or a civil servant who lodges a complaint or files a denunciation.[303] In a judicial capacity, the Standing Committee I is also responsible for the ex post control of 'specific and exceptional data collection methods' used by the intelligence and security services.[304] The term 'specific and exceptional data collection methods' is relatively broad, covering all forms of collection of communications data relevant to this report, since they interfere with individual privacy.[305] Moreover, the Standing Committee I may, on request, advise on bills and regulatory acts or any other document expressing the political orientations of the competent ministers regarding the functioning of the intelligence services or the Coordination Unit for Threat Assessment.[306] Belgium has a second expert body referred to as the Administrative Commission. It is responsible for monitoring specific and exceptional data collection methods used by the intelligence and security services. It controls the legality, subsidiarity and proportionality of these data collection methods.[307]

In Germany, the Independent Committee (*Unabhängiges Gremium*) is an expert body, at the Federal Court of Justice, consisting of two judges and a prosecutor.[308] Its task is to review the legality and necessity of the BND's strategic foreign-foreign communications data surveillance. It is involved in the *ex ante* approval of strategic surveillance measures when they relate to EU institutions and Member States' authorities. The Independent Committee is also granted ex post review powers when the surveillance measures are deployed on EU or other foreign citizens. The investigative powers available to the Independent Committee are not specified in the law.[309]

ECtHR case law: binding interventions of oversight institutions

"The supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the effectiveness of its supervision (see, for example, *Klass and Others*, cited above, § 53, where the intercepting agency was required to terminate the interception immediately if the G10 Commission found it illegal or unnecessary; and *Kennedy*, cited above, § 168, where any intercept material was to be destroyed as soon as the Interception of Communications Commissioner discovered that the interception was unlawful)."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,* para. 282

Give an external oversight body the power to quash surveillance warrants and discontinue surveillance measures undertaken without the need for a warrant when such activities are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

Council of Europe, Commissioner for Human Rights (2015), Democratic and effective oversight of national security services, *p. 13*

Whether an oversight body has the power to quash warrants, stop surveillance measures and require the rectification or erasure of collected data is also an important factor in assessing the effectiveness of the oversight system. To do so, it is granted continuous access to the gathered intelligence and is informed about any modifications. In France, if the CNCTR considers a surveillance measure to be carried out unlawfully, it can recommend to the prime minister, the relevant minister and the intelligence service that the surveillance be interrupted and the collected data destroyed. The prime minister must immediately inform the CNCTR about how the recommendation was followed up on.[310] If the recommendation is not followed appropriately, the CNCTR can bring the case before the Council of State.[311] In the United Kingdom, the Judicial Commissioner, once established, will be able to reject warrants or quash those in operation.

302 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union for Threat Assessment (*Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*), 18 July 1991, Art. 32.
303 *Ibid.* Art. 34.
304 Belgium, Organic Law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 43/2, as amended.
305 *Ibid.* Arts. 18/4 to 18/8 and 18/9 to 18/17, as amended.
306 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union for Threat Assessment (*Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*), 18 July 1991, Art. 33.
307 Belgium, Organic Law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 43/1, as amended.
308 Germany, BNDG, S. 16.
309 Wetzling, T. (2017), p. 8.
310 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-6.
311 *Ibid.,* Art. L. 833-8.

In Sweden, the expert body SIUN, is tasked with ensuring that the state's signals intelligence is carried out lawfully.[312] SIUN monitors the conduct of the intelligence service and must be informed about the search terms the services apply. It exerts control over the signals that telecommunications carriers must provide to interaction points. SIUN is also in charge of reviewing the processing of personal data by the intelligence service, and ensuring that data collection complies with the permits issued by the Defence Intelligence Court. It has the power to stop on-going signals intelligence and subsequently order the destruction of collected data.

ECtHR case law: access to relevant documents

"Turning now to the prosecutors' powers and competences, the Court notes that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 281

UN good practices on access to information

Practice 7. Oversight institutions have [...] full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses and obtaining documentation and other evidence.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Another key power of oversight bodies is access to information, IT systems, documents and data – including not only that relating to specific operations, but also to internal policies and guidance. While access need not be complete, it should cover everything that may be relevant for the oversight bodies. In addition, access should be autonomous: oversight bodies should not be required to rely on the services to provide them what they deem relevant.

In the United Kingdom, the Investigatory Powers Commissioner (IPC) must keep under review the majority of the targeted and bulk surveillance powers available to the intelligence services, such as the interception of communications, the acquisition or retention of communications data and equipment interference.[313]The primary aim of the IPC's oversight is to keep under review the operation of safeguards to protect privacy,[314] excluding cases already being considered by the courts.[315] The Investigatory Powers Act grants extensive powers to the IPC. The intelligence services must disclose or provide all the necessary documents and information for the purposes of IPC's functions.[316] In addition, if the IPC requires assistance in accessing apparatuses, systems or other facilities of the intelligence services when exercising oversight functions, this must be provided by the intelligence services.[317]

In the Netherlands, the new legislation stipulates that one of the two sub-committees of the CTIVD performs general oversight. It reviews on a regular basis the activities of both intelligence services by investigating whether their operations or actions are in accordance with the existing legal surveillance framework. The CTIVD may request information and the minister's cooperation, and can give the minister unsolicited advice. In addition, through in-depth investigations and its complaints-handling[318] role, the CTIVD ensures that the intelligence services perform their duties lawfully. To do so, it has unlimited and independent access to AIVD data.[319]

In France, the CNCTR enjoys permanent, complete and direct access to the implementation reports and registries of surveillance techniques, to the collected intelligence, as well as to the transcriptions and extractions carried out by the intelligence services. Moreover, the CNCTR has unlimited access to the premises where collected data are stored, in addition to the devices used to trace the collected data.[320]

312 Sweden, Signals Intelligence Act (*Lag [2008:717] om signalspaning I försvarsunderrättelseverksamhet)*, ss. 10 and 10a, 10 December 2009; and Sweden, Regulation with instructions for the Swedish Foreign Intelligence Inspectorate (*Förordning [2009:969] med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*), 15 October 2009.

313 United Kingdom, Investigatory Powers Act 2016, s. 229 (1).
314 *Ibid.* s. 229 (5).
315 *Ibid.* s. 229 (4).
316 *Ibid.* s. 235 (2).
317 *Ibid.* s. 235 (3) and (4).
318 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97.
319 *Ibid.,* Articles 107-111.
320 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-2.

In Italy, the DPA is responsible for providing ongoing and ex post oversight on the services. It has the right to initiate inspections and to access classified materials.[321]

Most of the interviewed expert oversight bodies indicated that they have full, unrestricted, relevant access to intelligence data. According to the interviewees, they have 'access to (very) confidential and secret information', 'unlimited access', 'the full access', 'access to all documents', 'can get every information we want', 'can get classified information', 'can request anything from the intelligence services'.

Oversight body representatives noted that accessing intelligence services' documents and systems is a usual practice of the oversight system and is regularly exercised to the extent possible, regardless of the scope of activities. A limited number of staff (directly involved) in data protection authorities, ombudsperson or national human rights institutions enjoy different levels of security clearance with regard to direct access to the intelligence services' files.

"The important thing is for the inspector to be able to inspect the records of the organisation itself directly. We are not dependent on the organisation to say "we are going to show you only these 10 files", to provide us material. They should and do volunteer matters which are within the scope of the inspection; however, this is insufficient. We should be able to inspect their computer records." (Expert body)

"The primary concern of the oversight is to have access to all the material available to the services. […] The oversight body needs to have access to the algorithms and to the strategies behind those algorithms." (Expert body)

Although full access to intelligence information is crucial for effective oversight, so is the ability to fully benefit from such access. Some respondents questioned oversight bodies' ability to do so, particularly due to limited technical capabilities. This was indicated both by way of critical self-assessment of the competences within the oversight bodies, and via criticisms from other bodies or organisations in the field. Representatives of civil society, academia and lawyers questioned the bodies' 'abilities to check the things properly', including their general understanding of the digital environment – for example, the digital (technical) skills of members of parliamentary committees.

"While the surveillance community, the secret service and the police are now immersed in big data and the advanced information society, the oversight bodies should not use coaches drawn by horses. But this is the situation today because intelligence organisations, services and police are hesitant to accept the use of [certain] software by control bodies, oversight bodies." (Data protection authority)

For effective compliance control, the *General Data Protection Regulation* grants powers of investigation (access and collection of necessary information), intervention (ordering corrective measures, banning data processing, warning or admonishing the data controller, referring the matter to national parliaments and other political institutions), and engagement in legal proceedings.[322] DPA decisions may be subject to judicial control. Additional Protocol 181 to Convention 108 also provides for these powers – except for advisory power, which is mentioned in the explanatory report to the protocol.[323]

DPAs' competences vis-à-vis intelligence services vary in the Member States, and depend on national legislation. DPAs may have no powers, limited powers or the same powers over the intelligence services as any other data controller.[324] FRA's findings show that, in most Member States, DPAs have either no competences over national intelligence services (in 11 EU Member States), or their powers are limited (in 10 Member States).

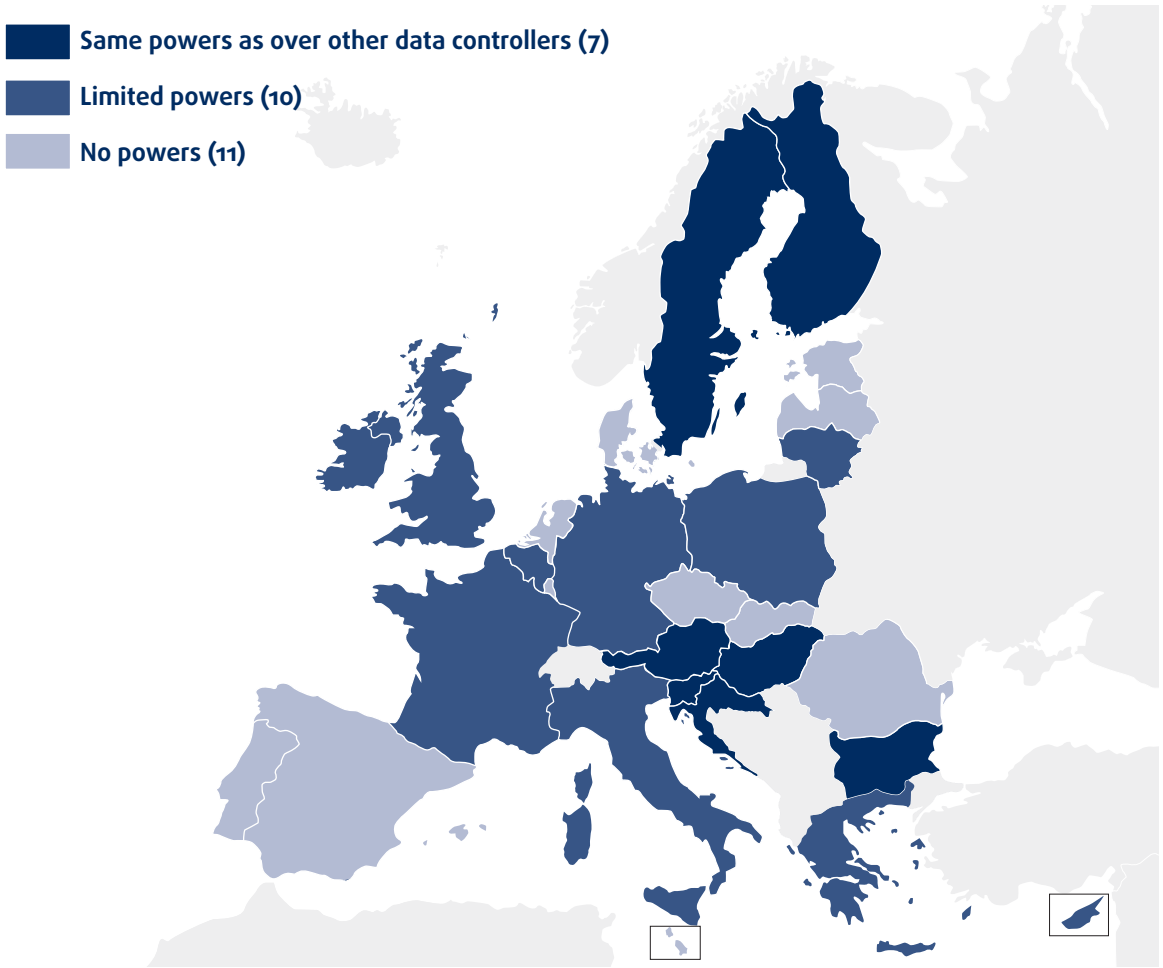
321 Italy, Data Protection Code, Art. 160 (4).

322 GDPR, Art 57.

323 Council of Europe, Convention 108, Additional Protocol, para. 16.

324 See FRA (2015a), pp. 46-51, for a detailed overview of DPAs' competences over intelligence services.

Figure 7: DPAs' powers over national intelligence services, by Member State



Source: *FRA, 2017*

As Figure 8 illustrates, the extent of oversight coverage among Member States is very diverse. In four Member States – Austria, Bulgaria, Hungary and Sweden – both the expert bodies and the DPA are competent to assess the legality of surveillance techniques conducted by intelligence services. By contrast, in six EU Member States, no expert body has been set up to supervise surveillance techniques, and the intelligence services are exempt from DPAs' scope of competences. The 2015 FRA report raised questions regarding possible overlapping supervision powers for Member States with both types of oversight bodies, and questioned the effectiveness of oversight in the EU Member States that have not established any expert bodies and have exempted their DPAs from overseeing intelligence services.[325]

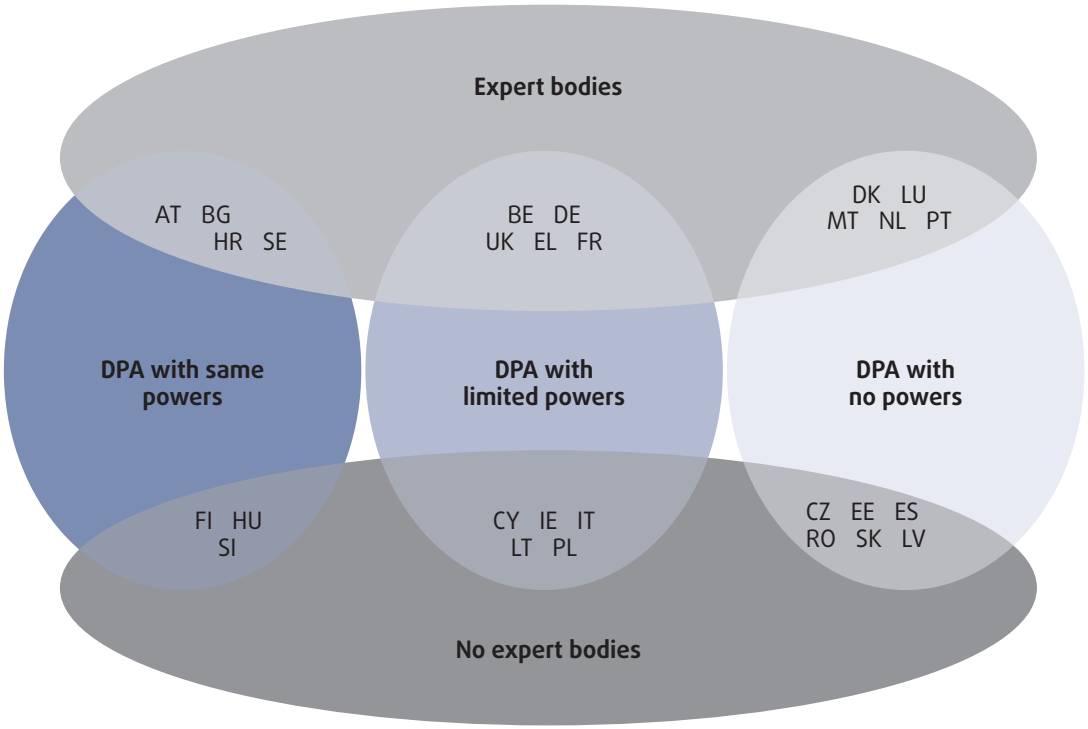
DPAs with limited powers act as regulators of the treatment of data used for intelligence purposes. They may have an advisory role, providing opinions on proposed laws that have an impact on personal data protection, including the setting up of new databases in the field of national security. DPAs treat intelligence services as data controllers and their oversight is limited to supervising the intelligence services' compliance with obligations linked to the processing of data. DPAs with limited powers do not look at the content of intercepted communications. For example, the DPAs could check through inspections whether the intelligence services respect the permissible period of retention of the collected data. However, the law may limit their access to databases containing data that were collected through certain intelligence techniques.

DPAs' powers are limited in 10 Member States. For instance, in the United Kingdom, the national intelligence services may rely upon the exemption for national security cases, which is provided in the data protection law.[326] The Information Commissioner Officer (ICO) must audit compliance with requirements or restrictions imposed by the retention of communications data in

325 FRA (2015a), p. 53.

326 United Kingdom, Data Protection Act 1998, s. 28 (1).

Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State



Notes: *'No powers' refers to DPAs that have no competence to supervise intelligence services.*
'Same powers' refers to DPAs that have the exact same powers over intelligence services as over any other data controller.
'Limited powers' refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers).

Source: *FRA, 2017*

relation to the integrity, security or destruction of data retained by the services. In other words, the ICO does have competence in reviewing *how* the data is retained, even if they have no access to *what* is retained. In practice the ICO liaises closely with the expert bodies and advises on data protection standards.

In Germany, the new federal data protection legislation only grants the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) the power to file non-binding complaints (*Beanstandungen*) against intelligence services when data breaches are detected.[327] Additionally, depending on how the law is interpreted, it may provide the commissioner the power to request, upon suspecting individual intelligence service staff members of committing specific data breaches, the court to impose individual sentences of up to three years on such staff members.[328] However, the legal provisions on sentencing are ambiguous regarding intelligence services staff, because intelligence activities are potentially excluded from the scope of application.[329] In 2016, the commissioner filed a formal complaint against the Federal Office for the Protection of the Constitution (BfV) for illegal practices in transferring data originating from domestic general surveillance of communications to a counter-terrorism database. The commissioner's latest annual report notes that this complaint was the result of a joint inspection with staff from the secretariat of the G10 Commission.[330]

In Member States where expert bodies exist and DPAs have the competence to oversee intelligence services, their interaction is sometimes organised by law, and sometimes in practice takes place without legal requirements. In Member States in which DPAs and other expert oversight bodies share competence, a lack of cooperation between these may leave gaps in the

327 Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), s. 16 (2), in force on 25 May 2018.
328 *Ibid.* s. 84 in conjunction with s. 42, in force on 25 May 2018.
329 *Ibid.* s. 45, in force on 25 May 2018.
330 Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2017), pp. 134-135. See also, Germany, Federal Parliament (2017a), p. 642 and following and on the challenges to control: Germany, Federal Parliament (2017a), p. 811 and following

overall oversight of the services. In Member States where DPAs lack competence over intelligence services, the oversight body is responsible for ensuring that privacy and data protection safeguards are properly applied (for example, in the Netherlands). An example of a prompt, practical reaction after the Snowden revelations is the Memorandum of Understanding (MoU) signed in 2013 by the Italian DPA and the intelligence services. The MoU lists the files subject to inspection by the DPA, and provides rules on the DPA's access to the premises and files, the secure storage of intelligence information at the DPA's premises, and the implementation by the intelligence services of the DPA's findings. Finally, it provides for the possibility of the intelligence services consulting the DPA beyond what is currently laid down in the legal framework.[331] Regrettably, the MoU's content is classified and not publicly available.

"The Memorandum [of Understanding] is an example of how to extend the law in favour of citizens' protection."

(Data protection authority)

Similarly, a 2016 report by a committee appointed by the Swedish executive considered possible supervisory overlaps and suggested moving some control functions from other agencies to the DPA.[332]

In the six Member States where no expert bodies have been set up to supervise surveillance techniques, and intelligence services are exempt from DPAs' scope of competences, the legal frameworks allow only for targeted surveillance and all foresee judicial involvement in the authorisation of such measures.

Two of these – Estonia and Slovakia – have empowered other authorities with controlling competences. In Estonia, the oversight of the services is since January 2016 exercised by the ombuds institution, the Chancellor of Justice, who may undertake ex post review both on its own initiative and further to a complaint. It can recommend changes to the legal framework and can initiate judicial review of the same by the Constitutional Court.[333] In Slovakia, the oversight of intelligence services is divided among five different oversight bodies: one specialises in reviewing decisions taken by the National Security Authority, three in reviewing the performance of the intelligence services (one per service), and a recent special commission was set up to supervise the use of information technology tools. This commission must include two independent experts, chosen by the parliament, who have at least ten years of professional experience as either police officers, prosecutors, judges or members of an intelligence service.[334]

The representatives of the oversight bodies (expert bodies, parliament committees and data protection authorities) were asked to assess their body's mandate in terms of its ability to conduct effective oversight over intelligence gathering. Powers to investigate, the scope of investigations, the implementation of their propositions, control limitations, and related matters were addressed. Most respondents described their current mandates as 'sufficient', 'robust', 'solid', 'clear', and as having 'broad powers', and claimed that these encompass important powers. Among the powers supporting the robustness of their mandate, respondents most often mentioned the following features along with defined powers (e.g. ex post oversight): (a) full access to intelligence information, including on-site visits to premises and direct contact with staff; (b) independent investigations and the ability to choose the subjects of investigations and which data collection techniques to investigate; (c) opinions, recommendations provided (e.g. on legislation).

Even where respondents considered the mandate of their oversight body to encompass sufficient powers, they mentioned the non-binding nature of their decisions (examples provided in France, Italy and the Netherlands) or limited competence as limitations (e.g., dealing only with a specific issue or stage of oversight or only with exceptional situations). A few respondents stated that the current powers are insufficient – and the impact of oversight low – and need to be expanded.

While discussing the role of DPAs in intelligence oversight, respondents highlighted that other actors in the field recognise their powers and expertise. In the past few years, an 'important level of listening' has been reached. The interviewees provided examples of regular consultation on relevant issues, including draft legislation (particularly in France, Italy and the United Kingdom). They maintained that they do see their contributions making an impact in terms of changes to legal frameworks. They also stated that DPAs' contributions – through cooperation with other institutions; by submitting opinions on relevant issues, annual reports, and special reports to the parliament; and by providing evidence during parliamentary

331 Italy, Italian Government (2013). See also COPASIR (2014), p. 19.

332 Sweden, State Official Reports (*Statens Offentliga Utredningar*) (2016), pp. 169 *et seq.*

333 Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, Article 1 para 9.

334 Slovakia, Act No. 404/2015 Coll. amending and supplementing Act N. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*), 19 December 2015, art. 8(a).

hearings or discussions, etc. – enhance the transparency of the intelligence oversight process. The interviewees believe that DPAs serve as 'a constant reminder to the balance of rights', raising public awareness on possible rights violations.

"In the past year, the consulting activity that is requested by [intelligence services] increased considerably. We were consulted three times, [...] opinions were requested. The DPA activities are perceived as important." (Data protection authority)

However, despite their recognised expertise in the area, DPAs feel they are operating in a 'fragmented system' ('fragmented nature of the regimes'). They noted that they have limited powers in the intelligence oversight process – for example, by focusing solely on data processing and not the techniques used; having oversight only of a specific step/stage in the process, such as ex ante; limiting their review to compliance with data retention rules; or having only indirect access to data. These give DPAs a sense of lacking power – as being unable to follow 'the file as a whole'. Interviewees also mentioned that they sometimes do not fully understand the competences of all the other actors in the field.

"[It is important] to make sure each body with powers in this area has an understanding about what one could do... But I think the concern is really around the fragmentation, complexity, lack of transparency." (Data protection authority)

"The other bodies are very important because the DPA cannot go as far in its review." (Data protection authority)

DPAs repeatedly emphasised the importance of institutional cooperation with different national and international authorities, the coordination of activities, and the complementarity of different actors' activities in the field. They acknowledged that they interact with few other national authorities, but noted that they have been developing beneficial cooperation with intelligence services (e.g. 'from suspicion to increasingly seen as a partner'; '[a] bond of trust is being established'). The interviewees noted that some of the cooperation is not formalised, and that it remains fragmented, selective and occasional. The Article 29 Working Party was referred to as the main forum for international cooperation, although differences between DPAs' competences in intelligence oversight hinder further cooperation.

"[Some] DPAs feel uncomfortable because they have no expertise in the field in question, and therefore stop themselves from even thinking about it."

(Data protection authority)

Providing oversight bodies with sufficient financial resources is key to ensuring that their oversight is effective.[335] Human resources also play a key part. A certain parity between the powers of the overseer and the mandate and powers of the intelligence services also contributes to the effectiveness of the oversight structure. Especially in view of the trend of intelligence services increasing their technological capacities, financial resources and their reliance on complex systems, "recourse to independent technical expertise has become indispensable for effective oversight".[336] Therefore, highly specialised legal and technical knowledge constitute particularly important resources for oversight systems.

The 2015 FRA report emphasised the need for oversight bodies to be technically competent.[337] Several expert bodies have tackled this issue by recruiting external technicians, either on an ad hoc or more permanent basis. In December 2014, the Dutch CTIVD established a 'knowledge network' of scientific experts (in the fields of security, intelligence, and information law) to regularly advise the Review Committee on specific reports relating to technological, legislative and social developments.[338] Indeed, with the increased sophistication of surveillance techniques, often automatised, the CTIVD recognised the need for ICT expertise and invested additional financial resources in technology for carrying out oversight. The CNCTR is provided with the human, technical and budgetary means needed to accomplish its missions.[339] A secretary general and 14 staff members assist its work.[340] It can also consult and answer the questions of the Electronic Communications and Posts Regulatory Authority (*Autorité de régulation des communications électroniques et des postes*, ARCEP).[341] In the United Kingdom, the Investigatory Powers Act requires the IPC to establish a Technology Advisory Panel, mandated to provide advice on "the impact of changing technology on the exercise of investigatory powers and the availability and development of techniques to use such powers while minimising interference with privacy".[342] Although not yet fully functional, IPC has already started identifying experts to fill this new panel.

While discussing the skills available in their institutions, the respondents – representing a variety of oversight bodies – confirmed that oversight of intelligence collection is dominated by legal expertise. Most interviewed staff working on relevant issues at expert oversight bodies, data protection authorities, ombuds or national human rights institutions have legal

335 Council of Europe, Commissioner for Human Rights (2015), p.9.
336 *Ibid.* p.10.
337 FRA (2015a), pp. 43, 60 and 73.
338 The Netherlands, CTIVD (2015), p. 10.
339 France, Interior Security Code (*Code de la Sécurité Intérieure*), Art. L. 832-4, first sentence.
340 France, CNCTR (2016), p. 60.
341 France, Interior Security Code (*Code de la Sécurité Intérieure)*, Art. L. 833-11.
342 United Kingdom, Investigatory Powers Act, s. 246 (1).

backgrounds. In some Member States, the legislation envisages a legal background for the staff and/or members of the committees. In a few Member States, information about the staff's background and possible needs was not made available for FRA's research.

"In principle, we are a committee of legal experts. […] As far as the secretariat is concerned, the staffing plan determines which qualifications are required." (Expert body)

Civil society organisations active in this field mainly engage lawyers. In some cases, their legal capacity is supported by technical experts, or certain knowledge is developed through involvement in the field. Many organisations have been involved in litigation on a variety of issues relating to data protection or privacy, including cases alleging unlawful data processing by intelligence agencies.

"We need more computer people." (Expert body)

"One area where we need to get some more expertise is in the technical field, maybe someone who knows more about data analysis, algorithms, that need is increasing."

(Expert body)

"You need someone who has the necessary expertise to understand specific technical processes. In my view, none of the members of the [expert body] are so well-versed in technical matters that they are able to assess complex situations – in particular situations concerning the [services] - on the basis of their own knowledge." (Expert body)

A few oversight body representatives said they have legal and technical expertise, and emphasised the importance of having both. In some cases, this combination was noted as a recent development. A few respondents believed that their technical capacity was sufficient, and no specific changes were needed. An absolute majority of the interviewees identified a great, increasing need for technical expertise, which is currently missing. Representatives of expert oversight bodies, parliamentary committees and executive control institutions expressed a clear demand for technical expertise, which is perceived as highly advantageous and beneficial for their authority. The respondents indicated that they believe a lack of technical expertise will remain one of the biggest challenges in the oversight field in the coming years.

"Regarding the intelligence services: it is working well for the moment but the growing technical complexity means that the DPA will have to increase its technical staff of IT experts who will be able to provide real technical expertise, particularly on the protection of data banks."

(Data protection authority)

The major need for technical expertise was acknowledged by oversight bodies and other experts in the field. During interviews, respondents representing civil society organisations, practicing lawyers and academia criticised the oversight bodies' limited technical capacity in terms of staff with technical background. As one respondent put it, 'with all my respect, they are not young IT types that you should have in an organisation as such'. Technical competence (capacity) was often mentioned by the respondents as one of the main features of effective oversight.

In terms of having sufficient resources, approximately two out of three respondents from oversight bodies expressed satisfaction with currently available human resources. Comments included that these 'are adequate', 'as things currently stand, it is remarkable', 'at the moment meet the needs', 'staff numbers are reasonably stable', 'there is no need to be expanded', 'it is effective because it is not too big', 'enough resources', and 'we have what we want'. Examples of these kinds of assessments were provided in most Member States.

Assessments of the size of the staff differed across the institutions. For example, some respondents said oversight can be effective in a small (limited) circle; others referred to limited resources, an increasing workload and the complexity of the work ('the work has become more complicated and [numbers of] investigators are no longer adequate'); and some indicated that they were in the unsatisfactory situation of being understaffed and said there was a clear lack of human resources.

"In the past, cases were simple; now they are more complex. The use of specific methods and appeals have increased, in technicality and volume." (Expert body)

"Even though we have not always been fully staffed, public confidence in our body has significantly increased due to the greater transparency of our procedures and the decisions we have made." (Expert body)

With regard to technical capacities, the respondents quite often noted difficulties in recruiting technical staff (ICT specialists) because the public sector is not able to compete with the private sector in terms of salaries. According to respondents, the same applies both to the intelligence services and their oversight.

Among the requirements for staff of oversight bodies, many respondents mentioned security clearance – the highest level of confidentiality in most cases – as the main criteria. Some said that the clearance procedure does not hinder recruitment and is not a restricting factor (e.g., 'an accelerated clearance procedures can be applied during the recruitment process'). Others said that it takes time and prolongs recruitment and might

be unattractive to possible candidates ('it is very tough procedure', 'it takes 4-5 months').

Among other difficulties faced by oversight bodies regarding resources, respondents mentioned the following issues: staff turnover, which can affect credibility and might risk leaked information; part-time staff (e.g. judges) with competing private practices; and a lack of control over outsourced staff.

Regarding budgets, opinions varied – ranging from being positive about sufficient budgets, recent increases or adequate funding to references to a lack of financial resources.

Respondents were also asked if they could hire or recruit additional external staff in case of need. There are no common opinions and experiences in this regard as situations differ quite extensively. In some Member States, oversight bodies have no possibility to hire external expertise; in other Member States, oversight bodies have never used this opportunity although it is provided for in the relevant legislation. In some Member States, expert bodies receive external support, including from academia, when needed. Still, the outsourcing of expertise is rare. Most institutions rely on available internal resources.

"The oversight process is becoming an extremely technical and massive task." (Expert body)

Some interviewees referred to computerised/automated oversight tools, including those built into the software used by intelligence services, as providing possibilities for furthering technological development and strengthening oversight. These include "automated checking", "the ability to carry out a technical verification at regular intervals", and "updates of the data banks", including "computerised clean-up techniques" or "automated data destruction". Other respondents refer to these as providing an important opportunity to identify possible violations at an early stage, and encourage application of, for example, data protection oversight by design. They are also considered a positive feature for the intelligence services, bringing more balanced oversight and a possible solution for oversight bodies' need for technical expertise. In some Member States, strategies for implementing such tools have recently been developed or implementation has just started. The oversight experts noted the importance of following closely ICT developments in the agencies themselves, and progress in understanding the digital world among the various stakeholders.

"At minimum, there must be very close cooperation governed by law, and not just dependent on the will and the intention of the acting persons." (Data protection authority)

Finally, in connection with resources, interviewees repeatedly pointed out that not only the resources themselves matter, but the way institutions work and communicate with each other does, as well. The interviewed experts generally raised the importance of cooperation in its different constellations – including with intelligence services, executive control; between oversight bodies; with civil society – and natures (e.g. prescribed by law by different functions, formalised through a MoU, informal exchanges) when discussing different topics, such as effective oversight, measures to uphold fundamental rights, and the transparency of the activities of both intelligence services and oversight bodies.

According to the interviewees, cooperation through 'constant dialogue' and 'continuous sharing of information' contributes to having a systematic approach to oversight and helps overcome possible fragmentation of the oversight system. Likewise, sharing good practices helps build trust, and sufficient levels of trust allow actors to cooperate. The respondents also expressed a great need for both national and international cooperation, and exchanges of information and best practices in the area. The *General Data Protection Regulation* gives advisory powers to DPAs when Member States draw up legislative or administrative measures. Therefore, DPAs can contribute by pointing out potential threats to data protection when Member States plan to modify surveillance powers granted to intelligence services.

Swedish government preparatory study recommends stronger role for DPA

In 2016, the national government appointed an expert committee to examine how a higher degree of integrity protection can function within a single governmental department, allowing thus the supervision of collection of personal data to be also attributed to a single authority. The expert committee issued a 222-page report which provides an overview of the role of the committee and previous work in the area, then scrutinises the current system of supervision and how it could be improved.

While the general assessment is positive, it does, for instance, call for some simplifications or clarifications in relation to the mandate of control functions. In particular, the committee recommends giving the DPA a more central role, mainly in relation to provisions in sector-specific legislation that are of a more general nature (such as related to cookies), and states that other monitoring bodies should consult the DPA or even hand issues over to it to resolve them.

Sweden, Government preparatory study (2016), 'Joint responsibility over personal integrity'

9.3. Openness to public scrutiny

The ECtHR puts great emphasis on the liability for the executive but also the oversight body to give account on their respective work in the area of intelligence services oversight.

ECtHR case law: executive and oversight bodies subject to public scrutiny

"The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny [...]. The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the activities of the national security services. However, the Court is not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, especially since it does not appear that the committee has access in detail to relevant documents. The scope of their supervision is therefore limited [...]."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 82

Oversight bodies need to be transparent and provide adequate information to the public about their activities and those of intelligence services. This is because oversight systems serve the ultimate goal of protecting the public against abuse in the implementation of surveillance measures. Due to their independent status, the various bodies of oversight systems are ideally placed to provide credible and reliable information to educate the public about the activities and role of intelligence services.[343]

Member States and oversight bodies take very divergent approaches when it comes to the regulations and/or practices aiming to provide for the transparent functioning of the oversight system. Considering the secret nature of the techniques and operations, it is beyond dispute that full transparency of oversight is neither possible nor desirable. However, as high a degree of transparency as possible is indispensable for ensuring that citizens can understand and thus trust the functioning of the oversight system and, consequently, that of the secret services.

In the United Kingdom, for example, the Investigatory Powers Commissioner must report "as soon as reasonably practicable after the end of each calendar year"[344] or at any time requested by the prime minister[345] or where the commissioner considers it appropriate.[346] With respect to the commissioner's annual reports, the prime minister has an obligation to publish them, and lay a copy thereof before parliament together with a statement on any matter that has been excluded.[347] Therefore, the prime minister has the power to exclude matters from the published report but may do so only after consultation with the commissioner.[348] The grounds on which some matters can be excluded are laid down in law.[349]

Representatives of oversight bodies were asked how their institutions contribute to the implementation of transparency in oversight. Issues relating to transparency were raised by the respondents while addressing accountability and the effectiveness of oversight, too.

In general, according to the interviewees, transparency is a relatively recent topic in the area of intelligence collection and its oversight. The Snowden revelations have significantly contributed to transparency – for example, several oversight bodies indicated that, 'in reaction to the Snowden leaks afterwards many governments all of the sudden published information *that beforehand was considered secret.*' The effects are reflected in publications, increased efforts to improve general communications, information exchanges and institutional cooperation. To a certain extent, the issues relating to transparency were mentioned in the context of upholding fundamental rights during the collection of intelligence and its oversight.

343 Council of Europe Commissioner for Human Rights (2015), p. 65.

344 United Kingdom, Investigatory Powers Act, s. 234 (1).
345 *Ibid.* s. 234 (3).
346 *Ibid.* s. 234 (4).
347 *Ibid.* s. 234 (6).
348 *Ibid.* s. 234 (7).
349 *Ibid.*

"It is rather difficult to talk about transparency in relation to services whose effectiveness depends upon secrecy."

(Parliamentary committee)

"The issue of transparency is discussed in connection with an area of activity the very principle of which is a lack of transparency, since classification of information as secret puts a limit on transparency." (Expert body)

"There is a lack of transparency on this issue, due in particular to its degree of technical complexity, which is itself heightened by the difficulty in accessing information, since the intelligence services are not very communicative."

(Civil society organisation)

While discussing transparency issues, many oversight body representatives mentioned existing limitations for transparency in the oversight of intelligence collection. Some respondents believe the general culture of secrecy around intelligence services interferes with transparency, and that the lack of transparency is inevitable. The limitations or lack of transparency are related to a great variety of issues, such as technical complexity, classification of information, level of secrecy ('the trade-off between transparency and secrecy'), and restrictions and limitations defined by legislation, which have to be respected. Some respondents said that secrecy constraints serve as a tool to keep the procedures implemented properly, e.g. observing classification levels. Some interviewees believe that transparency can nonetheless be maintained through cooperation or communication between the different institutions and public authorities that operate in the area.

According to Born and Wills, useful elements for achieving maximum transparency include availability of information about the conduct of the oversight bodies, regular reporting to a relevant authority and occasional publication of special reports.[350] Regarding these key aspects, it is relevant whether the oversight bodies have open sessions, whether their members are allowed to comment on their findings, and whether the body issues comprehensive, regular and largely informative reports. At the same time, the effectiveness of providing transparency will inevitably depend on the powers of the oversight bodies, as that will, among others, define the quality and quantity of information they have access to in the first place. As emphasised in FRA's 2015 report, expert bodies' ability to publish public versions of periodic and investigation reports is essential.[351]

The meetings of the Dutch CIVD are strictly confidential. It publishes an annual report, addressed to the House of Representatives, with information about the number of meetings and the agenda items.[352] The report of the Intelligence and Security Committee of the United Kingdom, whether annual or *ad hoc*, usually contains redactions on security grounds suggested by the services – but these must be justified, and the committee has the final say.[353] In a case of major disagreement, the prime minister may exceptionally insist on a redaction before a report is sent to parliament (the redaction is reported).[354] The ISC may also choose to report privately to the prime minister if a national security matter is exceptionally sensitive[355] – an example might be the handling of an ongoing espionage case. Though members of the German Parliamentary Control Panel are sworn to secrecy, they can comment publicly on certain issues, as long as the decision to do so is reached by two-thirds of its members.[356] It reports to the parliament twice during the legislature.[357]

FRA analysed some of the key features of the publicly accessible reports prepared by expert bodies[358] (Annex 3) and parliamentary oversight committees (Annex 4) in several Member States. A report's length can indicate the level of detail provided therein and thus how transparency is observed. For example, in 2016, the Belgian Standing Committee I produced an annual report of 131 pages. By contrast, the German G10 Commission published a 10-page report. However, some expert bodies publish separate reports on specific investigations conducted and exclude this information from their annual reports. It is also not uncommon for parliamentary committees to prepare *ad hoc* thematic reports, as is the case in the United Kingdom[359] and Italy.[360]

350 Born, H. and Wills, A. (2012), p. 80.
351 FRA (2015a), p. 41.

352 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*) (2016), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page.
353 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), p. iv (foreword).
354 United Kingdom, Justice and Security Act 2013, ss. 2 (3) and 2 (4) of Part 1.
355 United Kingdom, House of Commons Library (2017), p. 6.
356 Germany, PKGrG, S. 10 (1). See Bartodziej, P. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1556 and following.
357 See Germany, Federal Parliament (*Deutscher Bundestag*) (2016), the latest report covering November 2013 to November 2015. See also de With, H. and Kathmann, E. (2011), Policy Department C: Citizens' Rights and Constitutional Affairs, p. 218; Heumann, S. and Wetzling, T., Stiftung neue Verantwortung (2014).
358 Excluding data protection authorities.
359 For example, see United Kingdom, Intelligence and Security Committee of Parliament (2015).
360 For example, see Italy, COPASIR (2015), 'Report on so-called "Butterfly" and "Return" operations and on the affair "Flamia"' ('Relazione sulle cosiddette operazioni "Farfalla" e "Rientro" e sulla vicenda "Flamia"'), Rome, 12 March 2015.

In general, expert bodies' reports describe the surveillance legislation in the Member State concerned and outline the particular expert body's mandate, powers and internal functioning. Depending on these powers, the expert bodies present statistics on authorisations of surveillance measures and the ex post controls and investigations they conducted. In exceptional cases – for instance, in France and Germany – the number of individuals that were under surveillance during the reporting period is stated, as well as the purpose pursued by the surveillance. In France, the CNCTR has the possibility to publish the total number of people under surveillance because it controls all surveillance techniques in France. Between 3 October 2015 and 2 October 2016, 20,282 persons were subjected to a surveillance technique.[361] In Germany, the Parliamentary Control Panel publishes information on the number of individuals under targeted surveillance (pursuant to Section 3 of the G 10 Law). In 2015, there were 336 primary targeted persons (*Hauptbetroffene*) during the first semester and 322 in the second half of the year; and 249 indirectly targeted persons (*Nebenbetroffene*) during the first semester and 224 during the second. This means that 1,502 telecommunication connections (*Telekommunikationsanschlüsse*) were tapped during the first semester, and 1,336 during the second half of 2015.[362]

The Belgian Standing Committee I also publishes very detailed numerical information on surveillance authorisation issued to the services. These are separated according to each service and each surveillance method (specific and exceptional).[363] Where applicable, most annual reports contain statistics on the outcomes of complaints by individuals. Some expert bodies also report on their interactions with other domestic institutions and foreign expert bodies. Given that the expert bodies in parallel have an advisory role, some of them provide, in their annual reports, recommendations to governments concerning good practices and legislative improvements.

The Dutch CTIVD has criticised the ban on the publication of the number of wire taps performed by the intelligence services. It has noted that publishing mere tapping statistics does not reveal the factors affecting the number of interceptions, or the techniques used for such purposes. In addition, it does not influence the priorities or reveal sensitive information on the technical capacity of the intelligence services. Therefore, it has claimed that national security is not endangered.[364] Based on the CTIVD's opinion, the Dutch Council of State in 2016 annulled a decision of the Minister of Interior not to make tapping statistics available to the NGO Bits of Freedom following a Freedom of Information request.[365]

Parliamentary reports focus on the number of hearings conducted and the list of witnesses heard. Annual reports rarely provide details about the content of the hearings. However, this is done, for example, in Italy and the United Kingdom. In the United Kingdom, reporting on the hearings is not limited to a brief summary of the proceedings. An extensive degree of transparency is achieved by providing links to the full transcripts of the proceedings. Parliamentary committees tend to report on the budget of the intelligence services as well as the threats the intelligence services focused on during the reporting period. Parliamentary committees also provide explanations of the oversight methods used to gather information from the intelligence services and, when applicable, present statistics on the investigations conducted and the outcome of complaints received by individuals.

Overall, an analysis of the reports of expert bodies and parliamentary committees in several Member States shows that particularly in Belgium, France and United Kingdom, expert bodies or parliamentary committees have substantially taken into account transparency requirements. Their reports are accessible and provide detailed overviews of the concerned oversight systems and the results these produce, depending on their competence (e.g. extensive statistics on use of surveillance techniques, authorisations, *ex post* controls and complaints-handling). They also make use of their advisory role towards the government and outline recommendations regarding current practices and legislative reforms, while informing the public about the inter-institutional dialogue they conducted during the reporting period.

361 France, CNCTR (2016), p. 73.
362 Germany, Federal Parliament (2017), p. 5.
363 Belgium, Standing Committee I (2016), p. 49 and following.
364 The Netherlands, CTIVD (2012), pp. 26-28.
365 The Netherlands, Administrative Jurisdiction Division of the Council of State (*Afdeling Bestuursrechtspraak van de Raad van State*) (2016), *Case no. 201505432/1/A3*, 4 May 2016.

Promising practice

Promoting transparency in oversight

Regularly issuing detailed reports

The Italian COPASIR, the French DPR, the German PKGr and the United Kingdom's ISC are legally obliged to regularly publish reports. This promotes transparency by regularly informing parliament and the public about the parliamentary oversight committees' work.

Italy, COPASIR (2017); France, DPR (2017); Germany, PKGr (2016); and United Kingdom, ISC (2016)

Reporting on number of parliamentary committee sessions

In Italy, France, Germany and the United Kingdom, parliamentary oversight committees report on the number of sessions held during the reporting period. This allows the public to be informed about the amount of time invested in overseeing the work of intelligence services.

Italy, COPASIR (2017); France, DPR (2017); Germany, PKGr (2016); and United Kingdom, ISC (2016)

Reporting on content of parliamentary committee hearings

The United Kingdom's ISC provides in its annual report a link to the transcripts of the hearings held during the reporting period, hosted on its website, thereby providing a significant level of information about its work

United Kingdom, ISC (2016)

Reporting on number of staff of intelligence services

The United Kingdom's ISC and the French DPR specify the number of staff working for each of the intelligence services. This means the public is informed about the size of intelligence services.

United Kingdom, ISC (2016); and France, DPR (2017)

Availability of expert bodies' annual reports in English

The Belgian Standing Committee I, the Dutch CTIVD, the French DPR, the Danish TET and the Greek ADAE publish their respective annual reports in both the original language and in English. This promotes cooperation and a better understanding of the oversight bodies' work beyond national borders.

Belgium, Standing Committee I (2016); Netherlands, CTIVD (2016); France, DPR (2017); Denmark, TET (2017); and Greece, ADAE (2016)

Reports on safeguard breaches by intelligence services

The United Kingdom's IOCCO reports on interception errors by the intelligence services. IOCCO lists the safeguards provided by the surveillance legislation and presents statistics on the breaches per safeguard by the intelligence services.

United Kingdom, IOCCO (2016)

Reports on number of individuals under surveillance

The French CNCTR and the German G10 Commission's annual reports provide statistics on the number of individuals that were under surveillance during the reporting period. The data come from the exercise of the oversight powers granted to these expert bodies.

France, CNCTR (2016); Germany, Federal Parliament (2017)

Report on intelligence services cooperation

The Belgian Standing Committee I's annual report published in 2016 presents the committee's endorsement of international cooperation of intelligence services regarding foreign terrorist fighters. In the report, the committee also outlines a number of principles that should govern international cooperation among intelligence services as well as its oversight.

Belgium, Standing Committee I (2016)

When discussing transparency requirements, representatives of oversight bodies most often referred to their reports or other publications. The reports include annual reports, activity reports, investigation reports and other specific (occasional, thematic) reports, in addition to mandatory reports. In most cases, there are two versions of the reports prepared by oversight bodies: classified and declassified, or secret/redacted and public versions. Similarly, reports may include a confidential annex.

Representatives of oversight bodies described the reports as substantive, detailed and lengthy. They stated that discussions with the executive control and intelligence services on what is to be declassified in their reports are sometimes quite intense. The oversight body representatives also indicated that, with nearly every report or publication, they attempt to provide 'more transparency', 'to push the limit', to be able to report as much as possible, and to explain and substantiate why certain information is kept secret and cannot be published. This is viewed as contributing to the changing nature of the 'secret culture'. Other actors who engage in democratic control – mostly civil society representatives – have observed such changes, too.

Question: *"Do you have lots of discussions whilst the report is being drawn up?"*

Answer: *"Yes. This was particularly the case with the first report, in connection with which there was a real desire to educate and explain matters properly."*

(Parliamentary committee)

"Have we actually got more in our report? The answer is we do and I think that, following Mr. Snowden, there was undoubtedly greater pressure to put more in and this new legislation is a good example, where much more openness is being encouraged and I think we will go on pressing..."

(Expert body)

Many oversight body representatives said that it is important for the general public to know that some information is classified/secret/redacted, rather than publishing a report and implying that it is complete. They noted that the arguments for excluding certain information from reports are important and should be communicated.

"I think people need to realise how much of what we do is secret and it is such a small amount, and it really is only when there are real national security issues." (Expert body)

Respondents also talked about opinions, recommendations and proposals, and studies on specific issues that respond to specific requests or are initiated by the oversight bodies themselves.

The interviewees considered any other information to the general public or specific interest groups (e.g. journalists) to add to transparency – for example, information on the website, communications to encourage individuals to appeal to the review body, the ability to initiate 'contact' through the website, press releases, provision of information to media 'on request', and making decisions (judgements) available on the website. Participation in conferences and other events was mentioned by several respondents as ways to hold discussions within a wider international framework, as well as with civil society and the media.

Representatives of civil society organisations, academia, lawyers and some national human rights institutions tended to be critical of the content of oversight body reports and their transparency in general, and indicated they expected more. The main criticism was that there is very limited information on actual activities and little explanation of how the oversight or review is carried out, while the main focus is on describing the relevant legal basis.

"I think one third of the report is what they regularly say every two years... 'this is our legal basis...', and I say 'this is not what I want to know'. I want to know a bit more about their work." (National human rights institution)

"It sets out what it does, on what legal basis... blah, blah, blah. And there's nothing else in there. Absolutely nothing."

(Academia)

"But when it comes to the substantive issues, let's say: what have we learned from the [expert body]? How many interceptions have there been? Not just how many times did we meet, but what was the substance of that discussion. Were there any novel decisions? Were there any novel technologies that came to our attention? I want to know about this." (Civil society organisation)

"What's actually going on? We always had a feeling or hints that what was revealed in the Snowden revelations was in one form or another happening. But no one really knew substantially. The reform just now, even many members of parliamentary oversight committees I have talked to, say they only learn about these things from the media - and not from the official channels they are supposed to learn them from..." (Media)

Respondents representing various institutions mentioned diverse ways to improve transparency and to make themselves more open. Some spoke of possible improvements with regard to reporting (e.g. 'The reports could also go a little further without impacting on confidentiality concerns'). Others noted that the bodies should themselves be able to decide on what to report. Some expected legal reforms to introduce mandatory reporting by oversight bodies. Several representatives of expert oversight bodies mentioned

hiring communications consultants to improve communications (regarding information to the public, by reviewing/editing the reports 'to help turn our language into something that is accessible to anybody and to try and make it more obvious'). The recent disclosure of the location of an office was mentioned as an example of positive change.

Respondents representing different institutions and organisations pointed to different recent examples that they believed showed changes in the predominant culture of secrecy. Such developments involve both the intelligence services and oversight bodies. With regard to the intelligence services, for example, civil society members from the Netherlands noted that the head of the intelligence service is publicly known, is willing to participate in different forums, and 'is approachable'. Intelligence service representatives attend conferences and other public events, including some organised by academia. Examples of comments about changes in the United Kingdom include: 'you go to conferences now and you find people engaged in a civilised discussion with people from security side about the issues'; a round table convened 'a quite high profile group of individuals both from the government side and the agencies, and the existing oversight bodies, but also from privacy campaign side and individuals who are bringing cases'. Meanwhile, in Germany, after the Snowden revelations, the parliamentary control panel for the first time published its rules of procedure on its website.[366]

Respondents indicated that intelligence actors' participation in, and presentations at, national parliamentary hearings make important contributions to transparency. Members of parliamentary committees referred to these hearings, some of which are public, as an important information channel for the public who can watch, e.g., the heads of the intelligence services being interviewed.

366 Germany, Federal Parliament (*Deutscher Bundestag*) *Parliamentarisches Kontrollgremium (*2016), Rules of Procedures (*Geschäftsordnung*).

10 Stages of intelligence service oversight



Effective oversight of surveillance operations requires potentially being present at every stage. The ECtHR refers to this as 'continuous control' in the *Roman Zakharov* case. Factors that have a bearing on the effectiveness of oversight include: the independence of the relevant body, the scope of measures requested (targeted or general surveillance of communications; content or metadata; domestic or foreign), its powers to access or request information, and its resources – in terms of staff, time and expertise, including with a view to the number of warrant requests received. For *ex ante* oversight, the level of required detail in a warrant and the time period for which the warrant is provided is also relevant, especially in cases where ongoing oversight is weak.

This report's discussion of the implementation of the standards gives particular attention to ongoing and ex post oversight. A more detailed treatment of such oversight is given below, because it is at the stage of implementation of surveillance measures that safeguards on general surveillance of communications operations are most relevant.

ECtHR case law: stages of oversight

"Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 233

10.1. *Ex ante* authorisation and oversight

ECtHR case law: *ex ante* authorisation

"The Court will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 257

"The Court recalls that [...] it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 77

UN good practice on intelligence collection and oversight

Practice 22. [...] Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Continuity of oversight of surveillance operations requires, among others, that independent oversight be present at the stage when the surveillance measures are first ordered. The overseers must therefore be informed at once of the issuance of warrants. 'Authorisation' entails the issuing of a warrant, while 'approval' refers

to the review of a signed warrant before it is put into effect. Ex ante authorisation or approval by independent overseers is not yet common in EU Member States, but can be seen as a promising practice both to ensure that surveillance operations are fully justified as necessary and not ordered arbitrarily, and to enable meaningful ex post review of the warranted operations. Ex ante oversight may either take the form of the independent body actually authorising the warrant or of conducting an approval process involving independent review of a signed warrant before it enters into force.

"The ideal situation would be to never have to say 'no'. This is what I would like to aim for in the future; an understanding of the intrinsic and legal limits [by the services]." (Judiciary)

Supervision by the judiciary or experts

"[T]he value of judicial control depends upon the expertise the judges in question have in assessing risks to national security and in balancing these risks against infringements in human rights."

Council of Europe, European Commission for Democracy through Law (Venice Commission) (2007), Report on the democratic oversight of security services, *para. 206*

In Belgium, the State Security, before using exceptional methods of surveillance, must submit a duly motivated, written request to the Administrative Commission.[367] The Administrative Commission gives its opinion on such requests within four days. If the decision is negative, the proposed measures may not be implemented.[368] In case of a positive decision, the Administrative Commission notifies the Standing Committee I, which can overrule the commission's decision.[369]

In the United Kingdom, the double-lock system was introduced in 2016. It will require, once in force, that warrants or notices for both targeted surveillance and using bulk powers be authorised by the Secretary of State[370] and subsequently approved by the Judicial Commissioner.[371] The Judicial Commissioner is required to review whether the warrant or notice is necessary on relevant grounds and whether the measures applied for are proportionate to their aim. The warrant or notice can take effect only after the Judicial Commissioner has approved it.[372] Warrants are valid for six months,[373] and retention notices can require the retention of data for 12 months.[374] In the case of bulk interception warrants, for example, the requested measure should relate to the interception of overseas-related communication (either content or metadata). This means that for the communication to be intercepted, it must be sent or received by someone outside British territory.[375] In authorising the measures, the Secretary of State must ascertain that they are necessary to prevent serious crime, and/or ensure the economic well-being or national security of the state.[376] The Judicial Commissioner then reviews whether the measures are necessary and proportionate and can quash a warrant if not satisfied.[377]

However, with regards to the effectiveness of ex ante reviews of bulk measures, it is noteworthy that the core requirement in the UK system regarding the contents of the warrant is that it must specify the operational purpose(s) of the requested measures "in a greater level of detail" than described above.[378] Thus, in turn, the actual strength of the *ex ante* review relating to the necessity and proportionality of the requested measures will, to a great extent, depend on the level of detail regarding the purposes. This is relatively straightforward for simple targeted warrants where the specified individuals or premises are known and can be specified. For warrants for surveillance involving bulk measures not only must the objective relate to a sufficiently high intelligence priority but the review will have to take into account what has been

367 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 18 (10).
368 *Ibid.* Art. 18 (10)(3).
369 *Ibid.* Art. 18 (10)(7).
370 United Kingdom, Investigatory Powers Act, s. 19 for interception and examination, s. 87 for retention of communications data, s. 102 for equipment interference. S. 19 and 102 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
371 *Ibid.* s. 23 for interception and examination; and s. 87 (1) (b) for retention notices, s. 102 (1) (d). ss. 23 and 102 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
372 *Ibid.* s. 23 (1) for interception and examination, s. 89 (1) for retention, s. 108 (1) for equipment interference. Ss. 23, 89 and 108 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
373 *Ibid.* s. 32 (2) (b) for interception and examination, s. 116 (2) (b) for equipment interference. Ss. 32 and 116 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
374 *Ibid.* s. 87 (3).
375 *Ibid.* s. 136 (2)-(3). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
376 *Ibid.* s. 138 (2). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
377 *Ibid.* s. 140. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
378 *Ibid.* s. 142. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

previously established by the oversight body regarding the compatibility of the methods used (access, filtering and selection algorithms) to ensure the activity under the warrant will be compatible with privacy rights (Article 8 of the ECHR). In that way the overseer must, in the words of a UN Special Rapporteur, conduct the review such that "it is possible to make an objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation."[379]

Authorisation and approval of targeted surveillance

A detailed comparison of authorisation and approval processes for targeted measures is difficult, as they may vary within Member States depending on the different types of surveillance measures involved, whether they relate to content or metadata, and whether they have a domestic or foreign focus. Table 4 shows the different bodies that have a binding/final decision in the authorisation or approval processes of different types of targeted surveillance measures relating to content data. The information provided for one Member State covers all potential actors with a binding decision-making power in allowing targeted surveillance measures. Six Member States have two or more approval bodies. In some cases (e.g. in the United Kingdom), one body is in charge of authorising and the other one of approving the measures. In others (e.g. in Hungary), the involvement of different bodies depends on the type of techniques used by the intelligence services.

Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-28

	Judicial	Executive	Expert bodies	Services
AT			✓	
BE		✓	✓	
BG	✓			
CY		✓		
CZ	✓			
DE		✓	✓	
DK	✓			
EE	✓			
EL	✓			
ES	✓			
FI	✓			
FR		✓		
HR	✓			
HU	✓	✓		✓
IE		✓		
IT	✓			
LT	✓			
LU		✓		
LV	✓			
MT		✓		
NL*	✓	✓	✓	
PL		✓		✓
PT	✓			
RO	✓			
SE	✓			
SI	✓			✓
SK	✓			
UK**	✓	✓		

Note: * *Situation reflecting the requirements of the Intelligence and Security Services Act 2017, which will be applicable when the relevant sections enter into force.*

** *Situation reflecting the requirements of the Investigatory Powers Act, which will be applicable when the relevant sections enter into force.*

Source: *FRA, 2017*

379 UN, Human Rights Council (2014), Report of the Special Rapporteur Ben Emmerson, para. 7.

In general terms, as Table 4 illustrates, just over half of the Member States involve the judiciary (judges or prosecutors) in ex ante oversight, in relation to at least one type of targeted surveillance measure. In Portugal, the new law provides for access to metadata by intelligence services to be authorised by a judicial panel composed of the presidents of all criminal sections of the Supreme Court and a judge appointed by the Superior Council of Magistrates.[380] In Italy, requests for targeted interception measures need to be authorised by the Prosecutor General of Rome.[381] Three Member States – Austria, Belgium and Germany – involve expert bodies in all approval processes. At the same time, in six Member States – Cyprus, France, Ireland, Luxembourg, Malta and the Netherlands – all types of targeted surveillance measures may be implemented without ex ante oversight by an independent body with binding decision powers. In France, for example, requests for targeted surveillance measures are authorised by the prime minister after a non-binding opinion of the CNCTR, upon the receipt of a detailed request by the relevant minister, outlining the technique(s) to be used; the service for which it is presented; the purpose(s) pursued; the reason(s) for the measures; the period of validity of the authorisation; and the person(s), place or vehicles concerned.[382]

Ex ante oversight

There is growing support for extending external authorisation to:

- untargeted bulk collection of information;
- the use of key words or selectors to extract data from the information collected through bulk interception, particularly where they are related to identifiable individuals;
- the collection of and access to communications data (including when held by the private sector); and
- computer network exploitation.

Council of Europe Commissioner for Human Rights (2015), p. 62

Authorising general surveillance of communications

Unlike targeted surveillance, general surveillance of communications – at least during its initial stages – targets not an individual but rather large flows of data. As a consequence, such measures do not usually allow for an individualised proportionality analysis. *Ex ante* authorisation or approval has to focus on the seriousness of the objective of the operation as an intelligence requirement, the level of proportionality, and whether access, filtering and selection algorithms use discriminatory criteria. The analysis must establish whether the proposed operations are compatible with privacy rights. Table 5 presents the actors that have a binding/final say in the approval of general surveillance of communications measures in the five Member States that have detailed legislation on such surveillance measures.

In Sweden and Germany, an expert body is in charge of authorising the intelligence services to gather signals intelligence. In Sweden this is carried out by the Defence Intelligence Court, which can have four to nine members: two or three ordinary judges (the chair and vice chair; there can be a second vice chair), and two to six lay members.[383] The panel that hears a case and grants authorisations must be composed of at least the chair and two lay members (and not more than three lay members).[384] The government appoints all members. The chair and vice chair are appointed after an open recruitment process led by the Judges' Board (*Domarnämnden*).[385] Lay members of the court should have special knowledge in matters of importance to the court's activities.[386] The interests of individuals are represented by lawyers (*integritetsskyddsombud*) who are or have been members of the bar or served as judges, appointed for a four-year period.[387] The court may declare that its sessions are not public, and its decisions may not be appealed.[388]

In contrast, in France, when it comes to the use of the so-called 'algorithm', the prime minister authorises automatic processing based on selected parameters.[389]

380 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Art. 7.

381 Italy, Code of criminal procedure (*Codice di procedura penale*), Art. 266 and following and Italy, Implementing norms (*norme di attuazione*), Art. 226.

382 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 821-2.

383 Sweden, Act on the Defence Intelligence Court (*Lag (2009:966) om Försvarsunderrättelsedomstol*), 15 October 2009, Art. 2.

384 *Ibid.* Art. 9.

385 This is a government agency with a board consisting of nine members. Five members should have been judges; two should practice law outside of the court system (and one of these should be *'advokat'* (member of the bar)); and the remaining two should represent 'society' (presently two members of the national parliament).

386 Sweden, Act on the Defence Intelligence Court, Art. 3.

387 *Ibid.* Arts. 5 and 6.

388 *Ibid.* ss. 3, 5, 6, 9, 14 and 16. Details are provided in Sweden, Regulation 2009:968 with instructions for the Defence Intelligence Court. The website of the court is available in Swedish only. The court was established in 2009, replacing a previously existing Signals Intelligence Board.

389 France, Interior Security Code, Art. L. 851–3.

Table 5: Approval/authorisation of general surveillance of communications in France, Germany, the Netherlands, Sweden and the United Kingdom

	Judicial	Parliamentary	Executive	Expert
DE		✓		✓
FR			✓	
NL*	✓		✓	✓
SE				✓
UK**	✓		✓	

Notes: * *Situation reflecting the requirements of the Intelligence and Security Services Act 2017, which will be applicable when the relevant sections enter into force.*

** *Situation reflecting the requirements of the Investigatory Powers Act, which will be applicable when the relevant sections enter into force.*

Source: *FRA, 2017*

The CNCTR provides the prime minister with a non-binding opinion on both the automatic processing and the parameters. The oversight body is kept informed about every modification during the operation and has permanent, complete and direct access to this processing and the intelligence gathered. The first authorisation is valid for two months. It is renewable, but the renewal request should include the number of relevant targets obtained by the automatic processing and an analysis of their relevance. Should this data reveal the existence of a terrorist threat, the CNCTR again provides the prime minister with its opinion for authorising the identification of the person considered as threat. Since its creation in October 2015, no negative opinion from the CNCTR were overruled by the Prime Minister.[390]

As a general rule, when targeting communications' content data, prior oversight is required in most Member States for both targeted surveillance and the use of selectors in the context of general surveillance of communications. This changes, however, when intelligence services solely access metadata through rules governing access to retained data. In these cases, it is usually sufficient for the services' directors to authorise access.[391] This is problematic, because communications data reveal an individual's pertinent personal information in a similar way to content data.[392]

However, addressing any issue relating to prior oversight in isolation of the oversight system as a whole will not offer a complete picture of its effectiveness. Inevitably, national systems will strike different balances when designing their respective architecture of checks and balances. Consequently, apparent strengths or weaknesses of ex ante review may be undermined or remedied, respectively, in ongoing and ex post oversight.

10.2. Ongoing and *ex post* oversight

To meet the standard of continuity, oversight also needs to be present at the stage when the measures are being implemented – in other words, while the operations are ongoing – as well as at the time when they have already been concluded. In addition, oversight should cover all surveillance processes, from collection to the destruction of data.

The use of general surveillance of communications makes these functions of the oversight system particularly crucial safeguards, given that in such operations ex ante oversight will, by definition, have a limited scope of review. Ongoing and ex post oversight can also provide valuable insights in the form of feedback to the body authorising or approving general surveillance of communications. This section focuses on ongoing and ex post oversight of specific types of operations.

As Annex 5 illustrates, a number of Member States have expert bodies that undertake ongoing and ex post review, while only very few provide for judicial oversight during the implementation of surveillance measures. FRA's research shows that most Member States involve an independent oversight body either at the stage when surveillance measures are being implemented or after they have been concluded – or during both of these stages. Depending on the powers and competences of the oversight bodies at these stages, a combination of ongoing and ex post oversight may be the best approach.

390 France, CNCTR (2016), p. 66.

391 This is the case in the United Kingdom for targeted collection of metadata (Investigatory Powers Act, S. 61).

392 For the required safeguards in case of retention of data by telecommunications service providers, see CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Postoch telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, and the analysis of the case in the Introduction.

10.3. Exceptional situations and special protection

Two circumstances need to be considered separately because they derogate from the general framework of ordering and overseeing surveillance operations. These involve urgent operations, and surveillance of specific professional groups that benefit from enhanced protection.

Exceptional situations

ECtHR case law: safeguards for the use of urgent procedures

"[W]here situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours [...]. For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a *post factum* review, which is required, as a rule, in cases where the surveillance was authorised ex ante by a non-judicial authority."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 81

"[T]he Russian 'urgent procedure' does not provide for sufficient safeguards to ensure that it is used sparingly and only in duly justified cases. [...] The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure, thereby creating possibilities for abusive recourse to it [...]. Furthermore, although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed [...]. Russian law does therefore not provide for an effective judicial review of the urgency procedure."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 266

Member States' laws define cases of urgency as cases where undertaking the usual authorisation/approval procedures might irreversibly affect or undermine the purpose of the measures. This can occur because standard approval processes may take days. In urgent cases, safeguards are adapted to the extraordinary circumstances at issue, usually by way of a special ex ante approval procedure or via ex post approval. For example, Belgium provides for special ex ante approval in cases of "extreme urgency". In such cases, the head of the service may, with the approval of the Administrative Commission's president, authorise exceptional surveillance measures for up to 48 hours. The authorisation has to justify the use of the urgent procedure and has to be communicated to the members of the commission immediately.[393]

Examples of ex post approval can be found in France and the United Kingdom. In France, in case of "absolute emergency", the prime minister may authorise surveillance measures without the CNCTR's opinion. The prime minister is required to inform the CNCTR within 24 hours of giving the authorisation and justify the use of the urgent procedure.[394] Recourse to the urgent procedure was made only once between October 2015 and October 2016.[395] In the United Kingdom, in urgent cases, the Investigatory Powers Act foresees that a warrant can be issued for targeted interception and equipment interference as well as for bulk equipment interference and specific bulk personal datasets without the Judicial Commissioner's prior approval.[396] The Judicial Commissioner has to be notified and has three working days after the day the warrant was issued to decide whether or not they approve the warrant, and notify the authorising person. If the Judicial Commissioner refuses to approve then warrant, the implementing authority must, "so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible".[397] In addition, the Judicial Commissioner may decide to request the destruction of any material collected or impose conditions on its use or retention.[398]

Similarly, in Germany, a reform of the G 10 Law aligned the approval procedures in cases of emergency. While the competent federal ministry can provisionally approve

393 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 18 (10)(4).
394 France, Interior Security Code, Art. L. 821-5. The urgent procedure cannot be used when the services wish to use the so-called algorithm: France, Interior Security Code, Art. L. 851-3 V.
395 France, CNCTR (2016), p. 56.
396 United Kingdom, Investigatory Powers Act 2016, ss. 24 and 109 for targeted interception and examination, and equipment interference warrants respectively. S. 180 for bulk equipment interference, s. 209 for bulk personal datasets. Ss. 24, 109, 180, and 209 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
397 *Ibid.* ss. 25 (2); 110 (2); 181 (2); 210 (2) respectively. Ss. 25, 110, 181 and 210 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
398 *Ibid.* s. 25 (3). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

strategic surveillance, the chair of the Parliamentary Control Panel or the chair's proxy needs to give their provisional approval within three days, and full approval by the control panel has to be obtained within two weeks.[399] The surveillance measure can start before the G 10 Commission's approval but the data cannot be used. The approval request needs to take place with 24 hours.[400] In the context of foreign to foreign surveillance, the 2016 reform lists situations which qualify as emergency. The approval of the Independent Committee needs to be sought without delay. When a request is rejected, the data must be destroyed.[401]

Protected professions and privileged information

ECtHR case law: surveillance measures concerning media

"In the instant case, [...] the use of special powers would appear to have been authorised by the Minister of the Interior and Kingdom Relations, if not by the head of the AIVD or even a subordinate AIVD official, but in any case without prior review by an independent body with the power to prevent or terminate it [...]. Moreover, review post factum, cannot restore the confidentiality of journalistic sources once it is destroyed."

ECtHR, Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, paras. 100-101*

Special authorisation and approval procedures may also apply when the scope of the surveillance includes information protected by professional privilege. Member State laws often provide enhanced protection to certain professionals (e.g. media professionals, lawyers, judges). The Council of Bars and Law Societies of Europe (CCBE), for example, has adopted specific recommendations in this area.[402] In the Netherlands, several lawyers in 2015 filed a complaint in court, alleging that they had been under surveillance. The court decided that the procedure in place at the time for obtaining authorisation to intercept lawyers' communications was unlawful and violated the right to private life, in the absence of prior approval by an independent body.[403] At the end of 2015, this judgment as well as the ECtHR's decision in *Telegraaf Media Nederland Landelijke Media B.V. and Others* triggered a legislative amendment aiming to better protect journalists' sources. The Minister of the Interior and the Minister of Defence established an independent temporary commission to provide for the ex-ante oversight of surveillance operations in connection to the special powers included in the Intelligence and Security Services Act 2002, allowing for the tapping of lawyers and journalists. Since 1 January 2016, this commission, chaired by the chair of the CTIVD, gives binding advice to the ministers on the authorisation of measures that 1) may affect privileged lawyer-client communication or 2) are aimed at identifying journalists' sources.[404] The 2017 reform of the Dutch legislation transferred this authority to the Court of The Hague.[405]

In France, the law protects parliamentarians, lawyers, judges and journalists. Requests for surveillance measures in respect to these professionals must be considered by the CNCTR in a plenary session. The urgent procedure cannot be applied. Moreover, transcripts of the collected intelligence data must be transmitted to the CNCTR for a specific control of the necessity and proportionality of the risks entailed by targeting potentially privileged communication, assessed in terms of the need for enhanced safeguards.[406] The CNCTR outlined the scope of such enhanced protection, and provided definitions of the covered professional categories, in an opinion adopted in October 2015.[407]

CNCTR on enhanced protection for certain professions

"Any person, irrespective of nationality who, in France, his country of origin or internationally, exercises one of the professions cited in the law or holds a mandate of similar nature to that of French parliamentarians, shall enjoy the protection of the law."

France, CNCTR (2016), p. 102 [FRA translation]

Similarly, the United Kingdom provides for enhanced safeguards when interception or equipment interference would target parliamentarians or communications protected by legal privilege, would include confidential journalistic material, or where its purpose is to identify or confirm a source of journalistic information.[408]

399 Germany, G 10 Act, S. 14 (2).
400 *Ibid.* ss. 10 and 15 (6).
401 Germany, BNDG, S. 9 (4).
402 See CCBE (2016).
403 The Netherlands, District Court The Hague (*Rechtbank Den Haag*), Case No. C/09/487229/KG ZA 15-540, 1 July 2015.
404 Netherlands, Minister of the Interior and Kingdom Relations & Minister of Defence *(Minister van Binnenlandse Zaken en Koninkrijksrelaties & Minister van Defensie)* (2015). accessed on 12 February 2016.
405 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) Arts. 27 and 30.
406 France, Interior Security Code, Art. L. 821-7.
407 France, CNCTR (2016), p. 102 and following. See also the pending case ECtHR, *Association confraternelle de la press judiciaire v. France*, No. 49526/15.
408 United Kingdom, Investigatory Powers Act 2016, for interception: ss. 26-29; for equipment interference: ss. 111-114. Ss. 26-29 and 111-114 are yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note). See also ECtHR, *10 Human Rights Organisations and Others v. the United Kingdom*, No. 24960/15, pending before the ECtHR.

In Sweden, the law specifies that all gathered intelligence concerning communications of persons bound by legislated professional secrecy, suspects or accused and their defence counsel, as well as statements given in confession to a priest must be immediately destroyed.[409]

Interestingly, in Belgium, aside from lawyers and journalists, the law includes doctors among professionals of whom surveillance is in principle prohibited.[410] Exceptionally and when strictly necessary, the law prescribes enhanced safeguards for the authorisation of interceptions of the protected professions' communications. One of the safeguards envisaged is that, depending on the profession, the President of the Order of French and German speaking Bar Associations, the President of the Order of Flemish Bar Associations, the President of the National Council of Doctors or the President of Professional Journalists Association must be notified by the Administrative Commission prior to the implementation of the surveillance measure. The Administrative Commission must provide all necessary information to the presidents of these professional associations.[411]

In Germany, federal law provides enhanced protection to various professionals bound by professional secrecy – such as members of parliament, faith leaders and lawyers – only in case of targeted surveillance.[412] Enhanced protection is not available in case of strategic or foreign-to-foreign surveillance.

409 Sweden, Signals Intelligence Act, Art. 7.
410 Belgium, Organic law on intelligence and security services (*loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 2 (2), as amended.
411 *Ibid.* Art. 18/2 (3), as amended.
412 Germany, G10 A, S. 3b in conjunction with Code of Criminal Procedure, S. 53. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1201, p. 1252 and following and p. 1268.

11

Oversight of international intelligence cooperation



The internationalisation of threats led to an increased need for joint operations and the intensification of international communication and data exchanges between intelligence services. This in turn means that intelligence activities have become more diverse and include a growing cross-border element.

11.1. Specific safeguards

UN good practice on authorisation process

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

UN good practice on circumvention of national obligations through intelligence-sharing

Practice 35. Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The specificities of international intelligence sharing require Member States to establish safeguards that are tailored to these processes. These include – but are not limited to – prior approval of any agreement or pattern of cooperation by the executive, the implementation of fundamental rights risk assessments, strong guarantees for protection of sources and personal information, data reliability assessments and the obligation to keep records.

As identified by Born, Leigh and Wills, "requirements of this kind have a number of benefits. They establish a clear framework for approval of cooperation activities. They can help to ensure that cooperation is aligned with the government's foreign policy, defence, security, and diplomatic objectives and does not unwittingly undermine or contradict these. They ensure that political overseers have an understanding of the arrangements that the state's services have with partners. They allow for scrutiny to take place of any risks of particular partnerships at an appropriate political and managerial level."[413] Prior approval may be required before the establishment of the agreement and/or before the exchange of data.

In almost all Member States, intelligence services must obtain the approval of the executive before concluding an international agreement. Only in Slovenia is international intelligence cooperation at the discretion of the head of the service.[414]

In the Netherlands, under normal circumstances, decisions to cooperate with foreign services lie with the head of the service. However, authorisation by the

413 Born, H., Leigh, I. and Wills, A. (2015), p. 93.
414 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*), 7 April 1999, Art. 7.

relevant ministers is mandatory before collaborating with 'high-risk services'.[415] Cooperation criteria are not spelled out in the 2002 Act. Over the years, the Dutch oversight body carried out several investigations into this matter and issued recommendations to the relevant minister. These were partially incorporated into Articles 88 to 90 of the 2017 Law replacing the 2002 Act.[416] The law provides for a compulsory risk assessment before entering into a cooperation agreement. The assessment will serve not only to identify potential risks inherent in the cooperation, but also what type(s) of cooperation may be established by the intelligence services. Furthermore, the law requires ministerial approval, which can be delegated to the head of the service.[417] The CTIVD expressed some criticisms when the law was being debated in parliament and maintained that additional privacy- and data protection-related safeguards should be included.

In Sweden, the Ministry of Justice must only be briefed before the cooperation takes place.[418] Four Member States – Denmark, Germany, Hungary and Lithuania – require an additional form of approval before the actual exchange of data may take place. Such approval can be given either by the executive, the judiciary or by the head of the services. In Germany, strategic surveillance data exchange requires the agreement of the Federal Chancellery.[419] Foreign-foreign surveillance data can only be transferred to foreign intelligence services of EU, European Economic Area (EEA) and NATO Member States if such a transfer was approved by the Federal Chancellery. For any other country, additional approval by the Head of the Chancellery is needed.[420]

UN good practice on intelligence sharing

Practice 33: Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

UN, Human Rights Council, Report of the Special Rapporteur Martin Scheinin

415 The Netherlands, CTIVD (2016b), p. 5.
416 The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Arts. 88-90.
417 The Netherlands, CTIVD (2016b), p. 8 and following.
418 Sweden, Regulation on Defence intelligence service *(Förordning [2000:131] om försvarsunderrättelseverksamhet),* 30 March 2000, pp. 3 and 4.
419 Germany, G10 Act, S. 7a.
420 Germany, BNDG, S. 13 (5).

Fundamental rights risk assessments in international cooperation

"Intelligence service managers should put in place risk assessment processes for international intelligence co-operation that set out the factors which must be considered before undertaking particular types of cooperation. [...] The executive should ensure that there is cross-government sharing of appropriate information on countries' human rights records as this assists services in undertaking risk assessments."

Born, H., Leigh, I. and Wills, A. (2015), pp. 109 and 112

In 2016, while encouraging nations to establish intelligence-sharing platforms to better combat terrorism, the UN General Assembly stressed that any counter-terrorism effort should not neglect the rule of law, human rights and fundamental freedoms.[421] As a general rule, democratic states are keen to share information with partner states where similar democratic structures are guaranteed. To ensure this, some Member States – such as Croatia, Germany and the Netherlands – conduct risk assessments, i.e., a global evaluation of several factors, such as the legal principles regulating the potential partners' activities, the international political context in which foreign states operate, existing bilateral or international agreements, and/or an assessment of respect for fundamental rights.[422]

Risk assessments are conducted based on guidelines that are not accessible to the public. However, the 2016 CTIVD review report on the implementation of cooperation criteria spells out the various cooperation criteria taken into account before entering into a cooperation agreement:

- respect for human rights and democratic anchorage,
- professionalism and reliability of the foreign intelligence service,
- advisability in the context of international commitments,
- whether cooperation would enhance the performance of tasks and
- reciprocity rule.[423]

The assessment of potential partners' 'human rights footprint' is crucial. Indeed, as highlighted by Born, Leigh and Wills, "concerns about the human rights "foot print" of incoming information go beyond the implications for reliability; they also include possible legal implications of using such information".[424]

421 UN, GA (2016b), pp. 6 and 8.
422 Born, H., Leigh, I. and Wills, A. (2015), pp. 108-110.
423 The Netherlands, CTIVD (2016b), p. 5 and following.
424 Born, H., Leigh, I. and Wills, A. (2015), pp. 112-113.

When assessing the general level of human rights compliance, some Member States focus their analysis on specific rights, such as data protection and the protection of sources. This is the case, for instance, in Denmark,[425] Germany[426] and Slovenia,[427] where ensuring that a data protection framework exists in the recipient state is a pre-condition for any information sharing and disclosure of personal data. In addition, some Member States, such as Luxembourg,[428] require specific protection of sources of information.

Reliability of data: caveats and reliability assessments

"Intelligence services should ensure that caveats are attached to information shared with foreign partners."

"Caveats should set out in unambiguous terms the use to which that information may be put and with whom it may be shared."

"Reliability assessments should be attached to intelligence shared with foreign partners, particularly where it relates to identifiable individuals."

Born, H., Leigh, I. and Wills, A. (2015), pp. 114 and 115

Reliability of the received data is, indeed, crucial – not only to ensure a correct implementation of intelligence strategies, but also for the protection of fundamental rights. To secure reliability of the data, Member States may attach a specific caveat[429] to the transfer of data and/or conduct data reliability assessments. Germany, for instance, includes "appropriations clauses" that specify that the data cannot be used for a different purpose than the one for which they were originally collected, and that the use must respect democratic principles.[430]

It is difficult for intelligence officers to know the source of the data collected by foreign organisations or the conditions under which they were collected. There is therefore a potential for misguided decisions, affecting the implementation of intelligence strategies and the protection of fundamental rights.

A well-known example of the reliability question crystallised around the source of information that led the US into the 2003 Iraq invasion. Crucial data collected by the German intelligence service (BND) through an Iraqi source known as the "Curveball" was handed over to the CIA, but the reliability of the source, and consequently of the data transmitted, was later questioned.[431] The BND highlighted that doubts about the reliability of such information were earlier communicated to their American partners through caveats. This example illustrates the difficulties faced by agents in assessing the data they receive, and the vital importance for all intelligence services, senders and receivers, to attach data reliability assessments and caveats to the data transferred.

Caveats may also ensure greater transparency on the use of the data received, and therefore, more accountability on the lawful purpose for exchanging data. As emphasised by experts,[432] one of the risks inherent in international sharing of data is the possibility for intelligence services to circumvent domestic obligations by getting partners to collect or process data in ways that would have been deemed unlawful under national law. Such a practice is explicitly prohibited in the United Kingdom.[433] In Germany, both the BNDG and the G10 Act provide that intelligence services must seek written agreements from their foreign counterparts that guarantee that the information received was not collected or processed through activities contrary to rule of law principles.[434]

This is important to ensure compliance of intelligence measures with fundamental rights. As pointed out by several civil society organisations, the increasing practice of intelligence-sharing has reinforced the risk of such arrangements being used to infringe fundamental rights principles. Several civil society organisations around the globe – including three from EU Member States, specifically Hungary, Ireland and the United Kingdom – have decided to challenge the secrecy governing international intelligence cooperation by requesting access to the agreements under freedom of information rules.[435]

425 Denmark, Act on the Danish Security and Intelligence Service, section 10(2) and (4), cf. section 7.
426 Germany, G10 Act, S. 7a (1).
427 Slovenia, Slovene Intelligence and Security Agency Act, Art. 12 (11).
428 Luxembourg, Act of 5 July 2016 on the reorganisation of the State Intelligence Service, Art. 11 (4).
429 Born, H., Leigh, I. and Wills, A. define 'caveat' as "conditions restricting the use of information shared with a partner intelligence service", Born, H., Leigh, I. and Wills, A. (2015), p. 97.
430 Germany, BNDG, S. 13 (3).
431 See Born, H., Leigh, I. and Wills, A. (2015), p. 39; see also Lefebvre N. (2015), p. 29.
432 See Born, H., Leigh, I. and Wills, A. (2015), pp. 48-50, and UN, Human Rights Council, Scheinin, M. (2010), p. 29.
433 United Kingdom, Investigatory Powers Act, s. 9 and s. 10.
434 Germany, BNDG, S. 13 (3) and Germany, G10 Act, S. 7a
435 See International Network of Civil Liberties Organisations (INCLO) (2017), *International Intelligence-Sharing Project,* and Privacy International v. National Security Agency, Office of the Director of National intelligence, Department of State, and National Archives and Records Administration (Five Eyes FOIA), 5 July 2017.

Recording and tracking obligation

"Legislation should include provisions on the duty of record keeping for international intelligence cooperation, in particular, concerning the exchange of information with foreign partners."

Born, H., Leigh, I. and Wills, A. (2015), p. 94

To ensure adequate accountability, it is essential that intelligence services track and keep records of all transactions with foreign partners. Some EU Member States – including Croatia, Estonia, Germany and Hungary – have included such obligations in their laws governing the functioning of such services.[436] Recording obligations may be hampered, though, by the so-called 'third party rule' – further discussed in Section 11.3. Indeed, some partner and allied services only provide intelligence on the understanding that the receiving service will seek permission before disclosing it outside the intelligence community, and that such permission may be denied. Such a rule, referred to as the 'control principle', is widely adhered to within intelligence communities to ensure trust among partners.

In Germany, transfers have to be documented. The exchange agreement must state that the data may only be used for the same purpose for which they were transferred, and that the German intelligence service from which the data originate reserves the right to ask how data are used.[437] Receiving parties have to sign up to purpose limitation, to keep tag on the data that indicates their origin from telecommunication surveillance, and to provide information about further use on request of the BND. Similarly, in Croatia, the submitted data must be documented, including a written disclaimer that the information provided can only be used for the purposes for which they were provided.[438] In both Germany and Croatia, intelligence services include in these caveats the right to seek feedback on how the submitted data are used. In Germany, such caveats must be clearly indicated before the cooperation starts: the intelligence services must include, in the intent of cooperation that is transmitted to the Federal Chancellery for approval, these two agreements with the foreign partner, on purpose limitation and *a posteriori* information of the use made of the data.[439]

436 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 60 (3), Estonia, Security Authorities Act, s. 34; Germany, BNDG, S. 15 (2) and Germany, G10 Act, S. 7a (3); Hungary, Act CXXV of 1995 on the National Security Services, s. 46.
437 Germany, BNDG, S. 13 (3) and Germany, G10 Act, S 7a (4).
438 Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*), Official Gazette (Narodne novine) Nos. 79/06 and 105/06, 30 June 2006, Art. 60.
439 Germany, BNDG, S. 13 (3) and Germany, G10 Act 7a (4).

Prior controls and authorisations must be complemented by ex post controls, which can be performed internally or externally. However, oversight of international arrangements requires access to information relating to activities and data transfers conducted under international cooperation. In 2016, the CTIVD expressed regret that the draft intelligence bill did not include a recording requirement. According to the Dutch Review Committee, to enable internal and external control, "personal data should be provided exclusively in writing".[440] This is the case, in particular, for exchange of large volume of data that did not go through any evaluation from the services before being exchanged.[441]

11.2. Limited but existing oversight

UN good practices on oversight of international cooperation

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

UN, Human Rights Council, Report of the Special Rapporteur Martin Scheinin

ECtHR case law: external supervision of international cooperation

"The governments' more and more widespread practice of transferring and sharing among themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 78

Although essential for ensuring fundamental rights compliance and boosting trust among intelligence service partners, the laws of a majority of Member states – 17 out of 28 – do not enshrine a clear provision stating whether, and to which extent, oversight bodies have competence over international cooperation. The absence of such a legal basis obliges both intelligence services and oversight bodies to interpret the legal framework to define whether, and to what extent, oversight bodies may assess international exchanges of data. To be lawful, any measure that interferes with privacy must first and foremost be prescribed by law. In the United Kingdom, for example, the Interception of

440 Netherlands, CTIVD (2016a), p. 10.
441 The Netherlands, CTIVD (2016d), p. 27.

Communications Commissioner questioned the extent and exact scope of his remit in this area in his 2013 annual report.[442] Similarly, in Germany, a member of the G 10 Commission wondered to what extent the third party rule limits the commission's oversight over data transfers, when the G 10 Act does not refer to any limitation.[443] In some Member States, the absence of specific reference may be understood as a *de facto* application of the domestic oversight system to international cooperation.

> *"Legislation should include provisions that oblige the service and/or executive to inform the intelligence oversight body about international intelligence cooperation agreements."*
>
> *Born, H., Leigh, I. and Wills, A. (2015), p. 94*

> *"The legislative mandates of bodies that oversee the intelligence services [...] should make clear that their role and powers extend to relevant intelligence cooperation and activities of the services they oversee."*
>
> *Born, H., Leigh, I. and Wills, A., (2015), p. 190*

Eleven EU Members States have laws that specify the legal basis for oversight bodies to oversee international cooperation. Of these, three – France, Ireland and Spain – have excluded information originating from foreign services from the scope of oversight. Four – Denmark, Finland, the Netherlands and Romania – do not differentiate between the oversight regime for international sharing of data. Three – Luxembourg, Portugal and Sweden – have limited the scope of the control over such information. In Germany, the scope of competences of the oversight bodies depends on the type of surveillance conducted: it is limited for strategic surveillance, and similar to domestic oversight for foreign-to-foreign data transfers. The following paragraphs introduce some of the specificities of the legal frameworks prohibiting, allowing or limiting national oversight over international intelligence cooperation.

In the Netherlands, the CTIVD conducted several investigations into the legality of international cooperation.[444] In 2015, it conducted two investigations following requests from the House of Representatives, on the criteria for establishing cooperation and on the prior ministerial approval required before any exchange of data. The CTIVD concluded that the intelligence services' systematic acquisitions of personal data were done lawfully, but still deemed current privacy safeguards inadequate, and suggested enhancing them.[445] The CTIVD added that "the potential of the General Intelligence and Security Service of the Netherlands (AIVD) [...] to infringe privacy in the digital domain goes further than was foreseen when the ISS [Intelligence and Security Services] Act 2002 was drafted and enacted", and found some procedures that govern the intelligence services unlawful, calling for stricter oversight of the services' digital activities.[446] Based on past review reports, the CTIVD also emphasised that "the services have not yet been able to establish a procedure that ensures their consistent compliance with the statutory safeguards when selecting from untargeted interception (SIGINT)."[447]

In Belgium, the Standing Committee I in 2013 launched an investigation regarding one of the missions of the Coordinating Unit for Threat Analysis (OCAM), which establishes and maintains contacts with foreign partners. This investigation, jointly conducted with the Standing Committee P, followed previous similar investigations in 2009 and 2011 on OCAM's international activities. Concluded in 2015, the investigation recalled that OCAM is not an intelligence service as such, and therefore the foreign counterparts with whom it may establish cooperation should be better defined.[448] The oversight body clarified, though, that a directive regulating OCAM's international cooperation was adopted by the national security council after the investigation concluded.[449]

In France, Spain and the United Kingdom, similar wording included in the respective acts regulating intelligence services exempt "information communicated by foreign services or international organisations" from the remit of parliamentary oversight commissions,[450] as well as, in the case of France, the independent expert oversight body (CNCTR).[451]

In Luxembourg, Portugal and Sweden, the oversight bodies are not expressly tasked with overseeing international data transfers and they generally cannot exercise their full competences over international intelligence cooperation. However, in these four Member States, the body charged with ensuring the control of domestic intelligence activities must be informed of data transfers. In Sweden, for instance, the intelligence services must inform the Swedish

442 United Kingdom, IOCCO (2013), p. 62.
443 Huber, B., *in*: Schenke, W. et al. (eds.) (2014), p. 1451 and following.
444 See The Netherlands, CTIVD (2009), (2016), (2016a), (2016b) and (2016c).
445 The Netherlands, CTIVD (2014), p. 37 and following. See also The Netherlands, CTIVD (2015), p. 28.
446 The Netherlands, CTIVD (2014), p. 5.
447 *Ibid.* p. 28.
448 Belgium, Standing Committee I (2016), p. 33-37.
449 *Ibid.* p. 34.
450 France, Ordinance no. 58-110 of 17 November 1958 related to the functioning of parliamentary assemblies (*Ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires*), Art. 6 nonnies; Spain, Law 11/2002 of 6 May, regulation of National Intelligence Centre (*Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia*), Art. 11 and the United Kingdom, Justice and Security Act 2013, schedule 1, para. 5 (c).
451 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-2. - IV.

Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten*) of the principles applied in their international cooperation and the countries and/or organisations they cooperate with.[452]

In Germany, the scope of oversight bodies' competences over international cooperation differs depending on the type of surveillance conducted. The Independent Committee may conduct controls at all time over foreign to foreign data transfers.[453] However, in cases of strategic surveillance, the oversight is limited, as data transfers only need to be reported to the G 10 Commission on a monthly basis and to the PKGr every six months.[454] The German government informs the PKGr about the international data exchanges.[455] In 2015, the German intelligence service (BND) transferred data to two foreign services.[456]

The effectiveness of oversight exercised by national bodies over international intelligence cooperation was questioned by several institutions, both at national and international level. In Poland, where no limitations are expressly mentioned by law, a judgment of the ECtHR highlighted the absence of effective oversight over activities conducted under international cooperation, and in particular, of the effectiveness of the investigation powers of the parliamentary commission in this field. In *Al Nashiri v. Poland*, the court noted that the "instant case (...) also points out in this context to a more general problem of democratic oversight of intelligence services. The protection of human rights guaranteed by the Convention, especially in Articles 2 and 3, requires not only an effective investigation of alleged human rights abuses but also appropriate safeguards – both in law and in practice – against intelligence services violating Convention rights, notably in the pursuit of their covert operations. The circumstances of the instant case may raise concerns as to whether the Polish legal order fulfils this requirement."[457]

The absence of any specific mention of oversight over international cooperation in a law may be differently interpreted from one Member State to another. In some, this absence might be understood as implicit permission for oversight bodies to conduct similar control regarding international cooperation as over domestic intelligence efforts. Others may couple this absence with the third party rule (see Section 11.3), and interpret it as a tacit prohibition on controlling international intelligence-sharing.

452 Sweden, Regulation on Defence Intelligence Service, Art. 6.
453 Germany, BNDG, S. 15 (3).
454 Germany, G10 Act, S. 7a.
455 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), pp. 10-11.
456 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 9.
457 ECtHR, *Al Nashiri v. Poland,* No. 28761/11, 16 February 2015, para. 498.

11.3. Limits to oversight: the third party rule

> *"As the world becomes more and more wired and interconnected, these [personal digital] data are increasingly stored and transmitted freely across borders and through transit countries, leading to an unclear situation regarding jurisdiction and diminishing the relevance of national legislation and of national oversight."* European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013b)

The dominant principle of international cooperation is the 'third party rule', also known as the 'originator control principle'. This rule specifies that a foreign agency to which intelligence has been transmitted can neither share this information with a third party, nor use the data for an objective different from the one for which the exchange was established in the first place. While the rule is a core element of trust in which the global intelligence cooperation is rooted, it is also used by intelligence services to prevent oversight bodies from accessing any information related to international cooperation.

Third party rule should not act as a foreign veto

"[Member States should] [e]nsure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies."

Council of Europe, Democratic and effective oversight of national security services, *2015, Recommendation 16, p. 13*

Some Member States explicitly refer to the third party rule either in their laws or in the bilateral agreements signed with foreign partners.

The majority of parliamentary committees do not have access to classified information received from foreign secret services. This is explicitly stated in the cases of Spain,[458] France[459] and the United Kingdom,[460] among others. In its activity report, the German Parliamentary Control Panel acknowledged this fact and called for

458 Spain, Law 11/2002 of 6 May, National Intelligence Centre Act, Art. 11(2).
459 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6.
460 United Kingdom, Justice and Security Act 2013, s. 5(c) of Schedule 1.

amendment of the legislation to enhance parliamentary control of international exchanges between services.[461]

In some Member States, such as Belgium, the Netherlands and Sweden, the oversight body is not seen as a third party. This specific understanding of the nature of oversight bodies results from a parallel mechanism: oversight bodies acknowledge that the current form of the terrorist threat requires intelligence services to regularly exchange information, while overseers are granted full access to all information to effectively perform their tasks. In Belgium, for instance, following a request by the Defence Ministry, the Standing Committee I delivered a positive opinion on the international exchange of information relating to foreign terrorist fighters, but also clarified that the control over multilateral activities remains real.[462]

Promising practice

Enhancing international cooperation among oversight bodies

Equal access to information obtained via international cooperation could allow enhanced international cooperation among oversight bodies. In 2015, oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland launched joint project, whereby each body would conduct national investigation in relation to foreign terrorist fighters. A final report is due in 2017; intermediary assessments show the added-value of such coordinated efforts.

Belgium, Standing Committee I (2016), p. 80 and The Netherlands, CTIVD (2017), p. 33.

The third party rule has functional purposes: it ensures protection of sources, reinforces trust among intelligence partners and prevents intelligence data from being shared multiply, becoming thus their own reliability proof. The question of whether oversight bodies should be considered as third parties under the third party rule has crucial implications. As demonstrated above, oversight bodies play a very important part in achieving effective intelligence. Effective intelligence is, for foreign partners, a guarantee of valuable and trustworthy information and therefore ultimately increases and strengthens international cooperation. In that sense, the trend by some Member States to increasingly stop considering oversight bodies as third parties and grant them full access to information originating from international cooperation will ensure better cooperation among both overseers and intelligence services. A harmonised approach over oversight bodies' statutes in this regard (including parliamentarian committees) would foster exchange of best practices among Member States.

11.4. Powers and competences of oversight bodies over international cooperation

> *"Oversight bodies should receive copies of all such agreements at the time they are entered into or when they are revised. The oversight body should be obliged to review each agreement and, when possible, undertake random audits to measure compliance with the terms of the agreement. Such audits can help determine whether the agreement needs to be revised in light of past practice."*
>
> *Born H. and Leigh I., 2012, p. 144*

Very few Member States' legal frameworks provide for the possibility of an external review, either ex ante or ex post, of international agreements establishing international intelligence cooperation. Those that do include Belgium, Luxembourg and the Netherlands.

In Belgium, Hungary and the Netherlands, oversight bodies have access to internal guidelines governing exchanges of information. In Belgium, the Standing Committee I highlighted some weaknesses in the directives established by the National Security Council. Notably, the committee pointed out the absence of clear criteria clarifying when international cooperation can be established with foreign counterparts, and data transfers are allowed; delimiting the uses foreign counterparts may make of the data they receive; and reinforcing data protection safeguards when information is transferred to countries that do not offer the same level of data protection.[463] The Standing Committee I reiterated these concerns in its latest report.[464] The National Security Council eventually adopted a directive on this matter in 2016. In the Netherlands, the Dutch oversight body, CTIVD, has published detailed information, including recommendations, on the internal guidelines adopted by the General Intelligence and Security Service[465] and on the cooperation assessments (referred as "weighting notes") intelligence services must conduct before entering into international agreements.[466]

11.5. Bridging the gaps: peer constraints

The two restrictions mentioned above – the absence of a clear legal basis for the oversight of international

461 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), p. 14.
462 Belgium, Standing Committee I (2016), pp. 73-74.
463 Belgium, Standing Committee I (2015), p. 74.
464 Belgium, Standing Committee I (2016), p. 5.
465 The Netherlands, CTIVD (2009), pp. 6-12.
466 The Netherlands, CTIVD (2016c).

intelligence cooperation in some Member States and the limitations introduced in the legal frameworks of others – are not the only aspects hampering such oversight.

Accountability deficit

"Often, it is not possible for an oversight body to ascertain whether the data which the national service receives from abroad was collected lawfully. A national oversight body can only examine whether the national service provided or received information lawfully."

The Netherlands, CTIVD Annual Report 2014-2015, *p. 35*

The deficits described above by the Dutch oversight body prompted reflection on the possibility to create alternative oversight mechanisms that fit the specificities of international cooperation. An innovative way of performing oversight has emerged from these reflections: the "peer constraint" mechanism.

The third party rule restricts the majority of oversight bodies' ability to provide safeguards on the international exchange of data. However, the gaps are sometimes filled by other actors and in different ways, notably through peer-constraint mechanisms.[467] To receive intelligence, an intelligence service must be trustworthy in the eyes of its counterparts. Here, the pressure exercised by an intelligence service on its foreign counterpart replicates, to a certain extent, the constraint exercised by oversight bodies. In addition, the interest of any service in receiving intelligence magnifies this incentive. This is the case in Belgium where, since 2016, the intelligence services have a degree of control on international cooperation.

Of the 17 Member States where oversight of international cooperation is not provided for in law, guidance on the conditions for overseeing international intelligence cooperation might be included in classified internal guidelines drafted by the executive or the head of services. Generally, such guidance invites or imposes on the intelligence services the duty to exercise a priori and/or a posteriori control on data transfers taking place within international cooperation. In Belgium, this process was endorsed in January 2016, when the 1998 law on intelligence services was modified on the recommendation of the Parliament and the Standing Committee I to grant oversight competence to the Belgian intelligence services.[468]

Deeks describes 'peer constraints' as follows: "Through various mechanisms (formal and informal, public and private), one state's intelligence community can affect the way in which another intelligence community conducts [...] surveillance; the amount and type of intelligence the other intelligence community receives; and, less tangibly, how the other intelligence community views its own legal obligations".[469] Such constraint may be formally inserted as a caveat in the international agreement or may result from the tacit observation of one country's legal framework, including the extent of the oversight structure and the complaints and judicial decisions taken against the intelligence community.[470]

In the aftermath of the Snowden disclosures, peer constraints have become increasingly used among partners to ensure that international cooperation follows democratic principles. Approaches taken in to accessing, processing and controlling intelligence data are increasingly monitored by foreign partners to evaluate to which extent exchanged data will be lawfully processed, and to which extent they may access reliable data. Changes in legislation framing the access, use and control of intelligence may prompt either an intensification of or a decline in collaboration from foreign counterparts.

Peer-constraint mechanisms present certain added-value over classical oversight mechanisms. Firstly, they tackle the lack of expertise some overseers may have while assessing surveillance techniques and the implications of specific safeguards regarding the use of the data collected. Secondly, they give intelligence services a real interest in being deemed trustworthy by foreign counterparts. Third, they are completely independent from the executive of their foreign partner. However, peer-constraint mechanisms will only have (a limited) impact if they originate from a state with an effective oversight system.

467 Deeks, A. (2016), pp. 17-29.

468 Belgium, Organic Law concerning the intelligence and security services *(Loi organique des services de renseignement et de sécurité),* 30 November 1998, Art. 7 and 11.

469 Deeks, A., (2016), p. 4.

470 *Ibid.* pp. 17-22.

PART III: REMEDIES

KEY FINDINGS

Remedial avenues

- FRA's research shows that, in the context of surveillance, individuals' right to seek remedy is limited but not absent. A limited number of individuals seek remedies. On average, according to the experts interviewed, 10 to 20 complaints are filed a year.
- Non-judicial remedies are more accessible to individuals than judicial mechanisms. The procedural rules are less strict, and proceedings are faster and cheaper. Three EU Member States do not provide individuals with the possibility to lodge a complaint related to surveillance with non-judicial bodies. In ten of the 25 EU Member States that do provide that possibility, one single non-judicial body is entrusted with remedial powers, and in the remaining 15, individuals may lodge a complaint with two or more bodies with remedial powers.
- In 10 of the 16 Member States that have expert bodies, these bodies have the most powers to offer an effective remedy. They are also independent and enjoy full access to classified information and premises.
- Remedial bodies' effectiveness depends foremost on their binding decision making powers. In 18 Member States, remedial bodies can issue binding decisions. Most of them are expert bodies and data protection authorities.
- The effectiveness of remedies available to individuals has been questioned – predominantly by representatives from civil society organisations, lawyers and academia. Various factors hamper their effectiveness, including low levels of awareness about the existence of remedies and non-implementation of the right to access information and/or the notification obligation.

Limits to effective remedies

- FRA's findings show that EU Member States' laws limit individuals' rights to notification and access to information on various grounds linked to national security. Imposing limitations is in line with relevant ECtHR case law.
- In nine Member States, individuals may exercise the right to access their own data indirectly – through the DPAs who have competences in this area or through expert bodies.
- EU Member States address the judiciary's lack of expertise in secrecy and technical matters relating to intelligence services' work in various ways, including:
  - the development of alternative adversarial procedures to allow for the use of classified information;
  - cooperation mechanisms between remedial expert bodies to tackle the lack of expertise of judicial and non-judicial bodies; and
  - the establishment of quasi-judicial bodies.
- In four Member States, an expert body's decision or preliminary assessment can be appealed before a judge. Arrangements on access to sensitive information are then prescribed by law.

12 The remedial route



UN good practice on complaints and effective remedy

Practice 9. Any individual who believes that her or his rights have been infringed by an intelligence service can bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The 2015 FRA report recalled that the right to an effective remedy is an essential component of access to justice, and allows individuals to seek redress for violations of their rights. For a remedy to be 'effective' in practice and in law, judicial or non-judicial bodies need to have a number of specific powers (both from institutional and procedural perspectives)[471] offering individuals proper redress. In *Roman Zakharov v. Russia*, the ECtHR outlined the elements of an effective remedy and noted the challenges posed specifically by secret surveillance.

ECtHR case law: effective remedy in cases of surveillance

"Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...] As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications. [...] [E]ffectiveness [of remedies] is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. "

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015, paras. 233, 234 and 298

471 Gajdošová, J., in Dietrich/Sule (eds), forthcoming.

The 2015 FRA report highlighted that non-judicial avenues are usually more accessible to individuals than judicial mechanisms because the procedural rules are less strict, bringing complaints is less costly, and proceedings are faster. In the 28 EU Member States, non-judicial bodies such as DPAs, expert bodies, executive bodies, parliamentary committees, and ombuds institutions offer remedies.

Twenty-five Member States have empowered at least one of their oversight bodies or their ombuds institution with remedial power. In three Member States – the Czech Republic, Latvia and Poland – no non-judicial body is available, and individuals can lodge a complaint only with a judge. (As further discussed below, the United Kingdom's Investigatory Powers Tribunal is not a non-judicial body, but also does not qualify as an ordinary court.) Table 6 shows the types of non-judicial bodies with remedial powers in the Member States.

Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State

	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
AT		✓	✓		✓
BE		✓	✓		✓
BG			✓	✓	
CY			✓		
CZ					
DE		✓	✓	✓	*(acts as a filter: only reasonable complaints are sent to the PKGr)*
DK		✓			
EE					✓
EL			✓		
ES					✓
FI			✓		✓
FR		✓	✓		✓
HR		✓	✓	✓	✓
HU	✓		✓	✓	✓
IE		✓	✓		
IT			✓		
LT			✓	✓	✓
LU		✓			
LV					
MT		✓	✓		
NL*		✓			
PL					
PT		✓			✓
RO				✓	
SE		✓	✓		
SI			✓	✓	✓
SK				✓	
UK**					

Notes: * *Table reflects the situation under the Intelligence and Security Services Act 2017 and will be applicable when the relevant sections enter into force.*

** *The Investigatory Powers Tribunal, although not an ordinary court, cannot be classified as a non-judicial body.*

Source: *FRA, 2017*

The 2015 FRA report showed that the availability of various remedies does not necessarily help to ensure effectiveness.[472]

"The average citizen does not even know where to address a complaint." (Data protection authority)

The fieldwork interviews[473] addressed the availability of remedies in case of alleged unlawful data processing by intelligence services. Two dominating opinions emerged. Most respondents representing public authorities or institutions (such as expert oversight, executive control and judiciary) tended to list the avenues available and confirm their sufficiency, adequacy and satisfactory availability. Their existence appears to be seen as proof of their efficiency. Very few respondents from public authorities questioned the effectiveness of the remedies offered. These findings were also related to the generally low level of knowledge among the interviewees of practical implementation of the remedies in the Member States, the number of complaints, and little knowledge about their outcomes, unless the institution itself had a remedial function.

"Yes, the avenues available for individuals to complain are enough. Yes, I think the websites of the governments are quite good at this, they always have a page on this, send the letter to this address and online application for filing your complaints." (Expert body)

"[A] signed letter [is] enough to submit a request, with details on what is allegedly affected, such as a mobile number, bank account, or email account." (Expert body)

Representatives from civil society organisations, academia, and practicing lawyers acknowledged that it is positive that complaints against intelligence services do not need to be strongly substantiated for remedial bodies to consider them. However, they tended to be critical about available remedies and questioned their efficiency. Notably, a majority of the interviewed civil society representatives were lawyers who have been involved in lodging both judicial and non-judicial complaints, challenging the lawfulness of intelligence surveillance on behalf of individuals. Most respondents who were critical considered available remedies ineffective for safeguarding the right to privacy. Some respondents did not even consider them as remedies. Respondents indicated that several factors make the remedial process cumbersome or complicated. These include: low awareness among individuals about the possibility to seek remedies; that complaints are based on assumptions or suspicions when the notification requirement is not prescribed by law; and the types of responses given by remedial bodies. Respondents also mentioned poor capacities of remedial bodies in terms of staff and technical expertise. Moreover, they noted that, even though no costs are involved in seeking remedies through non-judicial avenues, the subject matter can be complex and complainants could benefit from legal advice – but legal aid is not available.

"There is already an existing complaints procedure. Even though it is not a formalised one, if you were to complain, these complaints would have to be taken seriously."

(Academia)

"A limited number of remedies is available for persons. For national surveillance measures, the procedure requires the person to file a complaint with the [expert body] before being granted recourse to the [judge], without any information required to be disclosed to the person on the existence of surveillance measures." (Civil society organisation)

"What will be the point of an individual lodging a complaint if he can base his arguments only on rumours? 'The direct and personal interest' of the law is difficult to demonstrate."

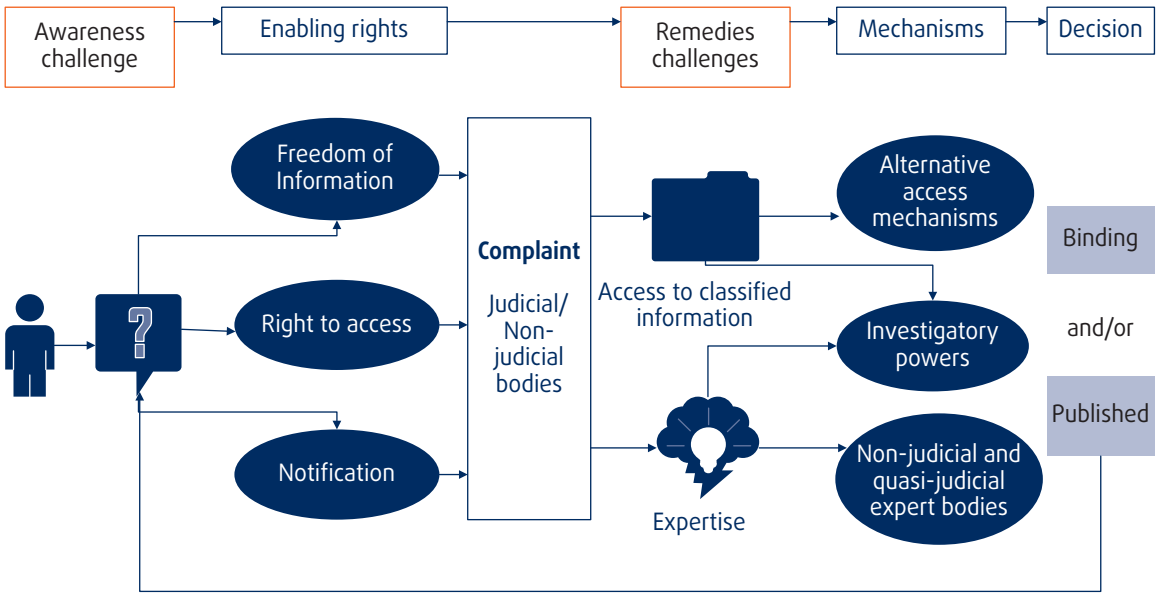
(National human rights institution)

Figure 9 illustrates the different challenges individuals and remedial bodies may confront when seeking, and seeking to provide, effective remedies. For individuals, the first issue is the lack of awareness of surveillance measures. Various tools can help enhance individuals' awareness: notification that they have been under surveillance or right to access to their own data serve as rights' enablers and open the way to a complaint. Remedial bodies are also confronted with several challenges. They can be denied access to classified information or they may lack the necessary expertise. As analysed in the following sections, these hindrances are addressed in various ways at Member State level.

472 FRA, (2015a), p. 59.

473 Annex 1, Section 2, Social fieldwork methodology, presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

Figure 9: Implementing effective remedies: challenges and solutions



Source: FRA, 2017

12.1. Investigative and decisional powers

Non-judicial avenues generally offer greater expertise than judicial mechanisms. However, non-judicial and quasi-judicial bodies lack effectiveness if they do not have full investigative and decisional powers. These include, but are not limited to, the competence to issue binding decisions, to access all relevant data (including through hearings or visits to intelligence services' premises), to inform complainants about decisions and for individuals to appeal the final decision. Table 7 shows the powers attributed to non-judicial bodies in EU Member States.

Expert bodies have the widest powers. In 22 Member States, at least one non-judicial body has full access to the data collected. In 11 Member States, non-judicial bodies inform complainants that a control was performed – without specifying the outcome. Such competence is mainly granted to expert bodies including DPAs. Across the EU, only in a few cases can decisions of non-judicial bodies be reviewed by a judge (for instance, following an oversight body decision in Austria and France).

Effectiveness depends on capacity to issue binding decisions

"Equipping complaint-handling bodies with mere powers of recommendation is insufficient and does not constitute an 'effective remedy'. Instead, these bodies should be given quasi-judicial remedy powers, such as the power to award financial compensation."

Born, H. and Wills, A. (2012), p. 195

The authority to issue binding decisions is a key element of an effective remedy. Binding decisions should include, at minimum, the ability to order (1) the termination of the surveillance, (2) the destruction of the data collected, and (3) the payment of appropriate compensation.[474] In 18 Member States, remedial bodies – mainly expert bodies and DPAs – may issue binding decisions on complaints relating to surveillance. In Belgium, for instance, the Standing Committee I may order intelligence services to terminate surveillance and destroy the data. In the Netherlands, the complaints sub-committee of the CTIVD may decide that an investigation by the services has to stop; that the exercise of a power by the intelligence services has to stop;

474 Born, H., and Leigh, I. (2005), p. 120.

Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
AT	Legal Protection Commissioner				
	Austrian Ombudsman Board				
	Austrian Data Protection Authority				
BE	Standing Committee I				
	The federal Ombudsman				
	Privacy Commission				
BG	Commission for Personal Data Protection				
	Committee for Oversight of the Security Services				
CY	Commissioner for Personal Data Protection				
DE	G10 Commission				
	Federal Data Protection Commissioner				
	Parliamentary Control Panel				
DK	Danish Intelligence Oversight Board				
EE	Chancellor of Justice				
EL	Hellenic Data Protection Authority				
ES	Spanish Ombudsman				
FR	National Commission for Control of Intelligence Techniques				
	Defender of Rights				
	National Commission on Informatics and Liberty				
FI	Parliamentary Ombudsman				
	Office of the Data Protection Ombudsman				
HR	Council for Civic Oversight of Security and Intelligence Agencies				
	Ombudsman of the Republic of Croatia				
	Personal Data Protection Agency				
	Committee for Internal Affairs and National Security				
HU	Commissioner for Fundamental Rights				
	Data Protection Commissioner				
	Parliamentary Committee for National Security				
	Relevant ministries				
IE	Complaints Referee				
	Data Protection Commissioner				
IT	Garante per la protezione dei dati personali				
LU	Control Authority «Article 17»				
	National Commission for Data Protection				
LT	Ombudsperson				
	State Data Protection				
	Parliamentary Committee on National Security and Defence				

Table 7: (continued)

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
MT	Commissioner of the Security Service				
NL	Review Committee for the Intelligence and Security Services				
PT	Council for the Oversight of the Intelligence				
	Portugese Ombudsman				
RO	Parliamentary Committees				
SE	Swedish Foreign Intelligence Inspectorate (SIUN)				
	Commission on Security and Integrity Protection (SIN)				
	Swedish Data Protection Authority (Datainspektionen)				
SI	Human Rights Ombudsman				
	Information Commissioner				
	Parlm. Supervision of the Intelligence and Security Services Act				
SK	Commission to Supervise the Use of IT Tools				

Note:

= Expert body
= Ombuds institution
= Data protection authority
= Parliamentary Committee
= Executive

Source: FRA, 2017

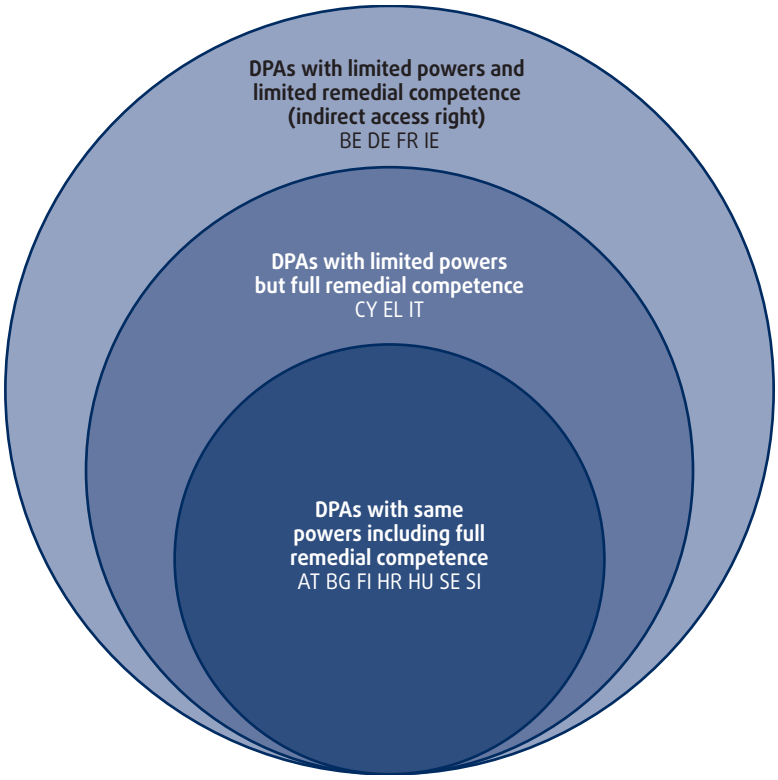
and/or the removal and destruction of data processed by the services.[475] Austria is the only country where both the expert body and the DPA have binding decision powers. Two Member States, Finland and Romania, have empowered another non-judicial body with such power: the ombuds institution and the parliamentary committees, respectively. Nonetheless, the examples introduced throughout this third part show that the power to issue binding decisions, although essential, may be greatly limited if the body's mandate does not include other crucial features, such as independence and full access to classified information and premises.

Of the 16 Member States that have established expert bodies, 12 entrust them with specific remedial powers, but only seven may issue binding decisions (in Belgium, Denmark, Ireland, Luxembourg, the Netherlands, Sweden and the United Kingdom).

DPAs in 14 EU Member States can examine individual complaints. Of these, ten may issue binding decisions; these are the seven Member States where DPAs enjoy the same powers over intelligence services as the expert oversight bodies, and Cyprus, Greece and Italy. In four other Member States (Belgium, France, Germany and Ireland), DPAs may process individual complaints or enable an individual's indirect right to access, but are not entitled to issue binding decisions. In four Member States (Cyprus, Germany, Greece and France), access is accompanied by enhanced requirements, e.g. the presence of the DPA head (Cyprus, Greece); a staff member of the DPA who has been a member of the Council of State, the Court of Cassation or the Court of Auditors (France); or an officer duly authorised in writing (Germany). FRA's fieldwork findings show that in France, Germany and Italy, such requirement proved, in practice, to be helpful for DPAs conducting on-site inspections. Figure 10 illustrates the diversity of DPAs' remedial competences over intelligence services across the EU.

475 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 124.

Figure 10: DPAs' remedial competences over intelligence services



Source: *FRA, 2017*

In Belgium, France and Italy, individuals can request the DPA to check whether their data are processed by intelligence services. The DPA proceeds with the necessary check, informs the individual that the control took place but not whether and which data were processed, if such information would affect national security. Should any irregularities be noted, the DPA can request the intelligence service to redress the situation.[476]

Finally, in eight Member States – Bulgaria, Croatia, Germany, Hungary, Lithuania, Romania, Slovakia and Slovenia – parliamentary committees function as complaints-handling bodies in cases of surveillance. Only in Romania can the parliamentary committee resolve complaints through binding decisions. In Germany, the complaint forms part of a petition to parliament.[477] Over a two-year reporting period, the PKGr received 65 petitions, 40 of which dealt with alleged surveillance measures.[478] The more serious ones were forwarded to the G 10 Commission. These complaints, in fact, serve to inform the PKGr.[479]

The extent to which parliamentary committees can provide an effective remedy depends on a number of factors. These include whether members of these special parliamentary committees are properly independent, have experience in the field of intelligence, as well as whether qualified supporting staff is available.[480] In *Bucur and Toma v. Romania*,[481] the ECtHR highlighted that a lack of independence can preclude the effectiveness of remedies. According to the Committee of Ministers of the Council of Europe, the situation in Romania has

476 See for example Italy, Data Protection Code, Art. 160(2).
477 Huber, B., *in*: Schenke, W. et al. (eds.) (2014), p. 1485 and Singer, J. (2016), p. 145.
478 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), p. 13.
479 Bartodziej, P., *in:* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1561.
480 Romania, Decision no. 30/1993 of the Romanian Parliament concerning the Organization and Functioning of the Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the Activity of the Romanian Intelligence Service, 23 June 1993, Art. 5 (b) and (c), and Romania, *Decision no. 44/1998 of the Romanian Parliament concerning the Organization and Functioning of the Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the activity of the External Intelligence Service*, 28 October 1998, Art. 6 (e) and (f).
481 ECtHR, *Bucur and Toma v. Romania*, No. 40238/02, 8 January 2013, para. 98.

not evolved since 2013, when the case was decided.[482] In Bulgaria and Romania, the parliamentary committee can investigate complaints; both must forward their positions, either to the relevant ministry (in Romania) or the public prosecutor (in Bulgaria).[483]

Individuals may lodge complaints relating to surveillance with their national ombuds institutions in 11 Member States; however, their mandate may explicitly exclude the issue of national security or the work of intelligence services. Only the Finnish Data Protection Ombuds institution is entitled to issue binding decisions, and only one Member State – Estonia – provides the ombuds institution with remedial powers via the relevant intelligence law.[484] Most ombuds institutions are denied access to classified information and often lack expertise in this field.[485] Consequently, in some Member States – such as Belgium – the ombuds institution will forward the question to the expert body. In Germany, the ombuds institution works in cooperation with the parliamentary oversight committee: its role is to assess the validity of the complaints before transmitting them to the parliamentary committee. Thus, the ombuds institutions' powers can be limited in this area. Complaints are typically concluded with non-binding recommendations that aim to put matters right and guide future action, rather than with binding, enforceable decisions.

The FRA 2015 report highlighted the importance of remedial bodies' adherence to general requirements of fairness, impartiality and independence.[486] In Hungary, for example, 'oversight' and complaints-handling functions relating to 'extraordinary measures' (such as the surveillance of telecommunications) are both performed by one executive institution: the government and its different ministries.[487]

12.2. Processing of complaints

Representatives from the institutions with remedial powers were asked specific questions about complaints received in the preceding three years, including the numbers per year, their outcomes and other specific details, if this information was available for discussion. For example, the average number of complaints received was discussed during approximately one third of the interviews. The content of the complaints is confidential.

"Very few citizens' complaints relate to intelligence work, and this is for two reasons: the real 'bad guys' don't attach any importance to it, or if the work is done well, they don't know about it." (Expert body)

Respondents referred to 'very rare cases' or very low numbers of complaints from individuals regarding allegedly unlawful activities by intelligence services. The average across different institutions in the selected Member States ranges from 10 to 20 complaints per year, with certain rare deviations in some Member States in relation to specific occurrences, such as the Snowden revelations, cases that became publicly-known due to disclosure by the media, or in response to terrorist attacks. In some cases, the number of complaints received is not publicly available and is confidential – for example, in Italy, the DPA does not publish the number of the complaints; this information can only be communicated to the parliamentary committee COPASIR. Some respondents said they never received any complaints and have no practical experience in handling complaints (or usually receive very few complaints per year). A few respondents expressed concern about abuses of complaint procedures – for example, a DPA noting that '[T]here are people who exercise this right creatively'. However, the relatively low numbers can hardly qualify as abuse. On the other hand, no complaints being received may raise questions regarding the effectiveness and quality of the working system.

"Three or four appeals can reasonably be expected per year, which will not be enough to establish precedents." (Expert body)

In terms of meeting the admissibility criteria (formal requirements) of complaints, the ratio between well-founded and ill-founded complaints differs per Member State and per type of institution presented. The interviews suggest there is a general tendency of complaints from individuals being ill-founded more often than being well-founded. No details or specific examples were disclosed during the interviews and very limited information was provided about the content of the complaints. The respondents described complaints as the 'usual', but acknowledged that these can be complex. They insisted that complaints are treated seriously, stating that investigating them requires expertise and access to the sources of the intelligence services.

482 Council of Europe, Department for the Execution of Judgments of the ECtHR (2016), Case of *Bucur and Toma v. Romania*, H/Exec(2016)6, 20 October 2016, para. 25.
483 Hungary, Act CXXV of 1995 on the National Security Services (*A nemzetbiztonsági szolgálatokról szóló 1995. Évi CXXV. törvény*), 28 December 1995, as amended, Section 14 (4).
484 Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), Art. 1(9).
485 FRA (2014c), p. 34.
486 FRA (2015a), pp. 70-72.
487 Hungary, *Governmental Decree No. 185/2016 on the cooperation between the service providers providing encrypted communications and the authorities entitled to conduct secret surveillance operations, 185/2016 (VII. 13.)*, 17 July 2016.

"You should also be aware that many people speculate about the intelligence services, and also many people who have personal or psychological issues also speculate a lot about that." (Expert body)

Respondents representing institutions with remedial powers were asked to describe potential or frequent complainants. Most respondents felt that the usual/typical complainants shared common characteristics, particularly implying that these are people with mental health problems. In describing potential or usual complainants, they chose their words carefully. The most common and neutral description of complainants was 'people who have difficulties'. The respondents also referred to complainants as having psychological problems, with some describing them as 'paranoid', 'mythomaniacs', and 'people who are quite simply suffering from a persecution complex'. Some respondents voiced concern about individuals lodging 'frivolous complaints'. Several noted that, in the absence of notification or other ways for individuals to access information collected about them by the intelligence services, complaints are based on assumptions or speculation about allegedly unlawful activity by the intelligence services.

"Eighty per cent of complaints from individuals come from persons with mental health problems or are manifestly unfounded cases. In this type of case, an internal process has been put in place to forewarn the prosecutor's office."

(Expert body)

"A significant part of the people who file complaints tend to have psychological problems." (Judiciary)

Frivolous complaints

"Concerns about frivolous or vexatious complaints may be remedied by rules allowing the complaint-handling body to dismiss such complaints early in the process. But caution should be exercised to avoid dismissing complaints that are difficult, politically controversial, or simply brought by difficult people."

Born and Wills (2012), p. 193

Information about the number of complaints is publicly available in a limited number of EU Member States. Information from the annual reports of expert bodies in Belgium, Germany, the Netherlands and Sweden is provided below.

In 2015, the Belgian expert body received 22 individuals' complaints (compared to 31 in 2014).[488] In 2014, most of them were dismissed (28 out of 31). By contrast, in 2015, 14 were rejected because they were ill-founded or the Standing Committee I found that it was not competent to process the complaint.[489] The remaining eight complaints were thoroughly investigated. One concerned an individual who complained about being under "oppressive" surveillance by the intelligence services. The Standing Committee I concluded that the services carried out surveillance but that the surveillance was probably carried out by a foreign service. The Standing Committee I raised the question whether the intelligence services had a 'positive obligation' under the constitution or the ECHR to protect a resident against possibly unfounded accusations by a foreign service.[490] The Standing Committee I must inform individuals about their investigations' results in general terms. A specific complaint procedure, taking into account the necessary confidentiality of the intelligence services' operations and the need for transparency, has been established by law with the introduction of the 'targeted surveillance measures'.[491]

The German G 10 Commission functions as a quasi-judicial institution[492] empowered with the ability to handle complaints, either in relation to targeted or strategic surveillance.[493] In 2015, the G 10 Commission received 16 complaints from citizens who believed that they were under surveillance. The commission could not establish any violation of their right to privacy (Article 10 of the constitution).[494] Concerning the cases brought before the administrative courts by individuals who received a notification that they had been under surveillance, the G10 Commission reported in 2015 that 14 complaints followed notification, six of which were assessed within the same year.[495]

In the Netherlands, in 2016, the CTIVD handled 11 complaints related to the AIVD (as compare to seven from April to December 2015). None of these were found to be fully well-founded, and three (four in 2015) were deemed partly well-founded. The minister followed the committee's opinion in all cases.[496] The previous annual report (covering the period 2014–2015) referred to 10 complaints, four of which were deemed partially

488 Belgium, Standing Committee I (2015), p. 7.

489 Belgium, Standing Committee I (2016), p. 7.
490 *Ibid.* p. 37–41.
491 Vande Walle, G. (2013), p. 258, and Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 43/4.
492 Wetzling, T. (2017), p. 5.
493 Germany, *G 10 Act*, S. 15.
494 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 6. In 2014, the G 10 Commission received 14 complaints, see Germany, Federal Parliament (*Deutscher Bundestag*) (2016b), p. 6 and in 2013, 21 complaints, see Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 6.
495 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 6 and 8. See Wöckel, H. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1607 and following.
496 The Netherlands, CTIVD (2016a), p. 17 and following and The Netherlands, CTIVD (2017), p. 23 and following.

or fully well-founded.[497] So, the number of complaints remains the same over the years. In the context of some of these complaints, the CTIVD raised the issue of secrecy surrounding the facts included in the CTIVD's opinion; in such cases, the minister decides which information may be provided to the individual. The CTIVD stated that it would favour declassifying information that would contribute to a better understanding of the working methods of the services, and in particular cases, it in fact suggested declassifying the information. Only in cases relating to the military intelligence services (GISS) did the minister not follow the CTIVD's suggestions.[498] While the CTIVD had limited remedial powers under the 2002 Act, the 2017 Law changed this and gave CTIVD biding decision powers.

In Sweden, both expert bodies – SIUN and the Commission on Security and Integrity Protection (SIN) – may be approached by citizens wishing to check whether they are under surveillance, and whether this surveillance was lawfully conducted by the intelligence services. Between 2008 and 2016, SIUN audited more than 80 cases. Between 2014 and 2016, SIUN received 46 requests from individuals wishing to check whether SIGINT surveillance was conducted according to the law.[499] These requests concerned the National Defence Radio Establishment as well as the three other entities monitored by SIUN. None of the individual requests highlighted serious faults. Of the total control work, including checks made not on the basis of a request from an individual, four opinions were delivered to the intelligence services, two of them to the National Defence Radio Establishment. SIUN never reached the stage where it may refer a case to the prosecutor or order the National Defence Radio Establishment to terminate data collection.[500]

"We disclose what we are allowed to disclose. However, we do not say, for example, that there's probably more. That would not be right. […] There is a specific formulation. We say: 'we have carried out our checks and there are no concerns from the perspective of data protection'."

(Data protection authority)

"In general, we will not confirm or deny that someone has been wiretapped. We will focus on whether there has been a wrongdoing, an illegal practice, and this we aim to communicate, even though often in an abstract way."

(Expert body)

While discussing the processing of complaints, respondents said they carry out comprehensive investigations on the basis of well-founded (in some cases ill-founded) complaints from individuals. This includes access to the intelligence service's sources or meetings with its staff, and can include inviting complainants to hearings. However, the responses received by individuals regarding complaints are more or less standard: if unlawful activity has taken place, the applicant is informed so that compensation can be sought; but if not, the response –'neither confirm nor deny' ('NCND') – can cover both situations where 'no surveillance actually took place' or where 'it did but was lawful'. As rare exceptions, in a few Member States, individuals are informed if they were under surveillance. Representatives of civil society organisations, lawyers, and academia noted that the standard 'NCND' response makes available remedies ineffective and questioned if the remedies are suited for individuals.

According to representatives of institutions dealing with individual complaints, the response might be different when the intelligence services were found to act 'illegally' or 'unlawfully'.

"I think in this highly complex area government has, in addition to the resources, the added advantage of the knowledge of what [the services] are doing and the ability to 'NCND' everything, which is a problem. We need much more transparency, robustness from the domestic court."

(Civil society organisation)

"So the complaint goes off, the [expert body] will consider it, there may be a hearing, there maybe not be, it may be that the [expert body] hears evidence from the intelligence services or the police, but maybe not, but if it does, I probably would be told, my client might be told, we wouldn't have a right to attend, we wouldn't have a right to approach them. The [expert body] makes a decision and will only notify me if they find a violation." (Lawyer)

Finally, individuals may also prefer to access justice through intermediaries, such as relevant civil society organisations. The latter may play a vital role in taking surveillance-related complaints to court when class actions are allowed, as well as in bringing cases of a more general nature requesting access to specific information on the activities and investigative methods of intelligence authorities to contribute to greater transparency and accountability in this area.[501] However, in some EU Member States, civil society organisations often lack adequate resources, and few are able to offer comprehensive services to victims of data protection violations.[502]

497 The Netherlands, CTIVD (2015), p. 19 and following.
498 *Ibid.* pp. 22–23.
499 Sweden, SIUN (2017), pp. 4-9.
500 Sweden, National Defence Radio Establishment (*Försvarets radioanstalt*) (2016).
501 Poland, Administrative Court in Warsaw (*Wojewódzki Sąd Administracyjny w Warszawie*), *Helsinki Foundation for Human Rights v. ABW*, II SA/Wa 710/14, 24 June 2014, pending appeal to the Supreme Administrative Court: Poland, Helsinki Foundation for Human Rights (2015).
502 FRA (2014c).

The representatives of civil society organisations interviewed for this report pointed to their contributions to, and role in, litigation, both in national and in EU courts. They litigate with pro bono legal support. All civil society organisations interviewed acknowledged that without pro bono legal support, the litigation – an important and significant part of their work – would not be possible. They stated that a legal remedy implemented in such a manner represents 'an obvious imbalance in terms of process and resources' in power relations between civil society organisations and the state. A similar imbalance affects individuals when seeking remedies. Other relevant factors include the difficulties caused by the costs involved for individuals to take their cases to court; the need for legal knowledge, expertise and support; and the stamina required.

"The only thing that we can do now is to have individual persons going to court. That is a problem, you need to have standing as an individual, you need to be individually targeted e.g. by secret services, then of course comes a question, how can you prove that you have been the target of the secret services because usually you never know, they will never notify you, maybe after 50 years. It is really difficult and has become more difficult for us to have these court cases." (Civil society organisation)

"We did the case pro bono. One of the benefits of the [expert body] is that there are no costs, compared to other proceedings. Even so, for an ordinary complainant there is no legal aid available, so the ordinary complainant would either fund themselves or find a human right organisation willing to take the case pro bono. That is an issue." (Lawyer)

Strategic litigation pursued by civil society organisations plays another important role. It raises awareness among the general public of possible rights violations in the areas of data and intelligence collection, and increases the public's interest in defending their rights and in looking for ways to prevent possible violations.

13 Raising individuals' awareness



Surveillance measures are characterised by secrecy. This is a key impediment to seeking a remedy. Surveillance must be in accordance with the law. However, in such a confidential context, the legality of a measure is not sufficient to ensure individuals' awareness of a potential breach. Several rights, though, may enable individuals to access information, and, where relevant, challenge wrongdoings or unlawful surveillance by intelligence services.

Fieldwork interviews addressed the reasons individuals have for lodging complaints. Respondents' comments mostly related to the implementation of the obligation to inform and the right of access. As one respondent from a national human rights institution put it: 'What will be the point of an individual lodging a complaint if she or he can base their arguments only on rumours?' Clear views on the issues did not emerge from the fieldwork. A variety of opinions and understandings were expressed. These are not particularly specific or well-elaborated, and include contradictory views among respondents from the same Member State. For example, some respondents considered notification or access to information to be a main prerequisite for learning about being subject to surveillance; others considered the provision as a dead letter in the legal framework; while others saw non-application to be problematic. In terms of the duty to notify, taking into account the different practices in the implementation of this obligation and the lack of systematic application in practice, this issue remains unclear, open to interpretation in terms of how to deal with it ('grey area'), not widely discussed in terms of its application, and sometimes questioned if necessary at all in the national legal framework. On the other hand, the limited information collected during the fieldwork shows that notifying individuals that they had been under surveillance has no significant impact on the abuse of complaint procedures.

Access to information and notification obligations

"The legislation should emphasize that transparency and access to information are fundamental principles of democracy and that classification of information must be used sparingly. The criteria for classification should indicate a sufficient degree of harm and certainty to warrant non-disclosure. The legislation should enable a person charged with unlawful disclosure of classified information to raise a public interest defence. The executive should be obliged to promote and facilitate public access to state-held information, including information on the intelligence services."

Born H. and Wills A., (2012), p. 64

"The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public. The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance. In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance. These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance."

The Tshwane Principles, Principle 10 E

"Experience shows, however, that in the majority of notifications the persons concerned do not bring legal action." (Expert body)

13.1. Freedom of information

To verify and, possibly, challenge surveillance measures, access to public documents may increase individuals' awareness of possible wrongdoings and support them, where relevant, in lodging a complaint. This right, generally grounded in freedom of information laws, contributes greatly to the accountability system. As emphasised by Born and Leigh, "Security and intelligence agencies should not be exempted from domestic freedom of information and access to files legislation. Instead they should be permitted, where relevant, to take advantage of specific exceptions to disclosure principles referring to a limited concept of national security and related to the agency's mandate."[503]

All but two EU Member States – Cyprus and Luxembourg – have enacted Freedom of Information laws, or similar laws. However, all include restrictions based on access to classified information, or the protection of national security, or the activities of intelligence services. These exemptions originate in the need for intelligence services to be able to protect the sources and methods applied to individual operations. Only Hungary does not exclude classified information or state security documents as a general rule. However, the heads of the Hungarian services have the discretion to deny the disclosure of public information on national security grounds.[504]

In Germany, the Security Check Act (*Sicherheitsüberprüfungsgesetz*) prevents citizens from requesting access to information that originates from the three federal intelligence services or other authorities and bodies of the federal state that are classified as "secret" or "top secret".[505] The Federal Administrative Court has clarified that this general exemption from the right to freedom of access to documents also covers documents originating from the intelligence services and held by supervisory authorities.[506]

This blanket exception based on national security shows that, within the legal frameworks of EU Member States, the Freedom of Information principle is, *de jure*, not adapted for individuals attempting to access relevant information and to challenge surveillance techniques. While it is clear that certain information should remain classified, total exceptions could be softened to safeguard individuals' fundamental rights. Notably, legitimate aim and proportionality tests could be conducted before denying access to public documents, or a competent authority could be in charge of assessing the level of confidentiality before issuing the denial.

Nevertheless, interviewed experts stated that there have been situations where Freedom of Information legislation proved useful to compel authorities to disclose certain findings, where national security is deemed not to be at risk and the information is not otherwise publicly available.

13.2. Notification obligation and right to access principles

The obligation to inform and the right to access one's own data can generally be perceived as strong safeguards for ensuring the effectiveness of remedial action, and, ultimately, legal scrutiny by judicial or non-judicial bodies.[507] In data protection laws, these safeguards also ensure transparency of data processing and the exercise of other rights of the individual, i.e. the rectification and/or deletion of data being processed unlawfully.[508] In the context of surveillance, even circumscribed by the necessary restrictions to safeguard national security and confidentiality,[509] these rights also enhance accountability of the intelligence services and help to develop citizens' trust in government actions.[510]

In the United Kingdom, for instance, IOCCO has the power to inform individuals if it finds that they have been adversely affected by any serious error or by any wilful or reckless conduct by a public authority.[511] Such notifications have led individuals to lodge complaints with the IPT.[512] This principle was confirmed in the Investigatory Powers Act, which obliges the Investigatory Powers Commissioner to inform persons of any "significant prejudice or harm" relating to them of which the Commissioner is aware. In doing so, the Investigatory Powers Commissioner will have to assess the seriousness of the error, to consider the potential impact on public interest or national security, and to inform the persons of their rights to apply to the IPT. However, the fact that there has been a breach of an individual's ECHR rights alone is not sufficient for an

503 Born, H. and Leigh, I. (2005), p. 44.
504 Hungary, Act CXXV of 1995 on the national security services, 27 March 1996, Article 48(1).
505 Germany, Act to Regulate Access to Federal Information (*Informationsfreiheitsgesetz, IFG*), Section 3 No. 8.
506 Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 7 C 18.14, 25 February 2016.
507 Born H. and Wills A., (2012), p. 52.
508 See for example Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999, para. 169.
509 See for example GDPR, Article 23(1).
510 UN, Human Rights Council, Scheinin, M. (2010), p. 23.
511 United Kingdom, Home Office (2015), 'Code of Practice of Acquisition and Disclosure of Communications Data', March 2015, ss. 6.22 and 8.3. See also, United Kingdom, IOCCO (2016a), paras 1.14 and 2.2.
512 United Kingdom, IOCCO (2016a), p. 71.

error to be serious, thus narrowing down the classes of individuals who may be informed.[513]

The 2015 FRA report emphasised that the right to access personal data and obtain rectification or erasure of such data belongs to the essence of the right to data protection, and recalled the principle of judicial review enshrined in Article 47 of the Charter.[514] The ECtHR considers the issue of notification to be inextricably linked to the effectiveness of remedies before the court, as long as it no longer jeopardises the purpose of the surveillance. While the court again emphasises the crucial importance of both the notification obligation and the right to access principles, it does note that the effectiveness of remedies may be guaranteed by the existence of one *or* the other right. This specification seems to take into account the difficulties inherent in the practical implementation of these rights – especially the obligation to notify.

ECtHR case law: notification and access to information in cases of surveillance

Notification

"It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, paras. 287*

Access to information

"It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational-search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive "information" about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed or that one or more elements of a criminal offence were missing. It is also significant that only information that does not contain State secrets may be disclosed to the interception subject and that under Russian law information about the facilities used in operational-search activities, the methods employed, the officials involved and the data collected constitutes a State secret (see paragraph 52 above). In view of the above features of Russian law, the possibility to obtain information about interceptions appears to be ineffective."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 289*

Minimum requirement for remedies' effectiveness

"The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 298*

513 United Kingdom, Investigatory Powers Act (2016), s. 231. Not yet in force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

514 FRA (2015a), p. 61.

13.3. Restrictions on notification obligation and right of access

The FRA 2015 report details how the obligation to inform and grant access are completely exempted in some Member States (the Czech Republic, Ireland, Lithuania, Poland and Slovakia) and restricted in the other 23 Member States.[515]

"The [expert body] drafts a report on the basis of the complaint, which is sent to the individual. […] [W]hichever of these options is chosen, it comes down to the same thing: there is no access to classified documents." (Expert body)

"The services are obliged to provide information, but there is no obligation concerning the specific content of information provided […] they must provide information, but their response can also be in the negative. For example: 'no, we have no data on file', or similar. If the matter were given close consideration, then individual legal protection would have to be improved." (Academia)

However, there are differences in the conditions and level of restrictions.[516] Limitations can be based on the *direct* aspect of the access to information, on the general aspect of surveillance, on the level of classifications, on national security, on the operational impact of surveillance, or on other procedural grounds.

The right to *indirect* access is the right for an individual to access his/her own data indirectly through the DPA or the expert body.[517] Such right exists in 12 EU Member States: Austria, Belgium, Bulgaria, Cyprus, Finland, France, Hungary, Ireland, Italy, Luxembourg, Portugal and Sweden. Between 2014 and 2016, the French DPA (CNIL) received an increasing number of indirect access requests: 159 in 2014, 243 in 2015, and 435 in 2016.[518] The French expert body (CNCTR) in charge of assessing the legality of the technique used received 51 complaints between October 2015 and October 2016.[519]

As stated in the 2015 FRA report,[520] of the five Member States with detailed legislation on general surveillance of communications, only Germany and Sweden stipulate a notification requirement in cases of general surveillance of communications. The obligation to inform does not apply if a) the search terms are not directly related to the individual (Sweden)[521] or b) if the data are deleted immediately (Germany).[522] The German 2016 reform of the BND Law does not stipulate any notification requirement in case of foreign-foreign surveillance measures.[523]

In some Member States – such as Ireland, Latvia, Spain and Sweden[524] – the obligation to inform and/or the right of access are restricted because of rules applicable to classified documents and official secrets. In Latvia, although amendments to the Investigatory Operations Law adopted on 10 March 2016 strengthened the state's obligations concerning the duty of those conducting operational activities to inform *ex post* the individual against whom the activities were conducted, such notification does not apply in cases of, among others, a possible threat to another person's legitimate rights and interests, national security or criminal procedure.[525]

The 2015 FRA report detailed how the right of access and obligation to notify may be limited on the ground that divulging the information could threaten the objectives of the intelligence services or national security.[526] In ten Member States, individuals are notified or information is provided at the end of surveillance, and only when the threat to national security has ceased to exist: Bulgaria, Croatia, Denmark, Finland, Germany, Greece, Latvia, the Netherlands, Spain and Romania.[527] In Denmark and Finland, the general obligation to inform individuals at the end of surveillance may be omitted or postponed upon a court order.[528]

Finally, in some Member States, additional conditions on *ex post* notification or access to data are enshrined in law.[529] For instance, in Sweden, individuals shall be notified of signals intelligence only if the search terms used therein are directly related to them, and not if reasons of confidentiality prevent notification.[530]

515 FRA (2015a), p. 62.
516 See also UN, GA (2014b), para. 39.
517 FRA (2015a), pp. 66-67.
518 See France, CNIL (2014) p. 48; CNIL (2015) p. 57 and CNIL (2016), p. 63.
519 France, CNCTR (2016), p. 90.
520 FRA (2015a), p. 63.
521 Sweden, Signals Intelligence Act (Lag [2008:717] *om signalspaning i försvarsunderrättelsetjänst*), Art 11 (a).
522 Germany, *G 10 Act*, S. 12.
523 Wetzling, T. (2017), p. 14.
524 See FRA (2015a) p. 64 for further information on these restrictions in Spain and Latvia.
525 Latvia, Investigatory Operations Law, Art. 24 (1).
526 FRA (2015a), p. 65.
527 See FRA (2015a) p. 64 for further information on this restriction in Romania and Denmark.
528 Denmark, Administration of Justice Act, Consolidated Act no. 1255 of 16 November 2015 with amendments (*Retsplejeloven, lovbekendtgørelse nr. 1255 af 16. november 2015 med senere ændringer*), Section 788 (1), (4).
529 See FRA (2015a) p. 65 for further information on this in Bulgaria, Croatia and Germany.
530 Sweden, Signals Intelligence Act, Arts. 11 (a) and 11 (b).

13.4. Restrictions on notification obligations and right to access with safeguards

Some Member States provide for the involvement of the expert body or a court in scrutinising whether the invoked grounds for restricting the rights of notification or access are reasonable. Examples below show that further controls assessing justifications of restrictions differ from one Member State to another. Some Member States – such as Germany and the Netherlands – provide for review of a notification's exemption by the expert oversight bodies. Others – such as Cyprus, Greece and the United Kingdom – vest their DPA with such competence. These assessments by oversight bodies also show that the notification's obligation is not implemented evenly across EU Member States.

In Cyprus and Greece**,** the DPA may decide to restrict or lift the obligations to inform and grant access on the grounds of national security, upon request of the intelligence services, and as stipulated by the data protection laws. In Germany, the G 10 Commission decides for how long the information may be withheld, unless it unanimously decides that, even after five years, disclosing the information would endanger national interests.[531]

In the United Kingdom, the intelligence services may rely upon the exemption for national security cases, which is provided in the data protection law.[532] The Secretary of State has issued certificates exempting the intelligence services from the application of data protection principles. Nonetheless, the DPA may assess whether invoking the relevant exemptions justifying nondisclosure and/or the "neither confirm nor deny response" was justified. In assessing the lawfulness of the non-disclosure of the information, the DPA may ask the services for reasoned explanations but has access to confidential information only in very exceptional cases. Individuals will not be given access to any of the explanations or confidential information provided to the Information Commissioner by the intelligence services, unless very specific exceptions are met.[533]

531 Germany, *G 10 Act*, s. 12.
532 United Kingdom, Data Protection Act 1998, s. 28.
533 United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding on National Security Cases (DPA)', 2 September 2013.

Promising practice

Transparent scrutiny of denials of rights

In both the **Netherlands** and **Germany**, oversight bodies assess the grounds on which notification of or access to information was denied. As no one was notified between 2007 and 2010, in 2013 the CTIVD decided to launch a special investigation on the obligation to inform. The Dutch oversight body found out that in the meantime, thirteen persons had been notified. A similar investigation started in 2016.

In Germany, the G 10 Commission may decide to notify individuals based on information provided by the intelligence services. In 2016, the oversight body decided to not yet inform 1,040 persons/institutions, and unanimously agreed that 188 would never be informed. In cases of strategic surveillance, the G 10 Commission dealt with 58 cases for information related to international terrorism. In the majority of cases (51), the BND informed the G 10 Commission that the individual could not be individualised through the surveillance measure. In six cases, the commission decided to postpone providing the information; in no cases rejected the information indefinitely; and in one case took note that the intelligence service (BND) provided the information.

See The Netherlands, (CTIVD) (2013) and CTIVD (2016), p. 14; Germany, Federal Parliament (Deutscher Bundestag) *(2017a), pp. 6 and 8*

While discussing the difficulties of notifications and the right to access information, the respondents interviewed in the selected EU Member States shared a variety of opinions. For example, in cases of general communications surveillance, it might be problematic to notify all subjects of the intelligence activities or ensure access to information when the intelligence services have no data about a specific individual. These arguments are not relevant in case of completed targeted surveillance activities. During some interviews, representatives from the oversight bodies, and other experts, questioned the principle of notification in the context of fundamental rights protection. They maintained that the value would lie in a systematic implementation of the safeguards built in the oversight process that would possibly prevent breaches of an individual's fundamental right. If the whole system of checks and balances is implemented through effective oversight, redress might not be necessary. By drawing an analogy to 'privacy by design', the proposed approach can be called 'data protection oversight by design'. The interviewees questioned the value of having the duty of notification defined in the legislative framework but not applicable in practice. The respondents called for a possibility of individual legal protection, possibility to seek redress. Representatives

from civil society organisations, practicing lawyers and academia tended to identify non-application of the duty to notify as problematic, especially with regard to an individual who might seek remedies. They also questioned the effectiveness of the redress, which is often linked to notification.

To conclude, even if secrecy does restrict individuals' awareness, it does not completely exclude it, either. FRA's research findings show that freedom of information principles are completely exempted in the context of surveillance. In this case, a degree of proportionality could be applied to ensure that no blanket exception based on national security is applied to freedom of information laws. Consequently, the obligation to inform and the right of access, either separately or combined, are crucial enablers of individuals' awareness. FRA research indicates that in a large majority of Member States, these rights are restricted to meet national security and confidentiality requirements, but are not left unsupervised.

14

Remedial bodies' challenges: access to classified information and necessary expertise



14.1. Access to classified information

ECtHR Rules of the Court

Rule 33 – Public character of documents

1. All documents deposited with the Registry by the parties or by any third party in connection with an application (...) shall be accessible to the public (...).

2. Public access to a document or to any part of it may be restricted in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties or of any person concerned so require, or to the extent strictly necessary in the opinion of the President of the Chamber in special circumstances where publicity would prejudice the interests of justice.

3. Any request for confidentiality made under paragraph 1 of this Rule must include reasons and specify whether it is requested that all or part of the documents be inaccessible to the public.

Rule 63 – Public character of hearings

1. Hearings shall be public unless, in accordance with paragraph 2 of this Rule, the Chamber in exceptional circumstances decides otherwise, either of its own motion or at the request of a party or any other person concerned.

2. The press and the public may be excluded from all or part of a hearing in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the Chamber in special circumstances where publicity would prejudice the interests of justice.

3. Any request for a hearing to be held in camera made under paragraph 1 of this Rule must include reasons and specify whether it concerns all or only part of the hearing.

ECtHR, Rules of the Court, Registry of the Court, 14 November 2016, pp. 17 and 34

There is no harmonisation among Member States of the conditions under which classified information may be disclosed and used as evidence during judicial proceedings. Most Member States do not allow courts to use intelligence information that is not available to the parties and that does not meet evidential standards. In Italy, for example, every piece of evidence must be disclosed to all parties. Classification of documents can only be challenged by a judge or prosecutor in cases where such information may be deemed as having been illegitimately classified.[534]

The FRA 2015 report highlighted how NCND policy can make remedial bodies inaccessible in practice.[535] To tackle this challenge, and increase remedies' effectiveness and transparency, some Member States have established alternative mechanisms. These include the use of 'second-hand' evidence, the 'assumed facts', the 'closed material procedures', the establishment of open hearing and *in camera* sessions and the use of 'shielded witnesses'.

The United Kingdom has developed adapted procedures aimed at enhancing transparency in access to information for complaints involving classified intelligence. The Investigatory Powers Tribunal may assume, "for the sake of the argument", that the facts asserted by the complainant are true ('assumed facts').[536] It may also implement the so-called 'Closed Material Procedures', which allow the court to use classified information as evidence.[537] Section 68(6) of the RIPA, which was not amended by the IPA, provides that "[i]t shall be the duty of the persons specified in subsection (7) to disclose or provide to the Tribunal

534 See ECtHR, *Nasr and Ghali v. Italy*, No. 44883/09, 23 February 2016; Bigo, D., Carrera, S., et al. (2014), p. 112.
535 See FRA (2015a), p. 69.
536 United Kingdom, IPT, (2016), p. 8.
537 Bigo, D., Carrera, S., et al. (2014), pp. 21-25.

all such documents and information as the Tribunal may require for the purpose of enabling them (a) to exercise the jurisdiction conferred on them by or under section 65; or (b) otherwise to exercise or perform any power or duty conferred or imposed on them by or under this Act." In such cases, only the judges and security-cleared 'special advocates' may access secret information. Finally, the IPT may decide to hold open *inter-partes* hearings for cases involving classified information, either on the basis of agreed or assumed facts. The practice to hold open hearings have been increasingly used by the IPT, reaching a quarter of all the complaints decided by the Tribunal in 2015.[538]

It has been the long-standing policy of the United Kingdom government to give a NCND response to questions about matters sensitive to national security. The IPT recognised the legitimate purpose and value of such a response in several cases. It held that "if allegations of interception or surveillance are made, but not denied, then, in the absence of the NCND policy, it is likely to be inferred by a complainant that such acts are taking place",[539] and that it does not interfere with the right to privacy in cases where there is no relevant information held on the complainant.[540]

Similarly, in France, the 2015 intelligence law significantly enhanced the remedies available to individuals.[541] Complainants can now bring a case before a specialised chamber (*formation spécialisée)* of the Council of State, the highest administrative court. Judges sitting on the specialised chamber are security cleared *ex officio*. The procedure requires first that either the CNCTR or the CNIL – depending on the object of the complaint – performs initial checks (see section on quasi-judicial bodies). To safeguard the secrecy of the documents handled while at the same time ensuring effective remedies, asymmetric adversarial proceedings are prescribed by law. The complainant, who can be heard, does not see any confidential documents communicated by the services or the CNCTR and/or CNIL to the specialised chamber. The chamber sits in camera when dealing with secret documents. If no surveillance measure was implemented against the complainants, the chamber informs them that no illegality was observed after verification, without stating whether a surveillance measure was implemented. If an illegality is found, the complainant is informed and the chamber annuls the authorisation of the intelligence measure and orders the deletion of the collected data.

The specialised chamber of the Council of State also applies a policy where no confirmation nor denial is provided to the complainant, although only in cases where no illegality has been established. In such cases, the decision of the panel will not state whether a surveillance technique has or has not been implemented, nor will it assert whether the complainant is or is not included in a database managed by intelligence services. On the other hand, where unlawful surveillance – either in the application of a surveillance technique or in the processing of data – has been established by the Council of State, it informs the complainant and requests the annulment of the authorisation to implement a surveillance technique or the rectification, update or deletion of the data illegally processed. In May 2017, the specialised chamber issued for the first time a deletion order addressed to the Ministry of Defence, because it illegally processed personal data.[542]

Some states may use additional protection by bringing classified information as evidence through testimonies of anonymous witnesses. This is the case in Germany, Spain and the Netherlands. In the Netherlands, the Act on Shielded Witnesses allows members of the security services to disclose anonymously classified information during a specific procedure. Such procedure must be held before the trial, in closed session, and the information is only disclosed to the judge and security-cleared special advocates.[543] In Spain and Germany, courts may rely on 'second-hand' evidence, consisting of declarations made by officials who did not have direct access to the classified information but have received a description of such information. The information remains 'confidential' and should therefore be disclosed only to a limited and security-cleared number of persons.[544] These mechanisms, though, still present some limits, as they imbalance the adversarial procedure, in which the defendant, excluded from the hearings, will not have the possibility to challenge the evidence.

Some Member States allow judicial bodies to declassify information – for example, in France and Poland. In Poland, the Prosecutor General is entitled to challenge the secrecy clause (*klauzula tajności*) of classified information by either modifying or completely declassifying it.[545] In France, in cases where the specialised chamber considers the illegality to constitute an offence, it will forward all information to the prime minister, who will decide whether to declassify all or part of the confidential information.[546]

538 United Kingdom, IPT, (2016), p. 23.
539 *Ibid.* p. 10.
540 United Kingdom, IPT (2014).
541 France, Interior Security Code, Art. L. 841-1 and L. 841-2 as well as Administrative Justice Code, Art. L. 311-4-1 and L. 773- to L. 773-8.
542 France, Council of State (*Conseil d'Etat*), *M. A.B.*, No. 396669, 5 May 2017.
543 Bigo, D., Carrera, et al. (2014), pp. 25-26
544 *Ibid.* pp. 28 and 30.
545 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Art. 57.5.
546 France, Administrative Justice Code (*Code de justice administrative*), Art. L773-7.

Striking a balance

"[B]oth the principle of the separation of powers as well as the existence of other constitutional demands require that [the legislator] strikes a reasonable balance between the rights of the individuals involved to apply for judicial legal remedy and the right to a fair trial as well as [...] the constitutional requirements inherent to safeguarding the fundamental interests of the Nation."

France, Constitutional Court (Conseil constitutionnel), Mrs Ekaterina B., spouse of D., and others, Decision 2011-192 QPC, *10 November 2011 [translation by Constitutional Court]*

"As for the requirements to be met by judicial review of the existence and validity of the reasons invoked by the competent national authority with regard to State security of the Member State concerned, it is necessary for a court to be entrusted with verifying whether those reasons stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence. Thus, the competent national authority has the task of proving, in accordance with the national procedural rules, that State security would in fact be compromised by precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken (...). It follows that there is no presumption that the reasons invoked by a national authority exist and are valid. In this connection, the national court with jurisdiction must carry out an independent examination of all the matters of law and fact relied upon by the competent national authority and it must determine, in accordance with the national procedural rules, whether State security stands in the way of such disclosure.

If that court concludes that State security does not stand in the way of precise and full disclosure to the person concerned of the grounds on which a decision (...) is based, it gives the competent national authority the opportunity to disclose the missing grounds and evidence to the person concerned. If that authority does not authorise their disclosure, the court proceeds to examine the legality of such a decision on the basis of solely the grounds and evidence which have been disclosed. On the other hand, if it turns out that State security does stand in the way of disclosure of the grounds to the person concerned, judicial review (...) of the legality of a decision (...) must (...) be carried out in a procedure which strikes an appropriate balance between the requirements flowing from State security and the requirements of the right to effective judicial protection while limiting any interference with the exercise of that right to that which is strictly necessary."

CJEU, C-300/11, ZZ v. Secretary of the State of Home Department, *4 June 2013, paras. 60-64*

"Nonetheless, it would have been desirable – to the extent compatible with the preservation of confidentiality and effectiveness of the investigations concerning the applicant – for the national authorities, or at least the Supreme Administrative Court, to have explained, if only summarily, the extent of the review they had carried out and the accusations against the applicant. (...) Having regard to the proceedings as a whole, to the nature of the dispute and to the margin of appreciation enjoyed by the national authorities, the Court considers that the restrictions curtailing the applicant's enjoyment of the rights afforded to him in accordance with the principles of adversarial proceedings and equality of arms were offset in such a manner that the fair balance between the parties was not affected to such an extent as to impair the very essence of the applicant's right to a fair trial."

ECtHR, Regner v. The Czech Republic [GC], *No. 35289/11, 19 September 2017, paras. 160-161*

14.2. Necessary expertise

Past FRA research has identified the judges' lack of specialisation in data protection as a serious obstacle to effectively remedy data protection violations.[547] This finding is relevant for surveillance, where, in addition to the necessary secrecy linked to intelligence, relevant expertise in ICT or in intelligence, for instance, is essential.

In the area of surveillance, the highly technical nature of intelligence matters requires relevant expertise on the part of the judge. From the perspective of a complainant, judicial lack of expertise in dealing with intelligence services may lead a judge to defer to the national intelligence services and their claim that national security and other special circumstances apply.[548]

Lack of expertise can be circumvented by establishing specific mechanisms. In most cases, where bodies are granted remedial powers but lack technical understanding of the matters, complementarity is established with either *ad hoc* experts or non-judicial expert bodies. Another form of tackling the lack of specialisation of the judges is the establishment of quasi-judicial bodies. The following section details how some Member States have developed these mechanisms to allow expert assessment of complaints.

547 FRA (2014c).

548 Forcese, C. (2012), p. 186.

Cooperation and complementarity between remedial and expert bodies

Some expert bodies, although not able to issue binding decisions, play an essential complementary role within the remedial landscape. Their expert understanding of both the technicalities and the legal framework put them in a good position to review complaints. Thus, when such experts are allowed to communicate with judicial or non-judicial bodies entitled to issue binding decisions, such cooperation can fill the expertise gap.

In France, individuals can ask the CNCTR to check whether a domestic or international surveillance technique was illegally implemented against them.[549] The commission follows the same verification procedure as for *ex post* controls launched on its own initiative.[550] Once completed, individuals are informed that a verification procedure took place. No further information is provided. Should the verification reveal an illegality, the CNCTR can address a recommendation to the prime minister, the relevant minister and the intelligence service requesting the suspension of the surveillance measure and the destruction of the data collected.[551] When the recommendations are not followed, the president or three members of the CNCTR can bring the case before the Council of State.[552] The CNCTR received 51 such verification requests during the first year since its establishment.[553] The Danish Oversight Board (TET) proceeds in a similar manner. However, in very specific cases with special circumstances, it can grant individuals full or partial access to information held by the services.[554]

In the Netherlands, the Intelligence and Security Services Act adopted in 2017 modifies the remedial mechanism available to individuals. While until the new law comes into force, the Dutch expert body (CTIVD) acts as an "independent complaints advisory committee"[555] in the sense that individuals are not able to complain directly to the CTIVD and the latter is not able to issue binding decisions, the 2017 Act creates a sub-committee within the CTIVD, responsible for handling complaints and issuing binding decisions.[556]

549 France, Interior Security Code, Art. L. 833-4 and L. 854-9.
550 France, CNCTR (2016), p. 90.
551 France, Interior Security Code, Art. L. 833-6.
552 *Ibid.* Art. L. 833-8.
553 France, CNCTR (2016), p. 90.
554 Denmark, Act on the Danish Security and Intelligence Service, Consolidated Act no. 1600 of 19 December 2014 with amendments, Section 13 (2) and Denmark, Act on the Danish Defence Intelligence Service, Consolidated Act no 1 of 4 January 2016, Section 10 (2). See also TET's website.
555 The Netherlands, CTIVD (2015), p. 19.
556 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Arts. 97, 114 and 126.

The FRA 2015 report highlighted existing cooperation between some DPAs and the courts, and in particular the *Schrems v. Data Protection Commissioner* case.[557] Complementarity is also crucial at an earlier stage, where some non-judicial bodies act as a filter to assess the legitimacy of the complaints to transfer only well-founded ones to the competent remedial body. This is the case, for instance, in Belgium, where citizens' petitions submitted to the Belgium Ombudsman (*Médiateurs*) and referring to the intelligence services can be forwarded to the Belgian expert body, the Standing Committee I. Before transferring a complaint to the Standing Committee I, the Ombudsman will assess the complaint and preselect relevant petitions from those that are deemed irrelevant because, for example, they are based on 'paranoia'. Such partnership among bodies is an important tool to enhance remedies' effectiveness, as it enables the competent remedial body to focus its assessment only on well-grounded complaints.

This trend was confirmed during the interviews FRA conducted in selected Member States. In France, for example, the members of the specialised chamber of the Council of State (*Conseil d'Etat*) have been trained on the techniques used by the intelligence services. In Sweden, the integrity protection counsels (some of whom are former judges) – who are appointed by the government to protect the interest of the people before the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*) – noted that the court provides them with training on the legal framework and substance to facilitate their work. Representatives of the United Kingdom's Investigatory Power Tribunal arranged visits of judges to the premises of the intelligence services or law enforcement institutions to permit them to gain direct knowledge of general surveillance of communication.

Quasi-judicial bodies

Four Member States – France, Germany, Ireland and the United Kingdom – introduced a system of specialised judges or courts to deal with cases in the area of surveillance. In addition, oversight bodies in Germany and Belgium (the G10 Commission and the Standing Committee I) are given powers similar to those of a court, qualifying them as quasi-judicial mechanisms. The composition, competences and procedures followed by the British IPT, the Irish Complaints Referee, the Belgian Standing Committee I and the German G10 Commission are detailed in the FRA 2015 report.[558] In France, the 2015 law on intelligence

557 FRA (2015a), p. 68.
558 FRA (2015a), pp. 68-69.

established a special litigation procedure, through which a specialised chamber (*formation spécialisée)* of the Council of State has competence to decide on complaints related to surveillance techniques. This formation is composed of a president and four judge-rapporteurs. Specific procedures were designed to conciliate the obligation to respect the secrecy of the files with the adversarial procedure.[559]

In the United Kingdom, between 2014 and 2017, the IPT handed down seven judgments in relation to intelligence and security services.[560] The Independent Reviewer of Terrorism Legislation recommended that the IPT have its jurisdiction expanded, that it be given the power to make declarations of incompatibility, and that its rulings be subject to appeal on points of law.[561] Of these recommendations, the Investigatory Powers Act followed the suggestion regarding appeals on points of law.[562] However, applicants need to be given permission (leave) to appeal by the IPT, or if that is refused, by the relevant appellate court.[563]

This report's findings confirm the FRA 2015 report's conclusions that quasi-judicial mechanisms contribute to the development of expertise in this area, and reinforce remedial actors' access to classified information.[564]

Number of complaints received by specialised judicial or quasi-judicial bodies

In 2015, 35 % of the 251 complaints received by the IPT were directed against intelligence services. The remaining complaints were directed against other types of public authorities that fall under the mandate of the IPT, such as law enforcement agencies (42 %); local authorities (12 %); and other public authorities, such as the Department for Work and Pensions (10 %). There are no specific statistics available in the IPT's annual report as to how many of the complaints directed against an intelligence agency were actually upheld in 2015. General statistics on the outcomes of 2015 complaints indicate, however, that the IPT upheld the complaint and ruled in favour of the complainant in eight of 251 cases (which covers all complaints resolved by the IPT in 2015, including those carried over from previous years).

United Kingdom, IPT (2016), p. 22

In October 2016, the Council of State issued its first decisions. In March 2017, 146 complaints were registered (136 concerning intelligence files and 10 concerning intelligence measures). A total of 52 decisions delivered. Some of these decisions highlighted the compatibility of the procedure with the ECHR.

France, Council of State, Contrôle des techniques de renseignement, *19 October 2016, CNCTR (2016), pp. 91-93; and France, DPR & CNCTR (2017), p. 37*

Finally, individuals who are unsatisfied with the decisions made by a judicial or non-judicial body may appeal this decision. In some cases, individuals may appeal a decision at national level: in Austria, for instance, individuals may lodge a complaint to the DPA following a decision made by the Legal Protection Commissioner in cases where security is at stake.[565] However, in most cases, the only route available will be to apply to the ECtHR. In the United Kingdom, until adoption of the Investigatory Powers Act in 2016, the only route for appeal following a decision by the IPT was the ECtHR. This absence of judicial review was challenged in 2017, and the Divisional Court confirmed that RIPA did not provide for appeal to the decision of the IPT.[566] Article 67A of the Investigatory Powers Act has tackled this issue and now provides the possibility for individuals to appeal any determination of the Tribunal to either the Court of Appeal in England and

559 France, Conseil d'Etat.
560 United Kingdom, IPT, *Belhaj v. Straw*, IPT/13/132-9H, 7 February 2014, *Liberty, Privacy International, Bytes for All and Amnesty v. UK*, judgments of 5 December 2014 and 6 February 2015, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 22 June 2015, *Privacy International and Greennet & Others v. the Secretary of State for Foreign and Commonwealth Affairs and GCHQ*, IPT 14/85/CH, 12 February 2016, *Privacy International v. the Secretary of State for Foreign and Commonwealth Affairs, GCHQ, MI5 and MI6*, IPT/15/110/CH, 17 October 2016, and *Privacy International & Others*, [2016] UKIPTrib 15_110-CH, 8 September 2017.
561 Anderson, D. (2015), p. 305.
562 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 67A.
563 United Kingdom, Investigatory Powers Act 2016, s. 67A (6) (b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
564 FRA (2015a), pp. 68-69.
565 Austria, Police State Protection Act (*5. Bundesgesetz mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden*), BGBl. I Nr. 5/2016, Art. 14.
566 United Kingdom, *R (On the Application Of) v Investigatory Powers Tribunal, Court of Appeal - Administrative Court, February 02, 2017,* [2017] EWHC 114 (Admin), 2 February 2017.

Wales or the Court of Session, whichever appears to be the most appropriate to the court.[567]

Previous sections identified two main challenges for both judicial and non-judicial remedial bodies in reviewing complaints: denials of access to classified information and a lack of expertise, much needed in such a complex area. However, FRA's research findings show that innovative systems introduced in some Member States – alternative mechanisms to access classified data, complementarity between remedial and expert bodies, establishment of quasi-judicial bodies and adapted adversarial procedures – may circumvent the main obstacles to judicial bodies implementing effective remedies, by introducing partial access to information and a certain level of expertise. On this basis, remedial bodies will have the ability to perform informed investigations and deliver reasoned decisions. An effective remedy is secured when a binding decision includes the order to terminate the surveillance measure, destroy the data and provide individuals with appropriate compensation. Less than two thirds of EU Member States provide remedial bodies with both access to the information and binding decisions. General surveillance of communications makes effective remedies even more difficult to implement. Remedies can only be provided on an individual basis, i.e. after identification of the individual who has submitted a complaint within the general data collected.

567 United Kingdom, Investigatory Powers Act (2016), s. 67A. Not yet in force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

General conclusions

ECtHR case law: using oversight to enhance citizens' trust

"[T]he external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance [...] by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 79

While this report shows that most EU Member States have enacted intelligence laws and have tasked independent expert bodies with overseeing the work of their intelligence services, it also reveals that opinions of these bodies' efficiency are mixed. Similarly, although diverse remedies are provided for in law, critics contend that actually accessing them is a less straightforward matter. Failing to confront these flaws carries the risk of undermining the public's trust in their governments' pledges to uphold the rule of law even when confronted with challenges that may make short-cuts look tempting.

With international intelligence cooperation as an absolute must in light of today's myriad threats, accountability, too, has to take on cross-border dimensions. Introducing safeguards specifically tailored to international cooperation would both ensure that intelligence sharing is conducted in a fundamental rights-compliant manner and reinforce the credibility of any data received. This would ultimately strengthen trust among partners – in turn encouraging more cooperation efforts, which have the potential to bring widespread benefits to the European public and beyond. Effective cooperation among oversight entities in different Member States could play an important role in fostering such trust.

"We want to strengthen our ties with the [other] European oversight committees, parliamentary, non-parliamentary, expert bodies, does not matter, everybody is welcome here and we do visits to them, and not only to say 'hello, how are you', but we also are trying to set up a system that we can work together." (Expert body)

Effective accountability systems involve a plurality of actors and require continuity, i.e., provide for oversight before, during and after any surveillance measures are utilised. As the European Court of Human Rights has emphasised, and as outlined in this report, certain safeguards are indispensable for ensuring accountability, particularly given the need for secrecy to carry out effective surveillance work. These include providing for reviews of the legality of measures deployed, and ensuring that entities overseeing the work are independent, have adequate resources (including expert knowledge), are accorded sufficient competences (including access to classified data), and are transparent.

Data protection rules and other rule of law principles should not be seen as potential hurdles to protecting the security of Europe's citizens, but instead as sources of mutual benefits for individuals and intelligence services. Respecting these rights and principles paves the way for more accurate data collection and analysis, renewed trust among European citizens towards their intelligence services and, as a result, a more effective defence of national security.

References

Access, Electronic Frontier Foundation, and Privacy International (2014), *International Principles on the Application of Human Rights to Communications Surveillance* (Necessary and Proportionate Principles), May 1994.

Anderson, D., Independent Reviewer of Terrorism Legislation (2015), *A question of trust: Report of the investigatory powers review*, London, 11 June 2015.

Anderson, D., Independent Reviewer of Terrorism Legislation (2016), *Report of the bulk powers review*, London, August 2016.

Belgium, House of Representatives (2016), 'Magazine La chambre', *LaChambre.be*.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2015), *Rapport d'activités 2014 Activiteitenverslag 2014*, Antwerp and Cambridge, Intersentia.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2016), *Rapport d'activités 2015 Activiteitenverslag 2015*, Antwerp and Cambridge, Intersentia.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. and Scherrer, A., Policy Department C: Citizens' Rights and Constitutional Affairs (2013), *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, Brussels, European Parliament Directorate-General for Internal Policies.

Born, H. (2003), *Parliamentary Oversight of the Security Sector – Principles, mechanisms and practices*, Geneva, Centre for the Democratic Control of Armed Forces (DCAF) and Inter-Parliamentary Union (IPU).

Born, H. and Leigh, I. (2005), *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*, Oslo, Publishing House of the Parliament of Norway.

Born, H., Leigh, I. and Wills, A. (2015), *Making international intelligence cooperation accountable*, Geneva, Centre for the Democratic Control of Armed Forces (DCAF).

Born, H. and Wills, A. (eds.) (2012), *Overseeing intelligence services: A toolkit*, Handbook, Geneva, Centre for the Democratic Control of Armed Forces (DCAF).

Bos-Ollermann, H. (2016), *New surveillance legislation & intelligence oversight challenges: the Dutch experience*, International Intelligence Oversight Forum 2016.

Brown, I., Halperin, M., Hayes, B., Scott, B. and Vermeulen, M. (2015), 'Towards multilateral standards for surveillance reforms', Oxford Internet Institute Discussion Paper, January 2015.

Bulgaria, National Bureau for Control over Special Intelligence Means (*Национално бюро за контрол на специалните разузнавателни средства, NBKSRS*) (2017), *Report of the National Bureau for Control over Special Intelligence Means for the performance of the operations in 2016* (*Доклад На Националното Бюро За Контрол На Специалните Разузнавателни Средства За Извършената Дейност През 2016 Г)*, Sofia, 31 May 2017.

Burgstaller, M. and Kubarth, L. (2016), 'Zentrale Daten des Rechtsschutzbeauftragten für 2015', SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3).

Cameron, I. (2013), 'Foreseeability and safeguards in the area of security: Some comments on the ECHR case law', in: Van Laethem, W. and Vanderborght, J. (eds.), Vast Comité I, Comité Permanent Contrôle des Services de Renseignements et de Sécutrité, *Inzicht in toezicht: Regards sur le contrôle*, Antwerp and Cambridge, Intersentia, pp. 163–180.

Council of Bars and Law Societies of Europe - CCBE (2016), *Recommendations on the protection of client confidentiality within the context of surveillance activities*, Brussels, CCBE.

Council of Europe, Commissioner for Human Rights (2015), 'Democratic and effective oversight of national security services', Issue paper, Strasbourg, Council of Europe.

Council of Europe, Commissioner for Human Rights (2016), *National human rights structures: protecting human rights while countering terrorism*, 6 December 2016.

Council of Europe, Committee of Ministers (2013), *Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*, 11 June 2013.

Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), 'Freedom of expression and democracy in the digital age: Opportunities, rights, responsibilities', Keynote speech by Nils Muižnieks, Council of Europe Commissioner for Human Rights,CommDH/Speech(2013)12, Belgrade, 7-8 November 2013.

Council of Europe (2016b), *Mass Surveillance – Who is watching the watchers?*, Strasbourg, Council of Europe Publishing.

Cousseran, J.-C. and Hayez, P. (2015), *Renseigner les démocraties, renseigner en démocratie*, Paris, Odile Jacob.

Croatia, Council for Civilian Oversight (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*) (2011), Summary of work report for 2010 (*Sažetak Izvješća O Radu Za 2010. Godinu*), Zagreb, March 2011.

de With, H. and Kathmann, E. (2011), 'Annex A-III: Parliamentary and specialised oversight of security and intelligence agencies in Germany' in: Wills, A., Vermeulen, M., Born, H., Scheinin, M., Wiebusch, M. and Thornton, A., Policy Department C: Citizens' Rights and Constitutional Affairs, *Parliamentary oversight of security and intelligence agencies in the European Union*, PE 453.207, Brussels, European Parliament Directorate-General for Internal Policies, pp. 218–229.

Deeks, A. (2016), 'Global Change and Megatrends, Implications for intelligence and its oversight', in: Goldman, Z. and Rascof, S. eds, *Global Intelligence Oversight*, Oxford University Press, Oxford, 2016.

Dietrich, J.-H. and Eiffler, S. (eds) (2017), *Handbuch des Rechts der Nachrichtendienste*, Boorberg Verlag, Stuttgart.

Dreusicke, L. (2017), 'Präsidentin des BGH in Osnabrück: Wer das Ausspähen des BND kontrollieren soll', *Osnabrücker Zeitung*, 27 April 2017.

European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council, "Enhancing Security in a world of mobility; improved information exchange in the fight against terrorism and stronger external border", COM(2016)602, Brussels, 14 September 2016.

European Commission for Democracy through Law (Venice Commission) (2007), *Report on the democratic oversight of the security services,* Study No. 388/2006, Doc. CDL-AD(2007)016, Strasbourg, Council of Europe, 11 June 2007.

European Commission, Juncker, J.-C. (2016), 'Juncker after Brussels terror attacks: "We need a Security Union"', Joint Press Conference with French Prime Minister Manuel Valls, 24 March 2016.

European Parliament (2014), *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*, P7_TA (2014)0230, 12 March 2014.

Finland, Ministry of Interior (2017), *Civilian Intelligence Legislation, Working Group Report, Ministry of Interior 8/2017 (Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017)*, Helsinki, 19 April 2017.

Foegle, J.-P. (2015), 'De Washington à Paris, la "protection de carton" des agents secrets lanceurs d'alerte', *Revue des droits de l'homme*, 6 June 2015.

Forcese, C. and LaViolette, N. (2006), Ottawa Principles on Anti-terrorism and Human Rights (2006), Toronto, 1 October 2006.

Forcese, C. (2012), 'Tool 9: Handling complaints about intelligence services', in: Born, H. and Wills, A. (eds.), *Overseeing intelligence services: A toolkit*, Geneva, DCAF, pp. 181–200.

FRA (2014a), *Fundamental rights: Challenges and achievements in 2013 – Annual report*, Luxembourg, Publications Office.

FRA (2014b), 'Ad hoc information request: National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies,' *Franet Guidelines*, Vienna, 18 August 2014.

FRA (2014c), *Access to data protection remedies*, Luxembourg, Publications Office.

FRA (2015a), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Members States' legal framework*, Luxembourg, Publication Office.

FRA (2015b), *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update – Guidelines for FRANET,* Vienna, 30 November 2016.

FRA (2017), *Monthly data collection on the current reform of intelligence legislation in Belgium, Finland, France, Germany, the Netherlands, Sweden and the United Kingdom – Guidelines for FRANET*, Vienna, 25 November 2016.

France, Adam, P., Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement, DPR*) (2017), *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016* (Annual Report 2016), Doc. No. 4573 (Assemblée nationale), Doc. No. 448 (Sénat), Assemblée Nationale and Sénat, 2 March 2017.

France, Défenseur des Droits (2017), *Avis du Défenseur des droits n°17-05*, 7 July 2017.

France, Commission Nationale Consultative des Droits de l'Homme (2015), *Avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la Présidence de l'Assemblée nationale*, 16 April 2015.

France, Commission Nationale Consultative des Droits de l'Homme (2016), *Avis sur le projet de loi de lutte contre le crime organisé et le terrorisme*, 17 March 2016.

France, Commission Nationale Consultative des Droits de l'Homme (2017a), *Avis sur la loi relative à la sécurité*, 23 February 2017.

France, Commission Nationale Consultative des Droits de l'Homme (2017b), *Avis sur le projet de loi visant à renforcer la sécurité intérieure et la lutte contre le terrorisme*, 6 July 2017.

France, Le Monde, *Jacques Toubon : le projet de loi antiterroriste est « une pilule empoisonnée »*, 22 June 2017.

France, National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés*, CNIL) (2016), *Rapport d'activité 2015*, Paris, La documentation française.

France, CNIL (2015), *Rapport d'activité 2014*, Paris, La documentation française.

France, CNIL (2014), *Rapport d'activité 2013*, Paris, La documentation française.

France, National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement, CNCTR*) (2016), *1er rapport d'activité 2015/2016*, Paris.

France, Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement, DPR*) & National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement, CNCTR*) (2017), *Colloque consacré au contrôle et à l'évaluation de la politique publique du renseignement, mercredi 22 mars 2017, projet de compte rendu*, Paris.

France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement*) (2014), *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014* (Annual Report 2014), Doc. No. 2482 (Assemblée nationale), Doc. No. 201 (Sénat), Assemblée Nationale and Sénat, 18 December 2014.

Gajdošová, J. (2017), 'Legal redress mechanisms for individuals against intelligence action', in Dietrich/Sule (eds.), *Intelligence Law and Policies in Europe: a handbook*, forthcoming.

Germany, German Institute for Human Rights (*Deutsches Institut für Menschenrechte*) (2016), Menschenrechtliche Anforderungen an die Ausland-Ausland-Fernmeldeaufklärung und ihre Kontrolle, Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 26. September 2016.

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2017), *Activity report on data protection for the years 2015 and 2016 (26. Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016)*, Bonn, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn, 30 May 2017.

Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), *Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2013 bis November 2015)*, Drucksache No. 18/7962, 21 March 2016.

Germany, Federal Parliament (*Deutscher Bundestag*) (2016b), *Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Article 10-Gesetz-G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2014),* Drucksache No. 18/7423, 29 January 2016.

Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), *Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Article 10-Gesetz-G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2015),* Drucksache No. 18/11227, 16 February 2017.

Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), *Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes – Beschlussempfelung*, Drucksache No. 18/12850, 23 Juni 2017.

Gohin, O. and Latour, X. (eds.) (2016), *Code de la sécurité intérieure 2016*, LexisNexis, Paris.

Greece, Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2016), *Activity Report for the year 2015*, State Printing Office.

Heumann, S. and Wetzling, T., Stiftung neue Verantwortung (2014), 'Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle', *Europäische Digitale Agenda: Privacy Project*, May 2014.

Huber, B. (2013), 'Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite', *Neue Juristische Wochenzeitschrift*, Vol. 32, No. 35, pp. 2572–2577.

Italy, Italian Government (*Governo italiano*) (2013), 'Sicurezza dati personali: Protocollo d'intenti tra l'Autorità Garante e il Direttore Generale del Dis', Press release, 11 November 2013.

Italy, Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza*

della Repubblica, COPASIR) (2014), *Relazione annuale (Attività svolta dal 6 giugno 2013 al 30 settembre 2014)*, Doc. XXXIV No.1, Senate of the Republic (*Senato della Repubblica*), Chamber of Deputies (*Camera dei Deputati*), 11 December 2014.

Italy, COPASIR (2015), 'Report on so-called "Butterfly" and "Return" operations and on the affair "Flamia"' ('*Relazione sulle cosiddette operazioni "Farfalla" e "Rientro" e sulla vicenda "Flamia"*'), Rome, 12 March 2015.

Italy, COPASIR (2017), *Relazione annuale (Attività svolta dal 1 gennaio 2016 al 31 dicembre 2016)*, Doc. XXXIV No.4, Senate of the Republic (*Senato della Repubblica*), Chamber of Deputies (*Camera dei Deputati*), 22 February 2017.

King J. (2016), 'Introductory remarks by the Commissioner-designate Sir Julian King to the LIBE Committee', Press release, Strasbourg, 12 September 2016.

Kojm, C. (2016), 'Global Change and Megatrends, Implications for intelligence and its oversight', in: Goldman, Z. and Rascof, S. eds, *Global Intelligence Oversight*, Oxford University Press, Oxford, 2016.

Korff, D. et al (2017*), Boundaries of Law – Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes – Global Report*, World Web Foundation.

La Quadrature du net (2015), 'Three French NGOs challenge French international surveillance', Press release, 3 September 2015.

Lefebvre, N. (2015), *Les services de renseignement européens face au terrorisme : coopération ou cloisonnement*, Presses Académiques Francophones, Saarbrücken, 2015.

Löning, M., Stiftung neue Verantwortung (2015), 'Eine Reformagenda für die deutschen Geheimdienste: Rechtstaatlich, demokratisch, effektiv', *Europäische Digitale Agenda: Privacy Project*, Impulse, 15 April 2015.

Lorenz, P. (2017), 'BND-Kontrolle am BHG: Unabhängiges Gremium nimmt Arbeit auf', *Legal Tribune Online*, 9 March 2017.

Luxembourg, Commission (*autorité de contrôle*) of the Criminal Investigation Code (Code d'Instruction Criminelle) (2016), *Report of the execution of the commission's mission during the years 2014 and 2015 (Rapport rendant compte de l'exécution de la mission de l'autorité de contrôle pendant les années 2014 et 2015)*, Luxembourg, 16 March 2016.

Luxembourg, Commission Nationale la Protection des Données (CNPD) (2016), *Rapport Annuel 2015,* 13 June 2016.

Mills, A. and Sarikakis, K. (2017), 'Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism', Big Data & Society, July – December 2016.

Omand, D. (2014), 'The future of intelligence. What are the threats, the challenges and the opportunities?', in Duyvesteyn, I., de Jong, B., van Reijn, J. eds, *The Future of Intelligence, Challenges in the 21st century*, London and New York, Routledge, 2014.

Open Society Justice Initiative (2013), Global Principles on National Security and the Right to Information (Tshwane Principles), Tshwane, South Africa, 12 June 2013.

Parliamentary Assembly of the Council of Europe (PACE) (1999), 'Control of internal security services in the Council of Europe Member States', Report Doc. 8301, 23 March 1999.

PACE, Committee on Legal Affairs and Human Rights (2015), *Improving the protection of whistleblowers*, Report Doc. 13791, Strasbourg, 6 June 2015.

Palacios, J.-M. (2016), 'L'expérience d l'Intcen européen : un concept commun du renseignement pour une communauté culturellement diverse' in Laurent, S.-Y. and Warusfel, B. (1st ed), *Transformations et Réformes de la sécurité et du renseignement en Europe*, Presses Universitaires de Bordeaux, p. 297.

Peers, S. (2016), *EU Justice and Home Affairs Law, Volume II: EU Criminal Law, Policing and Civil Law* (4th ed), Oxford, Oxford University Press.

Ranking Digital Rights (2017), *2017 Corporate Accountability Index*, Washington DC, Ranking Digital Rights.

Schenke, W.-R., Graulich, K. and Ruthig, J. (2014), *Sicherheitsrecht des Bundes*, Munich, Beck.

Singer, J. (2016), *Praxiskommentar zum Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes*, Springer-Verlag, Berlin Heidelberg.

Sule, S. (2006), *Spionage – Völkerrechtlich, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage*, Nomos, Baden-Baden.

Sule, S. (2017), 'EU law restraints on Intelligence Activities in view of National Security' in: Dietrich, J.-H. and Sule S. (1st ed.), *Intelligence Law and Policies in Europe: A Handbook*, Oxford, C.H. Beck, Hart, Nomos (*forthcoming*)

Sweden, Swedish Parliament (2007), Parliamentary communication (Riksdagsskrivelse 2007/08:266) on the Government Bill "Adaptation of Defence Intelligence Activities" *(Proposition 2006/07:63, En anpassad försvarsunderrättelseverkamhet*), 8 March 2007.

Sweden, State Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) (2017), *Annual Report 2016 (Årsredovisning och årsberättelse 2016)*, Stockholm, 21 February 2017.

Sweden, National Defence Radio Establishment (*Försvarets radioanstalt*) (2016), Article about the Swedish Foreign Intelligence Inspectorate's review of the National Defence Radio Establishment (*Artikel I DN om SIUN-granskning av FRA*), 12 December 2016.

Sweden, State Official Reports (*Statens Offentliga Utredningar*) (2016), *The general responsibility of the supervision of private life (Ett samlat ansvar för tillsyn över den personliga integriteten)*, Stockholm 2016.

Töpfer, E. (2013), *Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei,* Berlin: Deutsches Institut für Menschenrechte (Policy Paper, 21).

The Netherlands, General States (*Staten-Generaal*) (2017), Parliamentary Document 34588, Nr. 67, 2 May 2017.

The Netherlands, National Government (*Rijksoverheid*) (2016), Infographic about AIVD and MIVD's method of interception of information (*'Gemoderniseerde Wet op de inlichtingen- en veiligheidsdiensten: extra bescherming veiligheid én privacy'*), Press Release 28 October 2016.

The Netherlands, Review Committee on the intelligence and Security Services (CTIVD) (2009), Review Report no. 22A *on the cooperation of the GISS with foreign intelligence and/or security services,* The Hague, 12 August 2009.

The Netherlands, Review Committee for the Intelligence and Security Services (CTIVD) (2010), *Annual Report 2009-2010*, The Hague, 31 March 2010.

The Netherlands, CTIVD (2012), Monitoring Report No. 33 (*Toezichtsrapport CTIVD, nr. 33 inzake de rubricering van staatsgeheimen door de AIVD*), The Hague, 13 June 2012.

The Netherlands, CTIVD (2014), *Annual Report 2013-2014*, The Hague, 31 March 2014.

The Netherlands, CTIVD (2015), *Annual Report 2014-2015*, The Hague, 9 June 2015.

The Netherlands, CTIVD (2016a), *Annual Report 2015*, The Hague, 7 June 2016.

The Netherlands, CTIVD (2016b), *on the implementation of cooperation criteria by the AIVD and the MIVD*, The Hague, 4 May 2016.

The Netherlands, CTIVD (2016c), *The CTIVD's View on the ISS Act 20.. Bill*, November 2016.

The Netherlands, CTIVD (2016d), *Review report No. 49 on the exchange of unevaluated data by the AIVD and the MIVD, May 2016*.

The Netherlands, CTIVD (2017), *Annual Report 2016*, The Hague, 24 July 2017.

Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*)(2016), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page.

United Kingdom, Home Office (2015), 'Code of Practice of Acquisition and Disclosure of Communications Data', March 2015.

United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', 23 February 2017.

United Kingdom, House of Commons Library (2017), Intelligence and Security Committee, Briefing Paper, No. 02178, 14 June 2017.

United Kingdom, House of Lords (2016), Transcripts of debate on Investigatory Powers Bill, 17 October 2016.

United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), *Privacy and security: A modern and transparent legal framework*, London, 12 March 2015.

United Kingdom, ISC (2016), *Annual Report 2015-16,* London, 5 July 2016.

United Kingdom, ISC (2016), *Report on the draft Investigatory Powers Bill*, London, 9 February 2016.

United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2017), *Statement on work completed since July 2016*, London, 27 April 2017.

United Kingdom, Intelligence Services Commissioner (2016), *Report of the Intelligence Services Commissioner for 2015*, No. HC 459 SG/2016/96, London, July 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2014), *Annual Report of the interception of communications commissioner (covering the period of January to December 2013)*, No. HC 1184 SG/201425, London, April 2014.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016a), *Annual Report for 2015 (covering the period January to December 2015)*, No. HC 255 SG/2016/68, London, September 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016b), *Review of directions given under section 94 of the Telecommunications Act 1984*, No. HC 33 SG/2016/67, London, July 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016c), *IOCCO Points to Consider on the Investigatory Powers Bill* (*IP Bill*), London, 23 March 2016.

United Kingdom, IPT (2016), *Investigatory Powers Tribunal Report 2011 – 2015*.

United Kingdom, Ministry of Justice (2014), *'Memorandum of understanding on National Security Cases (DPA)'*, 2 September 2013.UN (United Nations), General Assembly (GA) (2014a), Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age, A/RES/68/167, 21 January 2014.

UN, GA (2014a) Resolution on the Right to Privacy in the digital age, Doc. A/RES/69/166, 18 December 2014.

UN, GA (2014b), The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, Doc. A/69/276, 7 August 2014.

UN, GA (2016a), Resolution on the Right to Privacy in the digital age, Doc. A/C.3/71/L.39/Rev.1, 16 November 2016.

UN, GA (2016b), Resolution adopted by the General Assembly on 1 July 2016: The United Nations Global Counter-Terrorism Strategy Review, Resolution A/RES/70/291, 19 July 2016.

UN, GA (2016c), Resolution on the right to privacy in the digital age, Doc. A/RES/71/199, 19 December 2016.

UN, GA (2016d), Report of the Special Rapporteur on the right to privacy, Cannataci, J., Doc. A/71/368, 30 August 2016.

UN, Human Rights Committee (2014), Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23 April 2014.

UN, Human Rights Committee (2015), Concluding observations on the fifth periodic report of France, CCPR/C/FRA/CO/5, 21 July 2015.

UN, Human Rights Council (2009), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, Scheinin, M.*, Doc. A/HRC/10/3, 4 February 2009.

UN, Human Rights Council (2010), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, Scheinin, M.*, Doc. A/HRC/14/46, 17 May 2010.

UN, Human Rights Council (2014), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Emmerson, B.*, Doc. A/69/397, 23 September 2014.

UN, Human Rights Council (2016), Resolution on the safety of journalists, Doc. A/HRC/33/L.6, 26 September 2016.

UN, Human Rights Council (2016), *Report of the Special Rapporteur on the right to privacy, Cannataci, J.*, Doc. A/HRC/31/64, 24 November 2016.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Emmerson, B.*, Doc. A/HRC/34/61, 21 February 2017.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the right to privacy, Cannataci, J.*, Doc. A/HRC/34/60, 24 February 2017.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Kaye, D., Doc. A/HRC/35/22, 30 March 2017.

UN, Human Rights Council (2017), *Resolution on the right to privacy in the digital age*, Doc. A/HRC/RES/34/7, 7 April 2017.

UN, Office of the High Commissioner for Human Rights (OHCHR) (2014), *The right to privacy in the digital age,* A/HRC/27/37, 30 June 2014.

UN, Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media, the Organization of American States (OAS), the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (2015), 'Joint declaration on freedom of expression and responses to conflict situations', Statement, 4 May 2015.

United States, National Research Council (2015), *Bulk collection of signals intelligence: Technical options*, Washington, The National Academies Press.

Urvoas, J.-J. (2015), 'Contrôler les services, la juste place du Parlement', in : CNCIS (2015b), *23e rapport d'activité : Années 2014-2015*, Paris, La documentation française, pp. 33–42.

Vande Walle, G. (2013), 'Le traitement des plaintes et des dénonciations: Une mission distincte pour le

Comité ?', in: Van Laethem, W. and Vanderbroght, J. (eds.), Vast Comité I, Comité Permanent Contrôle des Services de Renseignements et de Sécutrité, *Inzicht in toezicht – Regards sur le contrôle*, Antwerp and Cambridge, Intersentia, pp. 253–267.

Wetzling, T., Stiftung neue Verantwortung (2017), 'Germany's intelligence reform: More surveillance, modest restraints and inefficient controls'.

Wills, A., Vermeulen, M., Born, H., Scheinin, M., Wiebusch, M. and Thornton, A., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, PE 453.207, Brussels, European Parliament Directorate-General for Internal Policies.

Working Group on Data Protection in Telecommunications (2017), *Towards International Principles or Instruments to Govern Intelligence Gathering*, Working Paper of the 61st Meeting, 24-25 April 2017, Washington D.C., USA.

Indexes

Case law index

Court of Justice of the European Union

Commission v. Austria, C-614/10, 16 October 2012 75

Commission v. Hungary, C-288/12, 8 April 2014 75

Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, 8 April 2014 75

European Commission v. Federal Republic of Germany [GC], C-518/07, 9 March 2010 75

European Commission v. Italian Republic, C-387/05, 15 December 2009 23

Maximillian Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015 ..... 30, 69

Maximillian Schrems v. Data Protection Commissioner, C-362/14, Advocate General's Opinion, 23 September 2015 69

N, C-601/15, 15 February 2016 54

Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Opinion of the Advocate General, 8 September 2016 35

Sahar Fahimian v. Bundesrepublik Deutschland, C-544/15, 4 April 2017 54

Tele2 Sverige AB v. Post- och telestyrelsen and *Secretary of State for the Home Department v. Tom Watson and Others*, Joined cases C-203/15 and C-698/15, 21 December 2016 ..... 22, 30, 34, 38, 97

Tsakouridis, C-145/09, 23 November 2010 54

ZZ v. Secretary of the State of Home Department, C-300/11, 4 June 2013 ..... 54, 131

European Court of Human Rights

10 Human Rights Organisations and Others v. the United Kingdom, No. 24960/15, communicated on 24 November 2015 ..... 20, 99

Al Nashiri v. Poland, No. 28761/11, 16 February 2015 106

Association confraternelle de la presse judiciaire v. France, No. 49526/15, communicated on 24 November 2015 ..... 20, 99

Big Brother Watch and Others v. the United Kingdom, No. 58170/03, communicated on 9 January 2014 20

Bucur v. Romania, No. 40238/02, 8 January 2013 ..... 71, 117, 118

Bureau of investigative journalism and Alice Ross v. the United Kingdom, No. 62322/14, communicated on 5 January 2015 20

Campbell and Fell v. the United Kingdom, No. 7819/77 and 7878/77, 28 June 1984 74

Del Rio Prada v. Spain [GC], No. 42750/09, 21 October 2013 38

Guja v. Moldova [GC], No. 14277/04, 12 February 2008 ..... 71, 70

Kafkaris v. Cyprus [GC], No. 21906/04, 12 February 2008 38

Kennedy v. UK, No. 26839/05, 18 May 2010 33

Klass and Others v. Germany, No. 5029/71, 6 September 1978 29

M.N. and Others v. San Marino, No. 28005/12, 7 July 2015 19

Nasr and Ghali v. Italy, No. 44883/09, 23 February 2016 129

Regner v. The Czech Republic 131

Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015 ..... 20, 33, 53, 34, 38, 73, 75, 78, 79, 93, 98, 111, 125

Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016 ..... 87, 93, 98, 104, 135

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, No. 39315/06, 22 November 2012 ..... 19, 99

Weber and Saravia v. Germany, No. 54934/00, 29 June 2006 ..... 19, 29

Youth initiative for human rights v. Serbia, No. 48135/06, 25 June 2013 69

National courts

France, Constitutional Court (*Conseil constitutionnel*), La Quadrature du Net and Others, Decision 2016-590 QPC, 21 October 2016 ..... 42, 47, 69, 131

France, Constitutional Court (*Conseil constitutionnel*), No. 2015-722 DC, 26 November 2015 47

Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 6 A 7.14, 15 June 2016 70

Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 7 C 18.14, 25 February 2016 124

Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999 124

Poland, Administrative Court in Warsaw (*Wojewódzki Sąd Administracyjny w Warszawie*), *Helsinki Foundation for Human Rights v. ABW*, II SA/Wa 710/14, 24 June 2014 120

Poland, Constitutional Court (*Trybunał Konstytucyjny*), K 23/11, 30 July 2014 42

The Netherlands, District Court The Hague (*Rechtbank Den Haag*), Case No. C/09/487229/KG ZA 15-540, 1 July 2015 99

United Kingdom, *Belhaj v. Straw* IPT/13/132-9H, 7 February 2014 133

United Kingdom, Investigatory Powers Tribunal, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al,* IPT/14/85/CH 14/120-126/CH, 12 February 2016 ..... 69, 133

United Kingdom, Investigatory Powers Tribunal, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al*, IPT/15/110/CH, [2016] UKIPTrib 15_110-CH, 17 October 2016 ..... 45, 69, 133

United Kingdom, Investigatory Powers Tribunal, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al*, IPT/15/110/CH, [2017] UKIPTrib 15_110-CH, 8 September 2017 ..... 44, 69, 133

United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014 and 6 February 2015 ..... 50, 51, 133

United Kingdom, *R (On the Application Of) v Investigatory Powers Tribunal*, Court of Appeal - Administrative Court, February 02, 2017, [2017] EWHC 114 133

Legal instruments index

EU legislation

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215 30

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L207, 1 August 2016 22

Council Directive 2004/114/EC of 13 December 2004 on the conditions of admission of third-country nationals for the purposes of studies, pupil exchange, unremunerated training or voluntary service, OJ 2004 L 375 54

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002 (Directive on privacy and electronic communications) 22, 54

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119 21

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016 22

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 23 November 1995, pp. 31-50. 21

European Parliament (2017), European Parliament Decision of 6 July 2017 on setting up a special committee on terrorism, its responsibilities, numerical strength and term of office, P8_TA-PROV(2017) 0307, Strasbourg, 6 July 2017 22

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119 21

CoE legislation

Council of Europe, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows, CETS No. 181, 8 November 2001, pp. 1-4 ..... 23, 80

Council of Europe, Amendments to the Convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999 23

Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28 January 1981, pp. 1-10. ..... 23, 80

Council of Europe, Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 23

National legislation

Austria, EU Police Cooperation Act *(Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), EU – Polizeikooperationsgesetz, EU-PolKG)*, BGBl. I Nr. 132/2009 51

Austria, International Police Cooperation Act *(Bundesgesetz über die internationale polizeiliche Kooperation, Polizeikooperationsgesetz - PolKG)*, BGBl. I Nr. 104/1997 51

Austria, Police State Protection Act *(Bundesgesetz mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert wird)*, BGBl. I Nr. 5/2016 133

Belgium, House of Representatives, Text adopted by the temporary 'Fight against Terrorism' Commission – Bill concerning complementary measures related to the fight against terrorism (*Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme*), 14 April 2016 76

Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique de 30 novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended 41, 42, 50, 61, 78, 94, 98, 100, 108, 119

Belgium, Organic Law on the control of police and intelligence services and the Coordination Unit for Threat Assessment (*Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*), 18 July 1991 ..... 77, 78

Belgium, *Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'evolution et la gestion de la lutte contre le radicalisme et la menace terrorist,* 11 April 2016 76

Bulgaria, Internal rules on the procedures and operation of the Committee for Oversight of the Security Services, the Deployment of Special Surveillance Techniques and the Access of Data under the Electronic Communications Act

Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*), 21 October 1997 51

Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, 30 June 2006 ..... 50, 70, 104

Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*) No. 75(I)/2016 40

Czech Republic, Act on Military Intelligence (*Zákon o Vojenském zpravodajství*), No. 289/2005, 16 June 2005 40

Czech Republic, Act on the Security Information Service (Zákon o bezpečnostní informační službě), No. 154/1994, 7 July 1994 40

Denmark, Act No. 604 on the Danish Security and Intelligence Service as amended by Act. No. 1624 of 26 December 2013 (*Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET), som ændret ved lov nr. 1624 af 26. december 2013*), 12 June 2013 ..... 103, 132

Denmark, Administration of Justice Act, Consolidated Act No. 1255 of 16 November 2015 with amendments (*Retsplejeloven, lovbekendtgørelse nr. 1255 af 16. november 2015 med senere ændringer*), 16 November 2015 126

Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*) 83, 118

France, Administrative Justice Code (Code de justice administrative)....130

France, Bill reinforcing internal security and the fight against terrorism (*Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*), 22 June 2017 42

France, Decree No. 2014–833 on the Inspectorate of intelligence services (*Décret n° 2014–833 relatif à l'inspection des services de renseignement*), 24 July 2014....61

France, Defence Code (*Code de la Défense*) 27, 60, 61

France, Interior Security Code (*Code de la sécurité intérieure*)....28, 34, 45, 46, 47, 71, 75, 77, 78, 79, 84, 96, 98, 99, 105, 130, 132

France, Law No. 2015–1556 on international surveillance (*Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*), 30 November 2015.... 47

France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies (*Ordonnance n° 58-1100 relative au fonctionnement des assemblées parlementaires*), 17 November 1958, as amended....77, 105, 106

Germany, Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (Article 10, G 10 Act) (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10, Gesetz G 10)*), 26 June 2001, as amended 43, 44, 99, 100, 119, 126, 127

Germany, Act to Regulate Access to Federal Information (*Informationsfreiheitsgesetz*, IFG) 124

Germany, Basic Law (*Grundgezetz*) 43

Germany, Federal Budget Order (*Bundeshaushaltsordnung*), 19 August 1969, as amended.... 65

Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), 14 January 2003, as amended.... 82

Germany, Federal Intelligence Act (*Gesetz über den Bundesnachrichtendienst*), 20 December 1990, as amended....34

Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009.... 65, 71

Hungary, Act LIV of 2002 on the international cooperation of law enforcement bodies (*2002. évi LIV. törvény a bűnöldöző szervek nemzetközi együttműködéséről)*, 1 April 2003....51

Hungary, Act CXXV of 1995 on the National Security Services (*A nemzetbiztonsági szolgálatokról szóló 1995. Évi CXXV. törvény*), 28 December 1995, as amended.... 104, 118, 124

Hungary, Governmental Decree No. 185/2016 on the cooperation between the service providers providing encrypted communications and the authorities entitled to conduct secret surveillance operations, 185/2016 (VII. 13.), 17 July 2016. 118

Italy, Code of criminal procedure (*Codice di procedura penale*), 24 October 1989....96

Italy, Data Protection Code 80, 117

Italy, Implementing provisions of the Code of Criminal Procedure (*Disposizioni di attuazione del codice di procedura penale*)....41

Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on State secrets (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*), 3 August 2007 41

Italy, Legislative Decree No. 144 of 27 July 2005....41

Italy, Legislative Decree No. 7 of 18 February 2015....42

Latvia, Investigatory Operations Law (*Operatīvās darbības likums*), 16 December 1993 126

Latvia, Law on Constitution Protection Bureau (*Satversmes aizsardzības biroja likums*), 5 May 1994 50

Latvia, Law on the State Secrets *(Par valsts noslēpumu)*, 17 October 1997 ..... 50, 51

Luxembourg, Act of 15 June 2004 on the organisation of the State Intelligence Service (*Loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat*), 15 June 2004, as amended 50

Luxembourg, Law of 5 July 2016 1. reorganising the State Intelligence Service; 2. modifying the Code of Criminal Procedure, the Law of 15 June 2004 regarding the classification of documents and security clearances and the Law of 25 March 2015 setting the regime for the compensation and the conditions for promotion of the State civil servants (*Loi du 5 juillet 2016 1. portant réorganisation du Service de renseignement de l'État; 2. modifiant le Code d'instruction criminelle, la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, et- la loi du 25 mars 2015 fixant le régime des traitements et les conditions d'avancement des fonctionnaires de l'État*) 54, 103

Malta, Security Service Act, Chapter 391 of the Laws of Malta, 26 July 1996, as amended on 6 September 1996 ..... 50, 66

Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002 42

Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016 130

Portugal, Decree 426/XII approving and regulating the special procedure of access to telecommunication data and Internet by the information officials of SIS and SIED and proceeds to the amendment to the Law 62/2013 26 August, (Aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de Agosto), 19 July 2017 ..... 40, 42, 96

Portugal, Law 50/2014, 1st amendment to law 9/2007 of 19 February that lays down the Organic law of the Secretary-General of the Intelligence Services of the Portuguese Republic, the Strategic Defence Intelligence Service and the Security Intelligence Service, 13 August 2014 50

Romania, Decision No. 30/1993 of the Romanian Parliament concerning the organization and functioning of The Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the activity of the Romanian Intelligence Service (*Hotararea Nr. 30/1993 a Parlamentului Romaniei privind organizarea şi funcţionarea Comisiei comune permanente a Camerei Deputaţilor şi Senatului pentru exercitarea controlului parlamentar asupra activităţii Serviciului Roman de Informaţii*), 23 June 1993 117

Slovenia, Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji,* ZSOVA), 7 April 1999 101

Slovakia, Act No. 404/2015 Coll. amending and supplementing Act N. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*), 19 December 2015 83

Spain, Law 11/2002 of 6 May, National Intelligence Centre Act 105

Sweden, Act on the Defence Intelligence Court (*Lag (2009:966) om Försvarsunderrättelsedomstol*), 15 October 2009 96

Sweden, Regulation on Defence intelligence service (Förordning [2000:131] om försvarsunderrättelseverksamhet), 30 Mars 2000 ..... 102, 106

Sweden, Regulation 2009:968 with instructions for the Defence Intelligence Court (*Förordning (2009:968) med instruktion för Försvarsunderrättelsedomstolen)*, 15 October 2009 96

Sweden, Signals Intelligence Act (2008:717) (*Lag om signalspaning i försvarsunderrättelseverksamhet (2008:717)*), 10 July 2008 ..... 79, 100, 126

The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*) 47, 50, 61, 67, 71, 79, 99, 102, 116, 132

United Kingdom, Investigatory Powers Act 2016 ..... 34, 42, 43, 44, 45, 46, 47, 75, 79, 84, 87, 94, 97, 98, 99, 103, 125, 133, 134

United Kingdom, Regulation of Investigatory Powers Act 2000, 1 August 2000 133

United Kingdom, Justice and Security Act 2013, 25 April 2013 ..... 77, 88, 105, 106

United Kingdom, Data Protection Act 1998 ..... 81, 127

Annex 1: Data collection and coverage

Legal update in EU 28

The legal analysis draws on data provided by the agency's multidisciplinary research network, Franet, which were collected through desk research in all 28 EU Member States, based on a questionnaire submitted to the network.[568] The main data collection took place between August 2014 and September 2016. Later on, the selected Member States provided FRA with a series of monthly overviews. Franet contractors provided their latest deliverables in June 2017.

Additional information was gathered through desk research and exchanges with key partners, including a number of FRA's national liaison officers and individual experts in various Member States. These include Austria, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Sweden and the United Kingdom. The opinions and conclusions in this report do not necessarily represent the views of the organisations or individuals who helped develop the report.

The FRA findings also draw on existing reports and publications aimed at supporting national legislators in setting up legal frameworks for the intelligence services and their democratic oversight.[569] The findings refer in particular to the compilation of good practices issued by Scheinin as Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[570] Additional promising practices discussed during fieldwork are published in this report.

The legal comparative analysis follows the structure the ECtHR suggests for surveillance cases. So far, most of the cases brought before the Strasbourg judges have focused on the legality of interferences with the right to private life – in other words, whether the secret surveillance was "in accordance with the law". Following the ECtHR jurisprudence, this report presents the safeguards that the law should put in place to be considered compatible with the ECHR.[571] These relate to the approval mechanism of the surveillance measure and the oversight mechanism controlling its implementation, as well as to available remedies.

568 See FRA (2014b), FRA (2015b) and FRA (2017). See all Franet Guidelines online.
569 See, for example, Venice Commission (2007); Council of Europe (2016b); Born, H. and Wills, A. (eds.) (2012); Hans Born, H., Leigh I. and Wills, A. (2015); Anderson, A. (2015).
570 UN, Human Rights Council, Scheinin, M. (2010).
571 See Cameron, I. (2013), p. 164.

Social fieldwork methodology

Research Member States

The social fieldwork is based on qualitative research in the following seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom.

The selection of the Member States was determined by a set of interrelated factors. In the 2015 report *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, FRA presented the findings of the mapping of the legal frameworks in the EU Member States that regulate surveillance by intelligence services and their oversight. The report presented an overview of the institutions and bodies that operate in the field, discussing their different types, mandates and powers. On the basis of the findings of this institutional approach, the Member State selection for the fieldwork stage aimed to capture the variety of actors involved in the field of surveillance by the intelligence services and its oversight and to cover the whole range of different powers, mandates and national constellations of main actors in certain Member States. In line with this main ground, five out of the seven Member States have detailed legislation on general surveillance of communications. The size of the country played a role in this context in terms of institutions available, their number and staff working in the institutions, their openness and availability to discuss the issues.

Objectives

The objective of the field research was to provide FRA with country-specific information on the practical implementation of the national legal frameworks governing the intelligence services with respect to compliance with fundamental rights. The research aimed to study how the oversight of intelligence services was exercised in practice, to analyse the specificities of the day-to-day work of the oversight bodies and their effectiveness in the selected Member States. It thus has both exploratory and explanatory aspects. The research did not cover surveillance techniques or the content of the data collected.

The analysis of the data collected aims to identify cross-cutting and overarching issues that can be extrapolated to other EU Member States and discussed within their national context. The data collected and the findings are not used to provide country-specific reports or to

'check' the issues identified by the respondents with regard to their specific national contexts.

The methodology applied to the social research aims to identify prevailing understandings of and opinions about the legal framework that currently regulates oversight of intelligence gathering – a task that is shared by different actors in the field, such as different types of oversight bodies, data protection authorities, ombuds institutions, national human rights institutions, civil society organisations, practicing lawyers, academics and media representatives. The data collected provide insights into, and broader understanding of, the challenges of upholding fundamental rights in the area of oversight. It also provides an assessment of applied oversight practices and remedies from the perspective of different actors involved.

Data collection

The main data collection was carried out from December 2015 to July 2016, with a few interviews conducted in the late autumn of 2016. The final data set consists of 72 interviews in the selected EU Member States (see Table 1).

Table 1: Interviews by Member State

Member State	Number of interviews
Belgium	8
Germany	8
France	17
Italy	5
The Netherlands	8
Sweden	14
The United Kingdom	12
Total	**72**

Source: FRA, 2017

Table 2 presents a breakdown of the interviews by the institutions and bodies. The interviews with the representatives of the oversight bodies comprise the biggest share in the dataset (nearly half of the interviews). Both the type of institution approached and number of the interviews per Member State depended on the national context.

In the context of this research, the interviewees were addressed as individuals with special knowledge on intelligence, surveillance, oversight and related matters. The focus was on collecting the experts' process-related knowledge on gathering intelligence in accordance with existing fundamental rights standards.

Table 2: Interviews, by institution represented

Institution/organisation	Number of interviews
Expert body	16
Parliamentary committee	8
Executive control	4
Judiciary	6
Data protection authority	11
Ombuds institution, national human rights institution	5
Civil society organisation (including media representatives)	12
Academia	5
Lawyer	5
Total	**72**

Source: FRA, 2017

All potential interviewees were contacted with official FRA letters, as representatives of a specific public authority, body or organisation. In the communication, strict anonymity and confidentiality of the interviews were agreed on. Where quotes or statements from the interviews are used in publications, FRA committed to using no reference or using a generalised reference to avoid enabling personal identification.

FRA expressed its interest in interviewing separately the head of the institution and the staff (or member of the body) with relevant responsibilities that cover the areas of the research interest. In the final outcome, the respondents are distributed equally by their positions in the institutions, i.e., the final sample includes interviews with the heads (chairs, directors, presidents) of the authorities and the responsible staff in equal shares (22 interviews per each category). This breakdown was not applied for lawyers, academia and civil society organisations, where the same person might represent both positions. During most interviews, two respondents participated (in a few cases, more than two respondents were present, and the highest number of interviewees per interview was six). With regard to gender, in more than half of the interviews (44 out of 72), only men were present. In 15 cases, only women were present as interviewees. In the remaining 13 cases, both men and women were present during the interviews.

In the framework of the research, civil society organisations that have expertise in the area of data protection and surveillance specifically were approached. Such organisations were available in all the researched Member States except for Italy. In selecting the organisations, their experience on the international level was taken into account. The scale and scope of the activities vary among the civil society organisations and

across countries. Some have been operating for several decades, and some for several years. With regard to their background, mainly lawyers are active or work in the civil society organisations. Their legal expertise in some cases is supported by technical experts, or certain knowledge is developed through the involvement in the activity field. Many of these organisations have been involved in litigation on a variety of issues related to data protection or privacy, including cases on alleged unlawful data processing by intelligence agencies.

All the interviews were carried out by senior FRA research staff members, who travelled to the selected Member States. Most interviews were conducted face to face, with a few undertaken by telephone to suit the needs of the interviewee(s) and the researchers (ie, to find a time slot in the agendas and to reduce travelling).

On average, interviews lasted about one-and-a-half hours. Most of the interviewees kindly agreed to the interviews being audio recorded. When recording was not possible, notes were taken during the interview. For this reason, two FRA representatives were present during the interviews.

Most of the interviews took place in the respective national languages of the countries. FRA staff translated the anonymised transcripts and notes of the interviews from Italian and Swedish to English. The *Translation Centre for the Bodies of the European Union* translated the anonymised transcripts and notes of the interviews from French and German to English. The information retained its classified status, with a security grading 'confidential' assigned.

Interview content

The semi-structured interviews were designed to obtain detailed accounts of the following issues:

- assessment of the institutional setting of the authority, its mandate, power, and legal framework and its latest developments;
- implementation of oversight in practice, scope and content of oversight processes, including measures to ensure that intelligence gathering is compliant with fundamental rights;
- assessment of remedial mechanisms for individuals in case of fundamental rights violations;
- needs for reform, possible improvements in daily activities to ensure the fundamental rights compliance of the intelligence services and its oversight.

Interview guidelines followed the same structure of mainly open questions that were used to set an agenda, with the freedom to change the order of questions depending on the answers. The pre-defined structure contributed to capturing the perspectives and opinions of different actors involved about the same issues, with some adjustments in relation to the specificity of the experiences.

The sequence of the questions and the topics covered during each interview differed across different institutions, taking into account their relevance (including recent developments in the Member State, the institution's powers and competences, etc.). Therefore, there are differences in the nature and volume of information obtained from different respondents, which might lead to varying levels of consistency in the conclusions or findings on specific themes due to the volume of information. Overview of oversight operational practices, which was discussed only during 16 interviews, is an example. Although the discussions provided valuable in-depth information on, and explanations and understanding of, the procedures carried out by the oversight bodies, the analysis, generalisation and presentation of the data are limited due to the specificity of each institution, Member State context, and confidentiality issues. They mainly provide background information. For most cases, the main focus was on identifying trends in the data, i.e. looking for and combining statements and opinions that were similar or identical across different research participants. Table 3 provides a list of themes presented in the report and the number of interviews that covered them.

Data analysis

The analysis of the data collected through the semi-structured interviews was carried out by using the qualitative data analysis software 'NVivo 10'. The data analysis was constructed around the main topics and questions asked, following the interview guideline, and the key findings from the legal analysis of the 28 EU Member States. No interview or response to a specific question was considered on its own. Constant comparison of the data that went through automated and manual coding (categorising data on the basis of similarity, repetitiveness of the observations, concepts, topics and issues raised) enabled the researchers to identify emerging themes and opinions. The findings from the fieldwork contribute to understanding different aspects of intelligence collection and its oversight; it does not aim to validate the legal analysis results.

In the data analysis process, an inductive approach was mainly applied, which aimed to generate new information from the data (raw interview text data), explore the research subject matter from a different/new perspective (along the legal analysis), and establish (develop) understanding of the underlying opinions and views that are evident in the raw data collected

Table 3: Thematic areas presented in the report, by number of interviews

Theme	Number of interviews during which issue was discussed
Legal framework	67
Clarity of legal framework	53
Effective oversight	35
Mandate of the body	33
Independence of the body	16
Transparency of the oversight activities	29
Main challenges to upholding fundamental rights	38
Definition of national security	15
Resources and technical capacities	64
Oversight institutional framework	60
Cooperation with other institutions	46
Remedies	54
Duty of notification, right to access information	17
Whistle-blowers	14

Source: FRA, 2017

for this report. However, this approach does not make it possible to explain the causality of the issues and provide grounded explanations; instead, it provides a 'straightforward' approach for deriving findings in the context of interview guiding questions (namely, it condenses extensive and varied raw interview data through recurrent and most relevant themes or categories into a brief, summary format). Also, this type of qualitative research is based on the interviewees' opinions and judgments rather than factual results.

While looking for relationships and patterns in the data, the type of institution or organisation that the respondents represented was used as the main breakdown dimension. Other possible characteristics, such as country, position within the institution, or any other specific information, was considered with a particular focus only during the analysis process but disregarded while finalising the results and presenting the findings.

Presentation of the findings

The findings from the fieldwork complement the conclusions of the comparative national legal analysis and follow up on specific issues identified during the data collection or in earlier FRA reports. The analysis of the interview data is influenced by the content of, and language used during, the interviews. Therefore, the terminology used in the discussion of the findings predominantly originates from the respondents and is not necessarily closely connected to the legislative regulation (ie, does not follow the text of the regulation). It is worth mentioning that, during the interviews, respondents attempted to explain the complexity of their day-to-day practices and procedures in an understandable way.

The quotes included in the text of the report have been selected for being particularly illustrative or representative of the research findings. They primarily serve illustrative purposes. Only translated quotes are presented. They have been slightly edited, but only to improve understanding and readability. All the interviews were carried out in confidence; references to the interviewees are therefore kept general. In most cases, the category specified next to the quote refers to the body represented, e.g. expert body, parliamentary committee, data protection authority or civil society organisation, etc. Where interviewed individual experts hold an academic position or are practicing lawyers, broader categories are applied – such as 'academia' or 'lawyer'. The presentation of the findings does not aim to single out a specific country, so the countries are mentioned in the text where relevant, but are not specified alongside the quotes. Before publication of the report, all respondents consented to being cited in the way the citations and references are presented in the report.

Annex 2: Overview of intelligence services in the 28 EU Member States

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
AT	Federal Agency for State Protection and Counter Terrorism/*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (BVT) (part of the police)	http://www.bmi.gv.at/cms/bmi_verfassungsschutz/meldestelle/	N.A.	Annual report 2016 (87 pages)
	Military Intelligence Service/*Heeresnachrichtenamt* (HNA)	http://www.bundesheer.at/organisation/beitraege/n_dienste/index.shtml	N.A.	-
	Military Defence Agency/ *Heeresabwehramt* (HAA)	-	N.A.	-
BE	State Security/ *Staatsveiligheid /Sûreté de l'Etat* (SV/SE)	-	N.A.	-
	General Information and Security Service/ Algemene Dienst Inlichting en Veiligheid / Service Général du Renseignement et de la Sécurité (ADIV/SGRS)	-	N.A.	-
BG	State Intelligence Agency/*Nationalna Razuznavatelna Služba* (NRS)	www.nrs.bg	N.A.	Annual Report 2016 (18 pages)
	State Agency for National Security / Държавна Агенция "Национална сигурност (SANS)	http://www.dans.bg/index.php	N.A.	Access to information Report 2016 (1 page)
	State agency "Technical operations" / Държавна агенция „Технически операции (SATO)	https://www.dato.bg/	N.A.	Access to information Report 2016 (1 page)
	Military Information Service/*Sluzhba Voenna Informatsia*	http://dis.mod.bg/	N.A.	-
CY	Cypriot Intelligence Service/Κυπριακή Υπηρεσία Πληροφοριών (ΚΥΠ)	-	N.A.	-
CZ	Security Information Service/*Bezpečnostní informační služba* (BIS)	https://www.bis.cz/	N.A.	Annual Report 2015 (26 pages)
	Office for Foreign Relations and Information/ Úřad pro Zahraniční Styky a Informace (UZSI)	www.uzsi.cz	N.A.	-
	Military Intelligence/*Vojenské Zpravodajství*	http://www.vzcr.cz/	N.A.	Annual Activities Report 2015 (19 pages)
DE	Federal Office for the protection of the Constitution/ *Bundesamt für Verfassungsschutz* (BfV)	https://www.verfassungsschutz.de/en/index-en.html	2,813	Annual Report 2016 (38 pages)
	Federal Intelligence Service/*Bundesnachrichtendienst* (BND)	www.bnd.bund.de	circa 6,500	Not publicly available
	Military Counter-Intelligence Service/ *Militärischer Abschirmdienst* (MAD)	http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/start/weitdstst/mad	1,086	-
	State Office for the Protection of the Constitution of *Baden-Württemberg*/ Landesamt für Verfassungsschutz Baden-Württemberg	http://www.verfassungsschutz-bw.de/,Lde/Startseite	N.A.	Annual Report 2016 (181 pages)
	Bavarian Office for Protection of the Constitution/ *Bayerische Landesamt für Verfassungsschutz*	http://www.verfassungsschutz.bayern.de/	N.A.	Report for first half of 2017 (47 pages)
	Berlin Senate Administration for Home Affairs, Department of Protection of Constitution/*Senatsverwaltung für Inneres, Abteilung Verfassungsschutz Berlin*	https://www.berlin.de/sen/inneres/verfassungsschutz/	N.A.	Annual Report 2016 (221 pages)
	Brandenburg Ministry of Interior and Municipalities, Department of Protection of Constitution/*Ministerium des Innern und für Kommunales, Abteilung Verfassungsschutz Bradenburg*	http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/lbm1.c.336855.de	N.A.	Annual Report 2015 (344 pages)

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
DE	Bremen State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Bremen*	http://www.verfassungsschutz.bremen.de/	N.A.	Annual Report 2016 (97 pages)
	State Office for the Protection of Constitution of the Free and Hanseatic City of Hamburg/*Landesamt für Verfassungsschutz der Freien und Hansestadt Hamburg*	-	N.A.	Annual Report 2015 (244 pages)
	Hessen State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Hessen*	https://lfv.hessen.de/	N.A.	Annual Report 2015 (244 pages)
	Lower Saxony Ministry of Interior, Sport and Integration, Department 5/*Ministerium für Inneres, Sport und Integration, Abteilung 5 Niedersachsen*	https://www.verfassungsschutz.niedersachsen.de/startseite/	N.A.	Annual Report 2016 (401 pages)
	Mecklenburg-Vorpommern Ministry of Interior, Department II 5/*Mecklenburg-Vorpommern Innenministerium, Abteilung II 5*	http://www.verfassungsschutz-mv.de/	N.A.	Annual Report 2015 (194 pages)
	North Rhine-Westphalia Ministry of Interior and Municipalities, Department for the Protection of Constitution/*Nordrhein-Westfalen Ministerium für Inneres und Kommunales, Abteilung Verfassungsschutz*	http://www.mik.nrw.de/verfassungsschutz/aktuelles.html	N.A.	Annual Report 2015 (263 pages)
	Rhineland-Palatinate Ministry of Interior and Sport, Department for the Protection of Constitution/*Rheinland-Pfalz Ministerium des Innern und für Sport, Abteilung Verfassungsschutz*	https://mdi.rlp.de/de/unsere-themen/sicherheit/verfassungsschutz	N.A.	Annual Report 2016 (119 pages)
	Saarland State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Saarland*	http://www.saarland.de/verfassungsschutz.htm	N.A.	Annual Report 2016 (90 pages)
	Saxony State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Sachsen*	http://www.verfassungsschutz.sachsen.de/index.html	N.A.	Annual report 2016 (420 pages)
	Saxony-Anhalt Ministry of Interior and Sport, Department for the Protection of Constitution/*Sachsen-Anhalt Ministerium für Inneres und Sport, Abteilung Verfassungsschutz*	https://mi.sachsen-anhalt.de/verfassungsschutz/	N.A.	Annual Report 2016 (224 pages)
	Schleswig-Holstein Ministry of Interior, Department for the Protection of Constitution/*Schleswig-Holstein Innenministerium, Abteilung Verfassungsschutz*	http://www.schleswig-holstein.de/DE/Themen/V/verfassungsschutz.html	N.A.	Annual Report 2016 (172 pages)
	Thüringen Ministry of Interior and Municipalities, Office for the Protection of Constitution /*Thüringen Ministerium für Inneres und Kommunales, Amt für Verfassungsschutz*	http://www.thueringen.de/th3/verfassungsschutz/	N.A.	Report 2014/15 (232 pages)
DK	Danish Defence Intelligence Service/*Forsvarets Efterretningstjenst* (FE)	www.fe-ddis.dk	N.A.	Report 2015/16 (30 pages)
	Danish Security and Intelligence Service/*Politiets Efterretningstjeneste* (PET) (part of the police)	https://pet.dk/	N.A.	Annual Report 2015 (28 pages)
EE	Information Board/*Teabeamet* (TA)	https://www.teabeamet.ee/	N.A.	Estonia's International Security Environment 2017 (44 pages)
	Estonian Internal Security Service/*Kaitsepolitseiamet* (KAPO)	https://www.kapo.ee/	N.A.	Yearbook 2016 (45 pages)
	Intelligence Battalion of the Estonian Defence Forces /*Kaitseväe peastaabi luureosakond*	-	N.A.	-
EL	National Intelligence Service/Εθνική Υπηρεσία Πληροφοριών (EYP)	www.nis.gr	N.A.	-
	Directorate of Military Intelligence of the National Defence General Staff/Διεύθυνση Στρατιωτικών Πληροφοριών του Γενικού Επιτελείου Εθνικής Άμυνας	-	N.A.	-

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
ES	National Intelligence Centre/*Centro Nacional de Inteligencia* (CNI)	https://www.cni.es/	N.A.	-
	Intelligence Centre of the Armed Forces/ *Centro de Inteligencia de las Fuerzas Armadas* (CIFAS)	http://www.emad.mde.es/CIFAS/	N.A.	-
FI	Finnish Defence Intelligence Agency/ *Tiedustelulaitos* (FDIA)	http://puolustusvoimat.fi/en/about-us/finnish-defence-intelligence-agency	N.A.	-
	Finnish Security Intelligence Service/ *Suojelupoliisi/Skyddspolisen* (SUPO)	http://www.supo.fi/	N.A.	Yearbook 2016 (28 pages)
FR	Directorate General of External Security/ *Direction Générale de la Sécurité Exterieure* (DGSE)	http://www.defense.gouv.fr/dgse	5,376*	-
	Directorate of Defence Intelligence and Security/*Direction du renseignement et de la sécurité de la défense* (DRSD)	http://www.defense.gouv.fr/drsd	1,190*	-
	Directorate of Military Intelligence/ *Direction du renseignement militaire* (DRM)	http://www.defense.gouv.fr/ema/directions-et-services/la-direction-du-renseignement-militaire/la-drm	1,715*	-
	Directorate General of Interior Security/ *Direction générale de la sécurité intérieure* (DGSI)	http://www.interieur.gouv.fr/Le-ministere/DGSI	3,200**	-
	National Directorate of customs intelligence and investigations/*Direction nationale du renseignement et des enquêtes douanières (DNRED)*	http://www.douane.gouv.fr/	760*	Results 2016 (50 pages)
	Service du traitement du renseignement et action contre les circuits financiers clandestins (Tracfin)	http://www.economie.gouv.fr/tracfin/accueil-tracfin	132*	Annual Activities Report 2016 (87 pages)
HR	Security Intelligence Agency/*Sigurnosna-Obavjestanja Agencija* (SOA)	https://www.soa.hr/	N.A.	Public Report 2016 (49 pages)
	Military /*Vojna Sigurnosna-Obavjestanja Agencija* (VSOA)	-	N.A.	-
HU	Information Office/ *Informacios Hivatal* (MKIH)	http://www.mkih.hu/	N.A.	-
	Constitution Protection Office/ *Alkotmányvédelmi Hivatal*	http://www.ah.gov.hu/	N.A.	-
	Special Service for National Security/ *Nemzetbiztonsági Szakszolgálat* (NBSZ)	http://nbsz.gov.hu/	N.A.	-
	Counter Terrorism Centre/ *Terrorelhárítási Központ* (TEK) (service belonging to the police)	http://tek.gov.hu/	N.A.	-
	Counter-Terrorism Information and Criminal Analysis Centre/ *Terrorelhárítási Információs és Bűnügyi Elemző Központ* (TIBEK) (starting from 17 July 2016)	http://tibek.gov.hu/	N.A.	-
	Military National Security Service/*Katonai Nemzetbiztonsági Szolgála* (KNBSZ)	http://knbsz.gov.hu/hu/index.html	N.A.	National Security Review 2016 (127 pages)
IE	Directorate of Intelligence (G2)	-	N.A.	-
	Garda Síochána National Surveillance Unit (NSU) (belonging to the police)	-	N.A.	-
IT	Information and Internal Security Agency/ *Agenzia informazioni e sicurezza interna* (AISI)	http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html	N.A.	Common Activity report for AISI and AISE 2016 (128 pages)
	Information and External Security Agency/ *Agenzia informazioni e sicurezza esterna* (AISE)	http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html	N.A.	
	Department of information and security/ *Reparto informazioni e sicurezza* (RIS)	https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html	N.A.	-

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
LT	State Security Department/ *Valstybes Saugumo Departamentas* (VSD)	http://www.vsd.lt/	N.A.	Annual Activity Report 2016 (15 pages)
	Second Investigation Department under the Ministry of National Defence/*Antraisi Departamentas Prie Krasto Apsaugos Ministerijos*	https://kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html	N.A.	Annual Activity Report 2016 (9 pages)
LU	State Intelligence Service/*Service de Renseignements de l'Etat* (SREL)	http://www.gouvernement.lu/971456/service-de-renseignement-de-l-etat	N.A.	-
LV	Constitutional Protection Bureau/ *Satversmes Aizsardzibas Birojs* (SAB)	http://www.sab.gov.lv/	N.A.	-
	Defence Intelligence and Security Service/ *Militārās izlūkošanas un drošības dienests* (MIDD)	http://www.midd.gov.lv/Par_mums.aspx	N.A.	-
	Security Police/ *Drošības policija*	http://www.dp.gov.lv/lv/	N.A.	Annual Report 2016 (36 pages)
MT	Security Service / *Servizz tas-Sigurtà*	-	N.A.	-
NL	General Intelligence and Security Service/ *Algemene Inlichtingen- en Veiligheidsdienst* (AIVD)	https://www.aivd.nl/	circa 1,500	Annual report 2016 (19 pages)
	Military Intelligence and Security Service/ *Militaire Inlichtingen- en Veiligheidsdienst* (MIVD)	https://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd	795	Annual Report 2016 (50 pages)
PL	Foreign Intelligence Authority/*Agencja Wywiadu* (AW)	http://www.aw.gov.pl/	N.A.	-
	Military Counter-intelligence Service/ *Sluzba Wywiadu Woyskowego* (SWW)	http://www.sww.wp.mil.pl/pl/index.html	N.A.	-
	Internal Security Agency/*Agencja Bezpieczeństwa Wewnętrznego* (ABW)	https://www.abw.gov.pl/	N.A.	Internal Security Review 2017 (compliltion of articles)
	Central Anti–Corruption Bureau/*Centralne Biuro Antykorupcyjne* (CBA)	https://cba.gov.pl/	N.A.	-
PT	Strategic Intelligence and Defence Service/ *Serviço de Informações Estratégicas de Defesa* (SIED)	https://www.sied.pt/	N.A.	-
	Service of Security Intelligence/ *Serviço de Informações de Segurança* (SIS)	https://www.sis.pt/quem-somos/o-sis	N.A.	-
	Information System of the Portuguese Republic/Sistema *de Informações da República Portuguesa* (SIRP)	https://www.sirp.pt/	N.A.	'Year in Review' 2015 (38 pages)
RO	External Intelligence Service/*Serviciul de Informatii Externe* (SIE)	https://www.sie.ro/	N.A.	-
	Defence General Directorate for Information/*Direcția Generală de Informații a Apărării* (DGIA)	http://www.mapn.ro/structuri/dgia/	N.A.	-
	Romanian Intelligence Service/ *Serviciul Roman de Informatii* (SRI)	https://www.sri.ro/	N.A.	Annual Activity Report 2016 (2 pages)
	Department for Information and Internal Protection/ *Direcția Generală de Informații și Protecție Internă* (DGIPI)	http://dgpi.ro/	N.A.	Work started in June 2017
SE	National Defence Radio Establishment/ *Försvarets Radioanstalt* (FRA)	http://www.fra.se/	700	Annual Report 2016 (28 pages)
	Military Intelligence and Security Agency/ *Militära underrättelse- och säkerhetstjänsten*	http://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/	886	Annual Report 2015 (17 pages)
	Security Service/ Säkerhetspolisen, (SÄPO)	http://www.sakerhetspolisen.se/	1,100	Annual Report 2016 (71 pages)

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
SI	Slovene Intelligence and Security Agency/ *Slovenska obveščevalno-varnostna agencija* (SOVA)	http://www.sova.gov.si/	N.A.	-
	Intelligence and Security Service of the Ministry of Defence/ *Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo* (OVS MORS)	-	N.A.	-
SK	National Security Authority/*Národný bezpečnostný úrad* (NBÚ)	http://www.nbusr.sk/	N.A.	Activity report 2016 (23 pages)
	Slovak Information Service/*Slovenská informačná služba* (SIS)	http://www.sis.gov.sk/	N.A.	Activity report 2016 (18 pages)
	Millitary Intelligence/*Vojenské spravodajstvo* (VS)	http://vs.mosr.sk/	N.A.	Activity report 2016 (9 pages)
UK	Security Service or MI5	https://www.mi5.gov.uk/	4,037	-
	Secret Intelligence Service (SIS) or MI6	https://www.sis.gov.uk/	2,479	-
	Government Communications Headquarters (GCHQ)	https://www.gchq.gov.uk/	5,564	-
	Defence Intelligence (DI)	https://www.gov.uk/government/groups/defence-intelligence	3,697	-

Notes:

N.A. = not available.

– = not applicable (either no website or no public annual report).

** France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 29.*

*** France, website of Académie du renseignement.*

Source: FRA, 2017

Annex 3: Key features of expert oversight bodies' (excl. DPAs) annual reports of selected EU Member States

	Austria* *RSB*	Belgium *Standing Committee I*	Bulgaria *NBKSRS*	Croatia** *Council for Civilian Oversight*	Denmark*** *Defence TET*
Year of publication/reporting period	2016/2015	2016/2015	2017/2016	2011/2010	2017/2016
Length (in pages)	13	131	27	6	44
Available in English and/ or partially in English	✓	✓	-	-	✓
Publication of two versions: one public and one classified	✓	✓	-	✓	-
Description of existing/ new legislation	✓	✓	✓	-	✓
Expert body mandate and powers	✓	✓	-	✓	✓
Surveillance measures	✓	✓	✓	-	✓
Statistics and reasons on authorisations granted/refused	✓	✓	✓	N.A.	
Statistics on *ex post* controls	✓	✓	✓	-	✓
Statistics on investigations	N.A.	✓	✓	✓	
Statistics on breaches of safeguards	-	✓	✓	-	✓
Statistics on surveilled persons	-	-	✓	-	
Oversight methods	✓	✓		✓	✓
International cooperation/data transfer to foreign services	-	✓	-	-	
Remedies and statistics on complaints-handling	-	✓	✓	✓	✓
Internal functioning	-	✓	✓	✓	✓
Inter-institutional dialogue	-	✓	✓	✓	✓
International cooperation among expert bodies	-	✓	✓	-	
Recommendations	-	✓	✓	-	✓
Implementation of past recommendations	-	✓	-	-	✓
Separate publication on specific investigations	-	✓	-	-	

Notes:

N.A. = *not applicable.*

– = *Not done or not covered in the report.*

* *The report of the Legal Protection Commissioner (Rechtsschutzbeauftragter) is confidential, but a summary is published every year in a specialised journal on police studies. See Burgstaller, M. and Kubarth, L. (2016).*

** *The report of the Council for Civilian of Oversight (Vijeće za građanski nadzor sigurnosno-obavještajnih agencija) is submitted to the President of Parliament and is confidential, but a summary is published occasionally.*

*** *Defence TET (Forsvarets Efterretningstjeneste (FE))'s report is available on TET's website.*

**** *The G 10 Commission does not issue any independent reports. Its annual report is prepared by the Parliament Control Panel. See Germany, Federal Parliament (Deutscher Bundestag) (2017).*

Source: *FRA, 2017*

France *CNCTR*	Germany**** *G10*	Greece *ADAE*	Luxembourg *Autorité de contrôle*	Sweden *Siun*	The Netherlands *CTIVD*	United Kingdom *IOCCO / IScomm*
2016/10.2015 to 10.2016	2017/2015	2016/2015	2016/2014-15	2017/2016	2016/1.4 to 31.12.2015	2016/1.9 to 31.12.2015
204	10	79	18	33	40	99 / 71
✓	-	✓	-	-	✓	N.A.
-	-	-	-	-	-	✓
✓	-	N.A.	✓	✓	✓	✓
✓	✓	✓	✓	✓	-	✓
✓	-	-	✓	✓	-	✓
✓	-	N.A.	N.A.	✓	-	✓
✓	N.A.	✓	✓	✓	-	✓
-	N.A.	✓	-	✓	✓	-
-	N.A.	-	-	✓	-	✓
✓	✓	-	-		-	-
✓	-	✓	-	✓	-	✓
-	✓	-	-	✓	-	-
✓	✓	✓	✓	✓	✓	N.A.
✓	-	✓	✓	✓	✓	✓
✓	-	✓	✓	✓	-	✓
✓	-	✓	✓	✓	-	-
✓	-	✓		✓	-	✓
✓	-	-	-	-	-	✓
N.A.	✓	-	-	-	✓	✓

Annex 4: Key features of parliamentary oversight committees' reports, in fieldwork countries with public reports

	Italy *COPASIR*	France *DPR*	Germany *PKGr*	Sweden *Defence Committee*	United Kingdom *ISC*
Date of latest report/reporting period	2017 (covering 2016)	2017 (covering 2016)	2016 on (11.2013 to 11.2015)	2017*	2016 on (09.2015 to 07.2016)**
Obligation to report	✓	✓	✓	✓	✓
Length (in pages)	43	93	14	26	21
Comment on legislation	✓	✓	✓	✓	✓
Parliamentary committee mandate and powers	✓	✓	✓	✓	✓
Parliamentary Committee internal functioning	✓	✓	✓	✓	✓
Number of sessions or hours of work	✓ (59)	✓ (20 sessions - 75 h.)	✓ (32 sessions)	-	✓ (25 sessions)
Number of hearings	✓ (41)	✓ (23)***	-	-	✓ (17)
List of witnesses heard	✓ (28)	✓	✓	-	✓
Content of the hearings	✓	-	-	-	-****
Administration of the Intelligence Services	-	-	-	✓	✓
Expenditure of Intelligence Services	-	✓*****	✓	-	✓******
Policy focus/threats highlighted by the Intelligence Services	✓	✓	✓	✓	✓
Surveillance measures	-	-*******	✓	-	N.A.
Statistics on *ex post* controls	-	-	-	-	N.A.
Statistics on own investigations	✓	-	✓	-	N.A.
Statistics on breaches of safeguards	-	-	-	-	N.A.
Statistics on surveilled persons	-	-	-	-	N.A.
Oversight methods	✓	✓	✓	-	✓
Remedies and statistics on complaints-handling	N.A.	N.A.	✓	-	N.A.
Inter-institutional dialogue	✓	✓	✓	-	✓
Recommendations	-	✓	✓	✓	✓
Ad hoc thematic reports	✓	-	✓	-	✓

Notes: *N.A* = not applicable.
– = not mentioned or not addressed in report.
* The Defence Committee's report is a response to the government's report submitted to parliament, on the use of signals intelligence by the Swedish intelligence services in 2016.
** The ISC's Annual Report covering 2016-17 is ready but not published yet due to the dissolution of the parliament ahead of General Elections in the United Kingdom. A summary of the ISC's work done since July 2016 has been published in a press statement. See United Kingdom, Intelligence and Security Committee of Parliament (2017).
*** Twenty-three hearings, seven interviews/exchanges of views, four visits. See France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 15.
**** The content of all hearings is available on ISC's website under 'Transcripts and Public Evidence'.
***** The DPR is informed annually by the National intelligence coordinator (Coordonateur national au renseignement) about the expenditures of the services. See France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 22. The control of the special funds is carried out by the Audit Commission on Special Funds (CVFS), which belongs to the DPR.
****** Only the combined budgets of MI5, SIS and GCHQ are presented in ISC's Annual Report. The individual figures for each of the intelligence services have been redacted because they would allow the UK's adversaries to more accurately deduce the scale and focus of the services' activities.
******* The DPR refers to the report by the CNCTR.

Source: FRA, 2017

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: http://europa.eu/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

doi:10.2811/792946 TK-04-17-696-EN-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

With terrorism, cyber-attacks and sophisticated cross-border criminal networks posing growing threats, the work of intelligence services has become more urgent, complex and international. Such work can strongly interfere with fundamental rights, especially privacy and data protection. While continuous technological advances potentially exacerbate the threat of such interference, effective oversight and remedies can curb the potential for abuse.

This report is FRA's second publication addressing a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic, and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including its oversight.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 1580 30-0 – Fax +43 1580 30-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office

ISBN 978-92-9491-765-2

Cyber attack hits German train stations as hackers target Deutsche Bahn



An information monitor at a German train station displays the ransomware message CREDIT: @ZEICHENTATEN/TWITTER

Follow

By **Chris Graham**

13 MAY 2017 • 1:20AM

Germany's rail network was thrown into chaos on Friday night when it fell victim to the cyber attack roiling the world (https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/).

Hours after NHS hospitals were left crippled by the attack (https://www.telegraph.co.uk/news/2017/05/12/hacking-nhs-easy-ransomware-freely-available-dark-net/), Deutsche Bahn became the hackers' latest high profile victim.

Using tools widely believed to have been developed by the US National Security Agency, the cyber criminals tricked victims into opening malicious malware attachments to spam emails that appeared to contain invoices, job offers, security warnings and other legitimate files.

The ransomware, called WannaCry, (https://www.telegraph.co.uk/technology/0/ransomware-does-work/) encrypted data on the computers, demanding payments of $300 to $600 to restore access.

Deutsche Bahn computers appeared to be infected with the virus, with the "ransomware" message demanding money appearing on screens at train stations.

Pictures posted on social media by commuters showed train information monitors displaying the ransom demand to unlock the computers.

Èammdoesig
@rammdoesig

Liebe Deutsche Bahn. Behauptet Montag aber nicht, wir hätten Euch nicht gewarnt. #ransomeware #WannaCry (@DB_Presse)

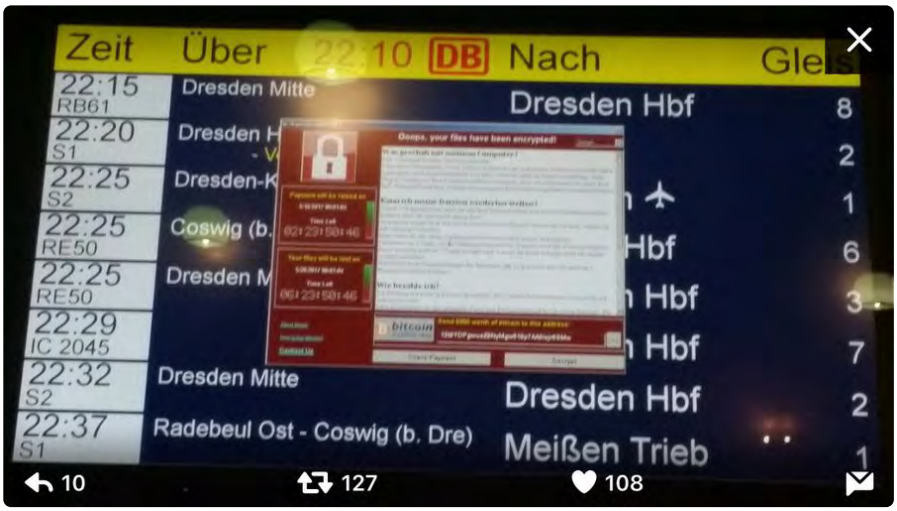


37 11:11 PM - May 12, 2017

66 people are talking about this

Jacob Husted
@jacobhusted69

Deutsche Bahn. #ransomware #criticalInfrastructureNext? #patchNow



2 9:59 PM - May 12, 2017

See Jacob Husted's other Tweets

Deutsche Bahn said (http://db-livemaps.hafas.de/bin/query.exe/dn?L=vs_baustellen&tpl=fullscreenmap&mapCenterX=5581054.6875&mapCenterY=52816043.19154934&mapZoom=6&): "Due to a Trojan attack there are system failures in various areas."

Security experts warn there is no guarantee that access will be granted after payment. Some ransomware that encrypts files ups the stakes after a few days, demanding more money and threatening to delete files altogether.

Researchers with security software maker Avast said they had seen 57,000 infections in 99 countries with Russia, Ukraine and Taiwan the top targets.

A mysterious cyber gang - called Shadow Brokers (https://www.telegraph.co.uk/news/2017/05/12/russian-linked-cyber-gang-shadow-brokers-blamed-nhs-computer/)- said last month it had stolen a 'cyber weapon' from the National Security Agency (NSA), America's powerful military intelligence unit.

NHS cyber attack | Organisations affected

NHS organisations across the country reported IT failures as a result of a major cyber attack. Those affected are believed to include:

ENGLAND

Barts Health Trust	Burton Hospitals NHS Foundation Trust
Blackpool Teaching Hospitals NHS Trust	Colchester General Hospital
Cheshire and Wirral Partnership NHS Foundation Trust	East Lancashire Hospitals NHS Trust
Derbyshire Community Health Services Trust	George Eliot Hospital NHS Trust, Warwickshire
East and North Hertfordshire NHS Trust	Nottinghamshire Healthcare NHS Trust
Hampshire Hospitals Trust	Northern Lincolnshire and Goole NHS Foundation Trust

Show more

The hacking tool, called 'Eternal Blue', gives unprecedented access to all computers using Microsoft Windows (https://www.telegraph.co.uk/technology/0/protect-ransomware/), the world's most popular computer operating system. It had been developed by the NSA to gain access to computers used by terrorists and enemy states.

The gang in turn 'dumped' the computer bug on an obscure website on April 14 and it is believed to have been picked up by a separate crime gang which has used it to gain remote access to computers around the world.

The hackers, who have not come forward to claim responsibility or otherwise been identified, likely made it a "worm," or self spreading malware.

Microsoft on Friday said it was pushing out automatic Windows updates (https://www.telegraph.co.uk/news/2017/05/12/cyber-attack-nhs-stark-warning-society-still-vulnerable-cyber/) to defend clients from WannaCry. It issued a patch on March 14 to protect them from Eternal Blue.

Erpressersoftware

450 Computer der Bahn von "WannaCry"-Virus betroffen

Wohl nirgendwo in Deutschland waren die Folgen des "WannaCry"-Online-Angriffs präsenter als auf Bahnhöfen. Bis die Anzeigetafeln der Deutschen Bahn wieder funktionieren, kann es noch dauern. Lösegeld will der Konzern nicht gezahlt haben.



DPA

Elektronische Anzeigentafel der Bahn im Hauptbahnhof Leipzig

Mehr erfahren

Teilen Twittern E-Mail

Dienstag, **16.05.2017** 12:55 Uhr

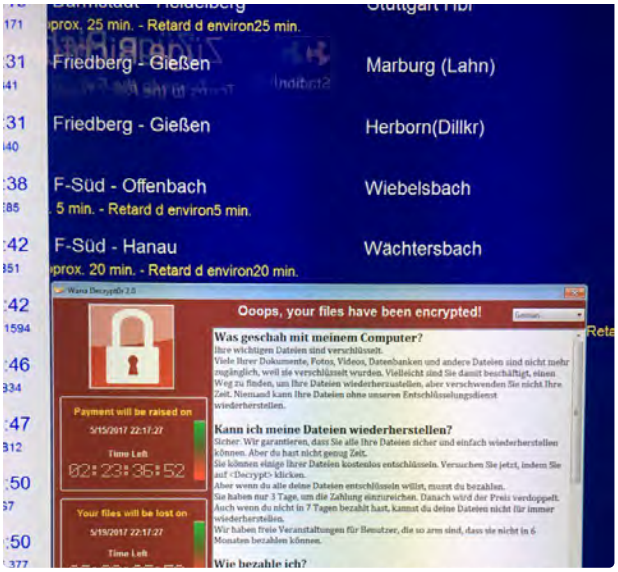
Drucken Nutzungsrechte Feedback Kommentieren

Von der weltweiten "WannaCry"-Attacke mit Erpressersoftware waren nach Angaben der Berliner Staatsanwaltschaft insgesamt 450 Rechner der Deutschen Bahn betroffen. Es gebe auch Hinweise auf weitere Geschädigte, sagte Sprecher Martin Steltner am Dienstag. Möglich sei, dass sich Betroffene bislang nicht gemeldet hätten, weil sie eine Rufschädigung befürchteten.

Die Hacker wollten mit ihrem Angriff Geld erpressen. Die Bahn habe aber nichts gezahlt, heißt es. Ermittelt werde auch wegen Computersabotage. Europäische Behörden wie Eurojust (für die Justiz) und Europol (für die Polizei) arbeiten laut Staatsanwaltschaft bei der Aufklärung zusammen. In Deutschland führt das Bundeskriminalamt die Ermittlungen.

Uwe Pleban
@uwepleban

Oops, the Deutsche Bahn has been hacked via ransomware.



105 18:45 - 12. Mai 2017

130 Nutzer sprechen darüber

Wegen des "WannaCry" genannten Cyber-Angriffs waren deutschlandweit zahlreiche digitale Anzeigetafeln sowie Ticketautomaten an Bahnhöfen ausgefallen. Die Reparatur der Anzeigen sollte laut Bahn mehrere Tage dauern. Auch die Technik zur Videoüberwachung war laut Bundesinnenministerium betroffen.

Lesetipp



DPA

Experten über "WannaCry"-Attacke: "Wir hatten noch Glück"

Nach SPIEGEL-Informationen war auch die Bahn-Logistiktochter Schenker von "WannaCry" betroffen. "Bei Schenker ist der Virus eingedämmt und die Auswirkungen auf Kunden waren minimal", sagte ein Bahn-Sprecher.

Nach der Angriffswelle haben die Grünen die IT-Sicherheitsstrategie der Bundesregierung scharf kritisiert. Sie werfen der Koalition vor, den Schutz von Bürgern und Unternehmen zu vernachlässigen, dabei seien diese "bislang am häufigsten tatsächlich Opfer von schlecht geschützten IT-Systemen, aber auch von gezielten Angriffen", heißt es in einem Positionspapier der Bundestagsfraktion, das dem SPIEGEL vorliegt.

Besonders harte Kritik üben die Grünen darin an Innenminister Thomas de Maizière (CDU). "Die Maßnahmen des Bundesinnenministeriums beschränkten sich allenfalls auf die Sicherheit der Bundesverwaltung." Es existiere "keine übergreifende Strategie, etwa für staatlich unterstützte Beratungsangebote oder zur Stärkung der Medienkompetenz." Das Thema IT-Sicherheit sei bei de Maizière falsch aufgehoben.

Leseraufruf

Sind Sie auch von "WannaCry" oder anderer Erpressungsoftware betroffen? Wir würden gerne mit Ihnen sprechen. Bitte melden Sie sich bei unserem Redakteur Fabian Reinbold.

Mail an die Netzwelt-Redaktion

mbö/fab/dpa

Zur Startseite

Diesen Artikel...

Drucken | Feedback | Nutzungsrechte

Teilen Twittern E-Mail

Auch interessant

ANZEIGE



Endlich Einfach Abnehmen
Das wird der Abnehm-Industrie nicht gefallen. Dozent für Ernährung verschenkt Abnehm-Bestseller

ANZEIGE



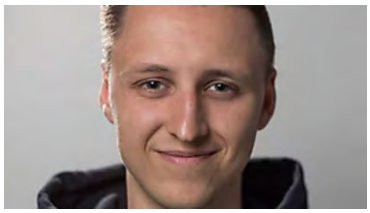
BWT
Wasser filtern oder Wasserflaschen kaufen? Das ist wirklich besser

ANZEIGE



Gesundheits-Pra mien
Gegen Sehschwäche im Alter: Das sind die 7 besten Übungen

ANZEIGE



Jasper Caven
Warum verschenkt dieser Ernährungsberater seinen Abnehm-Bestseller

ANZEIGE



Gesundheits-Pra mien
Ingwer: so wirkt es Wunder für Ihre Gesundheit!

ANZEIGE



Flightright
Flugverspätung? Flugausfall? Soviel Entschädigung steht Ihnen zu

empfohlen von

Anzeige

Mehr zum Thema

Computersicherheit **Deutsche Bahn** Alle Themenseiten

National Audit Office

Report
by the Comptroller
and Auditor General

Department of Health

Investigation: WannaCry cyber attack and the NHS

HC 414 SESSION 2017–2019 25 APRIL 2018

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of £734 million in 2016.

National Audit Office

Department of Health

Investigation: WannaCry cyber attack and the NHS

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 24 April 2018

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Sir Amyas Morse KCB
Comptroller and Auditor General
National Audit Office

24 October 2017

HC 414 | £10.00

This report investigates the NHS's response to the cyber attack that affected it in May 2017 and the impact on health services.

Investigations

We conduct investigations to establish the underlying facts in circumstances where concerns have been raised with us, or in response to intelligence that we have gathered through our wider work.

© National Audit Office 2018

The material featured in this document is subject to National Audit Office (NAO) copyright. The material may be copied or reproduced for non-commercial purposes only, namely reproduction for research, private study or for limited internal circulation within an organisation for the purpose of review.

Copying for non-commercial purposes is subject to the material being accompanied by a sufficient acknowledgement, reproduced accurately, and not being used in a misleading context. To reproduce NAO copyright material for any other use, you must contact copyright@nao.gsi.gov.uk. Please tell us who you are, the organisation you represent (if any) and how and why you wish to use our material. Please include your full contact details: name, address, telephone number and email.

Please note that the material featured in this document may not be reproduced for commercial gain without the NAO's express and direct permission and that the NAO reserves its right to pursue copyright infringement proceedings against individuals or companies who reproduce material for commercial gain without our permission.

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.

11594 04/18 NAO

Contents

What this investigation is about 4

Summary 5

Part One
The impact of the cyber attack 11

Part Two
Why some parts of
the NHS were affected 16

Part Three
How the Department and
the NHS responded 21

Appendix One
Our investigative approach 28

Appendix Two
Trusts infected or disrupted
by WannaCry 30

The National Audit Office study team consisted of:
Finnian Bamber, Alex Bowyer, Nigel Leung, Francisca Lopes, Linda Mills and David Williams, under the direction of Robert White.

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

What this investigation is about

1 On Friday 12 May 2017 a global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. In the UK, the attack particularly affected the NHS, although it was not the specific target. At 4 pm on 12 May, NHS England declared the cyber attack a major incident and implemented its emergency arrangements to maintain health and patient care. On the evening of 12 May a cyber-security researcher activated a kill-switch so that WannaCry stopped locking devices.

2 According to NHS England, the WannaCry ransomware affected at least 80 out of the 236 trusts across England, because they were either infected by the ransomware or turned off their devices or systems as a precaution. A further 603 primary care and other NHS organisations were also infected, including 595 GP practices.

3 Before the WannaCry attack the Department of Health (the Department) and its arm's-length bodies had work under way to strengthen cyber-security in the NHS. For example, NHS Digital was broadcasting alerts about cyber threats, providing a hotline for dealing with incidents, sharing best practice and carrying out on-site assessments to help protect against future cyber attacks; and NHS England had embedded the 10 Data Security Standards (recommended by the National Data Guardian) in the standard NHS contract for 2017-18 and was providing training to its Board and local teams to raise awareness of cyber threats. In light of the WannaCry attack, the Department announced further plans to strengthen NHS organisations' cyber-security.

4 Our investigation focuses on events immediately before 12 May 2017 and up until 30 September 2017. We only cover the effect the WannaCry attack had on the NHS in England. We do not cover how the WannaCry attack affected other countries or organisations outside the NHS. A cyber attack on either the health or social care sectors could cause disruption across the whole health and social care sector. For example, the Care Quality Commission (CQC) told us that, as some trusts were unable to communicate with social services, there could have been delays in the discharge of patients from hospital to social care, although the CQC relayed advice from NHS Digital and NHS England to social care providers to help manage any disruption. This investigation sets out the facts about:

- the ransomware attack's impact on the NHS and its patients;
- why some parts of the NHS were affected; and
- how the Department and NHS national bodies responded to the attack.

Summary

1 The WannaCry attack affected NHS services in the week from 12 May to 19 May 2017. The Department of Health (the Department) and NHS England worked with NHS Digital, NHS Improvement, the National Cyber Security Centre, the National Crime Agency and others to respond to the attack.

Key findings

The risk of a cyber attack affecting the NHS

2 **WannaCry was the largest cyber attack to affect the NHS, although individual trusts had been attacked before 12 May 2017.** For example, two of the trusts infected by WannaCry had been infected by previous cyber attacks. One of England's biggest trusts, Barts Health NHS Trust, had been infected before, and Northern Lincolnshire and Goole NHS Foundation Trust had been subject to a ransomware attack in October 2016, leading to the cancellation of 2,800 appointments (paragraph 3.7 and Figure 5).

3 **The Department was warned about the risks of cyber attacks on the NHS a year before WannaCry and although it had work under way it did not formally respond with a written report until July 2017**. The Secretary of State for Health asked the National Data Guardian and the Care Quality Commission (CQC) to undertake reviews of data security. These reports were published in July 2016 and warned the Department that cyber attacks could lead to patient information being lost or compromised and jeopardise access to critical patient record systems. They recommended that all health and care organisations needed to provide evidence that they were taking action to improve cyber-security, including moving off old operating systems. Although the Department and its arm's-length bodies had work under way to improve cyber-security in the NHS, the Department did not publish its formal response to the recommendations until July 2017 (paragraphs 3.6 and 3.11).

4 The Department and its arm's-length bodies did not know whether local NHS organisations were prepared for a cyber attack. Local healthcare organisations such as trusts and clinical commissioning groups are responsible for keeping the information they hold secure, and for having arrangements in place to respond to an incident or emergency, including a cyber attack. Local healthcare bodies are overseen by the Department and its arm's-length bodies. The Department and Cabinet Office wrote to trusts in 2014, saying it was essential they had "robust plans" to migrate away from old software, such as Windows XP, by April 2015. In March and April 2017, NHS Digital had issued critical alerts warning organisations to patch their systems to prevent WannaCry. However, before 12 May 2017, the Department had no formal mechanism for assessing whether NHS organisations had complied with its advice and guidance. Prior to the attack, NHS Digital had conducted an on-site cyber-security assessment for 88 out of 236 trusts, and none had passed. However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of an organisation (paragraphs 2.5, 2.7, 2.10 to 2.12 and 3.2, and Figure 4).

How the WannaCry attack affected the NHS

5 The attack led to disruption in at least 34% of trusts in England although the Department and NHS England do not know the full extent of the disruption (Figure 1). On 12 May, NHS England initially identified 45 NHS organisations including 37 trusts that had been infected by the WannaCry ransomware (although NHS England initially identified 37 trusts as being infected, three of these were mis-categorised and later re-categorised as not being infected but experiencing disruption). Over the following days, more organisations reported they had been affected. In total, at least 80 out of 236 trusts across England were affected. The trusts included:

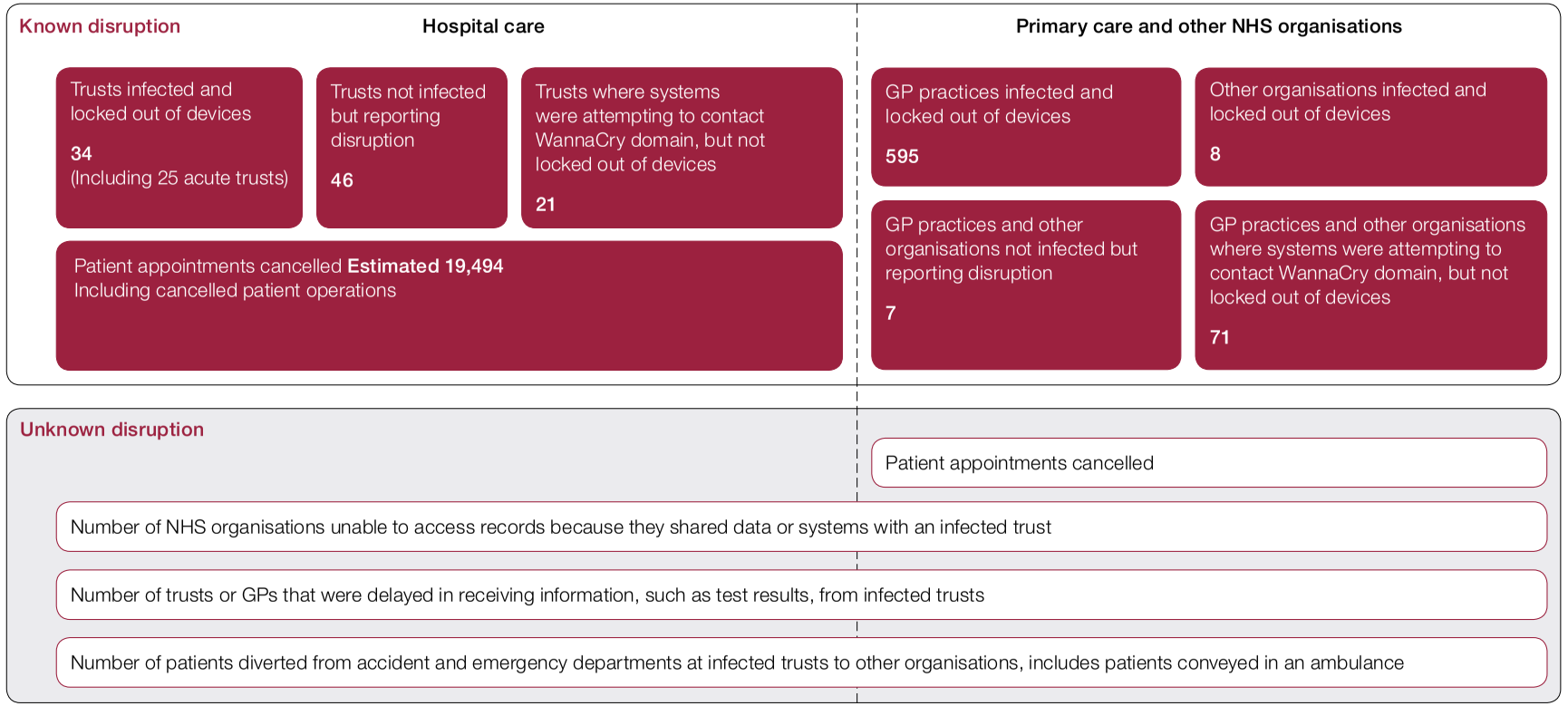
- 34 infected and locked out of devices (of which, 25 were acute trusts); and
- 46 not infected but reporting disruption. For example, these trusts shut down their email and other systems as a precaution and on their own initiative, as they had not received central advice early enough on 12 May to inform their decisions on what to do. This meant, for example, that they had to use pen and paper for activities usually performed electronically.

NHS England and NHS Digital identified a further 21 trusts that were attempting to contact the WannaCry domain, but were not locked out of their devices. There are two possible reasons for this. Trusts may have become infected after the kill-switch had been activated, and were therefore not locked out of their devices. Alternatively, they may have contacted the WannaCry domain as part of their cyber-security activity.

A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices. However, the Department does not know how many NHS organisations could not access records or receive information, because they shared data or systems with an infected trust. NHS Digital told us that it believes no patient data were compromised or stolen (paragraphs 1.2 to 1.5 and 1.9, and Figure 1).

Figure 1
The impact of WannaCry on the NHS

The NHS experienced a wide range of disruption as a consequence of the WannaCry cyber attack



Notes

1 'Other organisations' include clinical commissioning groups, commissioning support units, an NHS 111 provider, and non-NHS bodies that provide NHS care, such as a hospice, social enterprise and community interest companies.

2 The numbers shown are based on organisations self-reporting problems to national bodies, and NHS England and NHS Digital's analysis of internet activity, and may be higher if some organisations did not report the problems they experienced in a timely or accurate way.

3 Some of the trusts identified as not infected but reporting disruption did have a small number of devices infected. However, they did not report themselves to NHS England as infected, and NHS England did not recategorise them as being infected after the WannaCry attack was over.

4 Some trusts, GP practices and other organisations were identified as having systems that attempted to contact the WannaCry domain, but were not locked out of their devices. There are two possible explanations for this: they could have become infected after the kill-switch had been activated. Or, they could have avoided infection but contacted the WannaCry domain as part of their cyber-security activity. NHS England does not know which organisations fall into each category.

Source: National Audit Office analysis of NHS England data

6 **Thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments.** Between 12 May and 18 May, NHS England collected some information on cancelled appointments, to help it manage the incident, but this did not include all types of appointment. NHS England identified 6,912 appointments had been cancelled, and estimated more than 19,000 appointments would have been cancelled in total, based on the normal rate of follow-up appointments to first appointments. NHS England told us it does not plan to identify the actual number because it is focusing its efforts on responding appropriately to the lessons learned from WannaCry. As data were not collected during the incident, neither the Department nor NHS England know how many GP appointments were cancelled, or how many ambulances and patients were diverted from the five accident and emergency departments that were unable to treat some patients (paragraphs 1.7, 1.8 and 1.10, and Figure 1).

7 **The Department, NHS England and the National Crime Agency told us that no NHS organisation paid the ransom, but the Department does not know how much the disruption to services cost the NHS.** The Department, NHS England and the National Crime Agency told us no NHS organisation paid the ransom. NHS Digital told us it advised the trusts it spoke to not to pay the ransom, and wrote to all trusts on 14 May advising against the payment of ransoms. The Department does not know the cost of the disruption to services. Costs include: cancelled appointments; additional IT support provided by local NHS bodies, or IT consultants; or the cost of restoring data and systems affected by the attack. National and local NHS staff worked overtime including over the weekend of 13-14 May to resolve problems and to prevent a fresh wave of organisations being affected by WannaCry on Monday 15 May (paragraphs 1.11 and 1.12).

8 **The cyber attack could have caused more disruption if it had not been stopped by a cyber researcher activating a 'kill-switch'.** On the evening of 12 May a cyber-security researcher activated a 'kill-switch' so that WannaCry stopped locking devices. This meant that some NHS organisations had been infected by the WannaCry ransomware, but because of the researcher's actions, they were not locked out of their devices and systems. Between 15 May and mid-September NHS Digital and NHS England identified a further 92 organisations, including 21 trusts, as contacting the WannaCry domain, although some of these may have been contacting the domain as part of their cyber-security activity. Of the 34 trusts infected and locked out of devices, 29 were located in the North NHS region and the Midlands and East NHS region. NHS England believes more organisations were infected in these regions because they were hit early on 12 May before the WannaCry 'kill-switch' was activated (paragraphs 1.14 and 2.2, and Figure 3).

The NHS response to the attack

9 **The Department had developed a plan, which included roles and responsibilities of national and local organisations for responding to an attack, but had not tested the plan at a local level.** This meant the NHS was not clear what actions it should take when affected by WannaCry. NHS England found that responding to WannaCry was different from dealing with other incidents, such as a major transport accident. Because WannaCry was different it took more time to determine the cause of the problem, the scale of the problem and the number of organisations and people affected (paragraph 3.3 and Figure 2).

10 **As the NHS had not rehearsed for a national cyber attack it was not immediately clear who should lead the response and there were problems with communications.** The WannaCry attack began on the morning of 12 May. At 4 pm NHS England declared the cyber attack a major incident and at 6:45 pm initiated its existing Emergency, Preparedness, Resilience and Response plans to act as the single point of coordination for incident management, with support from NHS Digital and NHS Improvement. In the absence of clear guidelines on responding to a national cyber attack, local organisations reported the attack to different organisations within and outside the health sector, including local police. Communication was difficult in the early stages of the attack as many local organisations could not communicate with national NHS bodies by email as they had been infected by WannaCry or had shut down their email systems as a precaution, although NHS Improvement did communicate with trusts' chief executive officers by telephone. Locally, NHS staff shared information through personal mobile devices, including using the encrypted WhatsApp application. Although not an official communication channel, national bodies and trusts told us it worked well during this incident (paragraphs 3.3 to 3.5 and Figure 2).

11 **In line with its existing procedures for managing a major incident, NHS England initially focused on maintaining emergency care.** Since the attack occurred on a Friday this caused minimal disruption to primary care services, which tend to be closed over the weekend. Twenty of the 25 infected acute trusts managed to continue treating urgent and emergency patients throughout the weekend. However, five – in London, Essex, Hertfordshire, Hampshire and Cumbria – had to divert patients to other accident and emergency departments, and a further two needed outside help to continue treating patients. By 16 May only two hospitals were still diverting patients. The recovery was helped by the work of the cyber-security researcher that stopped WannaCry spreading (paragraphs 1.7, 1.13 and 1.14).

Lessons learned

12 NHS Digital told us that all organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves. All NHS organisations infected by WannaCry had unpatched or unsupported Windows operating systems so were susceptible to the ransomware. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection. NHS Digital told us that the majority of NHS devices infected were unpatched but on supported Microsoft Windows 7 operating systems. Unsupported devices (those on XP) were in the minority of identified issues. NHS Digital has also confirmed that the ransomware spread via the internet, including through the N3 network (the broadband network connecting all NHS sites in England), but that there were no instances of the ransomware spreading via NHSmail (the NHS email system) (paragraphs 1.2, 1.6 and 2.4 to 2.6).

13 There was no clear relationship between vulnerability to the WannaCry attack and leadership in trusts. We found no clear relationship between trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission (paragraph 2.8).

14 The NHS has accepted that there are lessons to learn from WannaCry and is taking action. Lessons identified by the Department and NHS national bodies include the need to:

- develop a response plan setting out what the NHS should do in the event of a cyber attack and establish the roles and responsibilities of local and national NHS bodies and the Department;
- ensure organisations implement critical CareCERT alerts (emails sent by NHS Digital providing information or requiring action), including applying software patches and keeping anti-virus software up to date;
- ensure essential communications are getting through during an attack when systems are down; and
- ensure that organisations, boards and their staff are taking the cyber threat seriously, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise impacts on patient care.

Since WannaCry, NHS England and NHS Improvement have written to every trust, clinical commissioning group and commissioning support unit asking boards to ensure that they have implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and taken essential action to secure local firewalls (paragraphs 3.8 and 3.9).

Part One

The impact of the cyber attack

1.1 WannaCry was the largest ever cyber attack to affect the NHS in England. The timeline of the main events relating to the WannaCry ransomware attack which affected NHS services in the week from 12 May to 19 May 2017 is set out in **Figure 2** overleaf.

The scale of the attack

1.2 NHS Digital told us that the ransomware spread via the internet, including through the N3 network. As shown in Figure 1 (page 7), the WannaCry ransomware attack affected at least 80 out of 236 trusts across England. These numbers are based on NHS organisations' own reports to NHS England. Of these 80 trusts, there were:

- 34 trusts infected and locked out of devices (of which, 25 were acute trusts); and
- 46 trusts not infected but reporting disruption.

NHS England and NHS Digital identified a further 21 trusts that were attempting to contact the WannaCry domain, but were not locked out of their devices. There are two possible reasons for this. Trusts may have become infected after the kill-switch had been activated, and were therefore not locked out of their devices.[1] Alternatively, they may have contacted the WannaCry domain as part of their cyber-security activity.

1.3 The trusts infected by the WannaCry ransomware experienced two main types of disruption including:

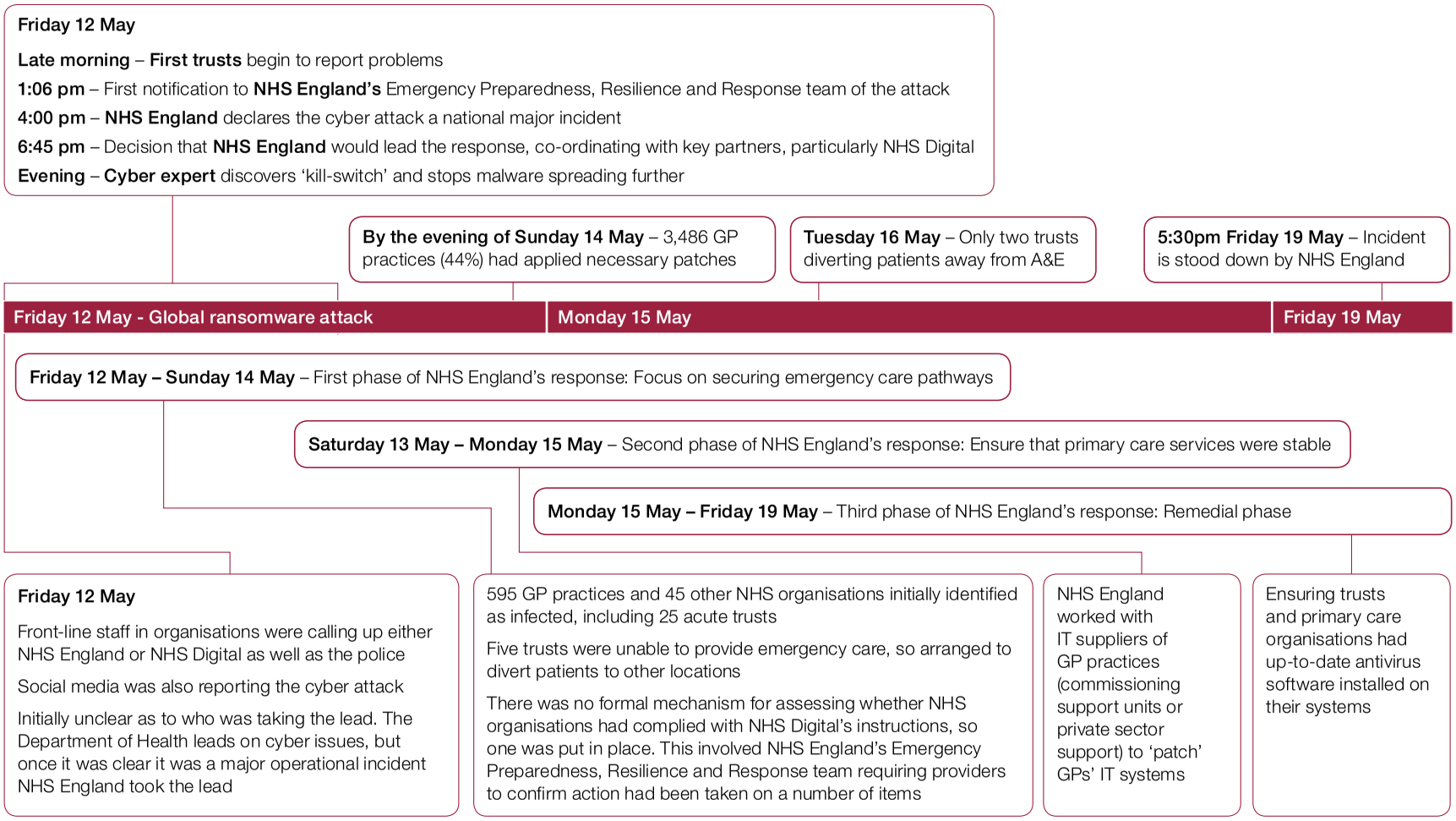
- NHS staff being locked out of devices, which prevented or delayed staff accessing and updating patient information, sending test results to patients' GPs and transferring or discharging patients from hospital; and
- medical equipment and devices being locked, or isolated from trusts' IT systems to prevent them being locked. This meant trusts' radiology and pathology departments were disrupted as the trusts relied on the equipment and devices for diagnostic imaging (such as MRI scanners) and for testing blood and tissue samples.

1 A 'kill-switch' is a mechanism that is incorporated into software to shut down that software, or the device on which it sits, in an emergency situation in which it cannot be shut down in the usual manner.

Figure 2

Timeline of the WannaCry attack from 12 May to 19 May 2017

NHS England emergency response to WannaCry lasted one week



Note

1 On Friday 12 May NHS England initially identified 45 organisations as being infected, but three of these were mistakenly identified as being infected and later re-categorised as not being infected but experiencing disruption. Twenty-five of the 42 organisations actually infected were acute trusts.

Source: National Audit Office

As at 19 May 2017, NHS England had identified 1,220 pieces of diagnostic equipment that had been infected, 1% of all such NHS equipment. Although a relatively small proportion of devices, the figure does not include devices disconnected from IT systems to prevent infection. The trusts we spoke to told us about the disruption they had experienced due to diagnostic equipment being infected or isolated, such as not being able to send MRI scan results to clinicians treating patients in other parts of the hospital.

1.4 The disruption at trusts not infected by the ransomware was caused by:

- the absence of timely central direction, leading to the trusts taking actions on their own initiative to avoid becoming infected, including shutting down devices or isolating devices from their networks to protect themselves from the ransomware; or
- trusts not being able to access electronic patient records or receive information, such as test results, because they shared data or systems with an infected trust which had shut down its systems; or
- trusts disconnecting from the N3 network, the broadband network connecting all NHS sites in England.

1.5 The disruption at these trusts took a number of forms. For example, some trusts had to use manual workarounds to perform their usual tasks, such as providing medication to patients, and record information using pen and paper. In addition, organisations could not receive external emails, so communication with national bodies and others outside their trust was severely limited.

1.6 Despite widespread local disruption, NHS Digital told us that national NHS IT systems managed by NHS Digital were not infected, such as the NHS Spine (a service holding secure databases of demographic and clinical information) and NHSmail (the NHS email system).

1.7 Of the 25 acute trusts infected and locked out of devices, five had to divert emergency ambulance services to other hospitals. The five trusts and hospitals were:

- Barts Health NHS Trust (Royal London Hospital);
- Mid Essex Hospital Services NHS Trust (Broomfield Hospital);
- East and North Hertfordshire NHS Trust (Lister Hospital);
- Hampshire Hospitals NHS Foundation Trust (Basingstoke Hospital); and
- North Cumbria University Hospitals NHS Trust (West Cumberland Hospital).

The impact on patients

1.8 As infected NHS organisations could not access important information and electronic systems, including patient records, they had to cancel appointments and operations and some trusts had to divert patients to other accident and emergency departments. Between 12 May and 18 May, NHS England collected some information on how many appointments had been cancelled to help it manage the incident, but did not collect data on all types of appointment. NHS England identified that the NHS had cancelled 6,912 appointments, but this figure does not include repeat outpatient appointments and cancellations identified after 18 May. NHS England estimated the total number of cancelled appointments as being around 19,494, based on the normal rate of follow-up appointments to first appointments, but told us it does not plan to identify the actual number because it is focusing its efforts on responding appropriately to the lessons learned from WannaCry. NHS England did not collect data on how many GP appointments were cancelled or how many ambulances and patients were diverted from the accident and emergency departments that were unable to treat patients.

1.9 NHS organisations did not report any cases of harm to patients or of data being compromised or stolen. If the WannaCry ransomware attack had led to any patient harm or loss of data then NHS England told us that it would expect trusts to report cases through existing reporting channels, such as reporting data loss direct to the Information Commissioner's Office (ICO) in line with existing policy and guidance on information governance. NHS Digital also told us that analysis of the WannaCry ransomware suggested that the cyber attack was not aimed at accessing or stealing data, although it does not know for certain that this is the case.

1.10 The NHS continued to provide emergency care from 12 May to 19 May, although some patients had to travel further as five hospitals had diverted services (paragraph 1.7). Patients with planned appointments experienced most disruption. Cancer charities, including Macmillan Cancer Support and Cancer Research UK, reported cancellations causing distress to patients. NHS England's own review identified at least 139 patients who had an urgent referral for potential cancer cancelled, as at 18 May, although the actual number may be higher if trusts misreported during the data collection or identified cancellations after 18 May.

The financial impact

1.11 The Department of Health (the Department), NHS England and the National Crime Agency have told us that no NHS organisations paid the ransom. NHS Digital told us it advised against the payment of the WannaCry ransom during site visits and telephone conferences with infected trusts. Furthermore, NHS England and NHS Digital wrote to all trusts on 14 May advising them against the payment of ransoms, but these emails did not always reach trusts after that attack had begun.

1.12 The NHS has not calculated the total cost of cancelled appointments; of NHS staff overtime; of additional IT support provided by NHS local bodies or IT consultants; or the cost of restoring data and systems affected by the attack. For example, trusts and other NHS organisations had to roll back systems and restore data and systems, including re-entering data recorded manually while trusts' systems were down. National and local NHS staff had to work overtime, including over the weekend of 13–14 May, to resolve problems and to prevent a fresh wave of organisations being affected by WannaCry on Monday 15 May.

The recovery

1.13 In line with its established procedures for responding to a major incident, NHS England focused its initial response on maintaining emergency care, and within 24 hours began attending to primary care. Since the attack occurred on a Friday it caused minimal disruption to primary care services, which tend to be closed over the weekend. Twenty of the 25 infected acute trusts continued treating urgent and emergency patients throughout the weekend. However, five trusts, including Barts Health NHS Trust, were unable to see some patients and had to divert them to other hospitals, and a further two needed outside help to continue treating patients. NHS England worked with trusts to ensure diverts were put in place and help provided. By Tuesday 16 May, only two hospitals were still diverting patients: Lister Hospital in Hertfordshire and Broomfield Hospital in Essex. NHS England 'stood down' the incident on Friday 19 May.

1.14 The recovery was aided by the work of a cyber-security researcher who activated a kill-switch so that WannaCry stopped locking devices. The researcher triggered the kill-switch on the evening of Friday 12 May. This meant that some NHS organisations were infected by the WannaCry malware, but because of the actions of the researcher they were not locked out of their devices and systems. Between 15 May and mid-September, NHS Digital and NHS England identified a further 92 organisations, including 21 trusts, attempting to contact the WannaCry domain, in addition to the initial 45 organisations they had identified as being infected.[2] Although some of these trusts may have contacted the WannaCry domain as part of their cyber-security activity.

2 NHS England initially identified 45 organisations as being infected, but three of these were mistakenly identified as being infected and later re-categorised as not being infected but experiencing disruption.

Part Two

Why some parts of the NHS were affected

2.1 NHS organisations across England were affected by the WannaCry attack. **Figure 3** sets out the location of the trusts affected and shows the:

- 34 trusts infected by the WannaCry malware; and
- 46 trusts not infected by the malware but reporting disruption.

2.2 Of the 34 trusts infected, 29 were located in the North NHS region and the Midlands and East NHS region. NHS England believes more organisations were infected in these regions because they were hit early on 12 May before the WannaCry kill-switch was activated.

Failure to patch and update systems and reliance on old software

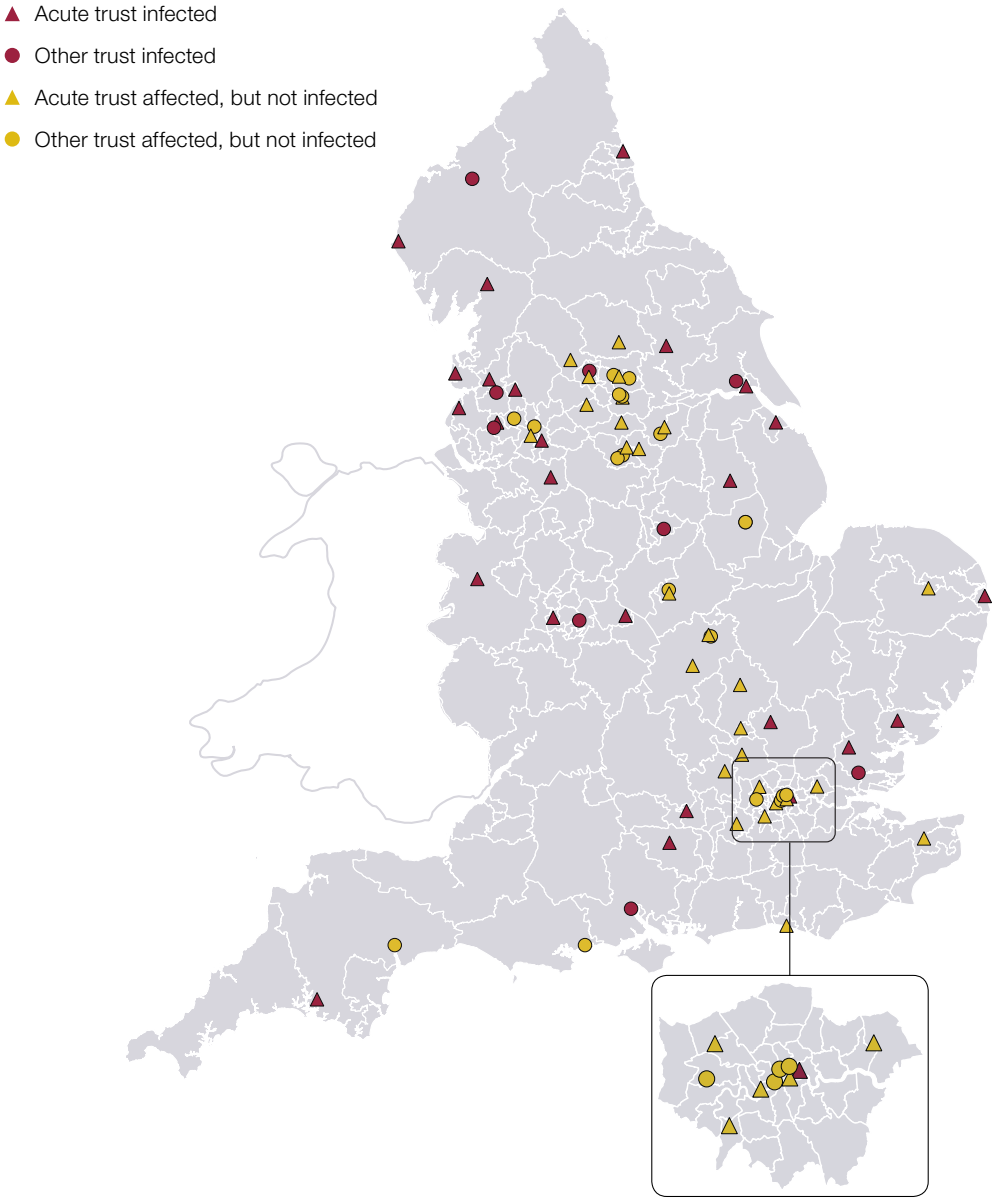
2.3 It is not possible to eliminate all cyber threats but organisations can prevent harm through good cyber-security. Such practice includes maintaining up-to-date firewalls and anti-virus software, and applying patches (updates) in a timely manner. NHS England's view is that WannaCry infected some parts of the NHS mainly because organisations had failed to maintain good cyber-security practices.

2.4 NHS Digital told us that all the infected trusts had a common vulnerability in their Windows operating systems which was exploited by the WannaCry attack. All NHS organisations infected by WannaCry had unpatched, or unsupported, Windows operating systems. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded the organisations against infection.

Figure 3

Trusts affected by the cyber attack

Disruption to front-line services affected all parts of the country but was concentrated in the North NHS region and the Midlands and East NHS region



Note

1 NHS England believes the concentration of infected trusts in the North NHS region and the Midlands and East NHS region does not reflect variations in cyber-security, but may be partially explained by these organisations becoming infected earlier in the day, before the WannaCry 'kill-switch' was activated.

Source: National Audit Office analysis of NHS England data

2.5 NHS Digital told us that the majority of NHS devices infected were unpatched but on the supported Windows 7 operating system. Trusts using Windows 7 could have protected themselves against WannaCry by applying a patch (or update) issued by Microsoft in March 2017, and NHS Digital had issued CareCERT alerts on 17 March and 28 April asking trusts to apply the patch.[3] According to the Department of Health (the Department), more than 90% of devices in the NHS use the Windows 7 operating system.

2.6 A second issue was that some trusts were running the older Windows XP operating system on some devices. This made the trusts vulnerable because Microsoft was no longer releasing patches for this operating system, and so they could not protect their systems from WannaCry unless they isolated those devices from the network. Some trusts also experienced issues with some medical equipment, such as MRI scanners that have Windows XP embedded within them (see paragraph 1.3). This equipment is generally managed by the system vendors and local trusts are not capable of applying updates themselves. Support from the vendors of these devices was often poor according to NHS England and NHS Digital. However, trusts running Windows XP on their medical equipment could have protected themselves by isolating these devices from the rest of the network (although this may necessitate manual workarounds). In July 2017, as part of its response to the National Data Guardian review, the Department told local bodies to ensure that they had moved away from, or were actively managing, unsupported software by April 2018.

2.7 The Department and Cabinet Office had written to trusts in 2014 offering some temporary help with security for old equipment until April 2015, after which time there would be no support. This meant that it was essential that all NHS organisations had "robust plans" to migrate away from Windows XP. Despite this, the Department told us about 5% of the NHS IT estate, including computers and medical equipment, was still using Windows XP on 12 May 2017. This is partly explained by the fact that it is not always possible to remove or update Windows XP in applications and IT services based on that operating system. Immediately after the WannaCry attack Microsoft issued a patch for Windows XP that would prevent WannaCry and similar ransomware.

Leadership and size of trusts

2.8 We found no clear relationship between those trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission (CQC). Of the 34 trusts infected by WannaCry, four (12%) had been rated as 'inadequate' against the 'well-led' domain at their last CQC inspection, compared with 7% of NHS organisations not infected.[4] However, CQC had not focused on how well led trusts were in relation to cyber-security in their inspections before 12 May 2017. We understand CQC has plans to enhance its line of questions regarding information and digital systems as part of its inspection of the leadership of trusts in the future.

3 A CareCERT alert is an email sent by NHS Digital providing information or requiring action from NHS organisations.
4 Of the 34 trusts infected by WannaCry, 33 had a CQC rating.

2.9 We also found that infected trusts tended to employ more staff than average. Of the 34 infected trusts:

- 12 (35%) were among the 25% of trusts employing the most staff; and
- 23 (68%) employed more than the median number of staff.

Although there is limited evidence on why this should be the case, we found that:

- some of the trusts we spoke to told us that integrating IT systems when trusts merge (and become larger) and running many different versions of Windows operating systems, not all of which are supported, can be a challenge; and
- WannaCry exploited weaknesses within parts of Microsoft's Windows operating system used to share files within organisations. This meant it spread automatically in some cases, and organisations with large Windows networks were among the worst affected.

Prepared for a cyber attack

2.10 Before 12 May, the Department and its arm's-length bodies did not know whether trusts had complied with CareCERT alerts as no formal mechanism of assessment existed at that time. On 12 May, NHS Digital worked with NHS England to put in place a formal mechanism for assessing whether NHS organisations had complied with CareCERT alerts. Emergency, Preparedness, Resilience and Response (EPRR) teams requested a positive return from providers by midnight on 12 May that, for example where they had:

- not been subject to an attack, they had implemented the patch; and
- been subject to an attack, they had implemented remedial works; had been able to roll back their systems; and could continue to provide emergency services or – if not – had put mitigations in place.

2.11 Before the WannaCry attack, NHS Digital offered an on-site inspection to hospitals to assess their cyber-security (known as 'CareCERT Assure'). This inspection was voluntary. By 12 May, NHS Digital had inspected 88 out of 236 trusts and none had passed. NHS Digital's review of the WannaCry attack concluded that CareCERT advice and guidance (including inspections) was mostly followed by organisations with relatively mature cyber-security arrangements, while vulnerable trusts were not taking action to improve their security. NHS Digital also found that, in general, trusts had not identified cyber-security as being a risk to patient outcomes, and had tended to overestimate their readiness to manage a cyber attack. NHS Digital believes this reflects a lack of understanding of the nature of cyber risk among trusts, rather than a neglect of cyber-security.

2.12 The Department and its arm's-length bodies did not hold information on how prepared local organisations were to respond to a cyber attack, such as whether cyber-security appeared on organisations' risk registers or whether trusts complied with good practice. The Department and its arm's-length bodies also had limited central information on trusts' IT and digital assets such as anti-virus software and IP addresses. At the start of its investigation, the National Crime Agency had to gather evidence from all sites, including information on the devices affected, IP addresses and network traffic, to assess the impact of WannaCry on the NHS, rather than being able to access the information centrally.

Part Three

How the Department and the NHS responded

Devolved responsibility for cyber-security

3.1 The Department of Health (the Department) has overall national responsibility for cyber-security resilience and responding to incidents in the health sector. However, the Department devolves responsibility for managing cyber-security to local organisations – NHS trusts, GPs, clinical commissioning groups and social care providers. Regulators and other national bodies oversee and support local NHS organisations. While NHS foundation trusts are directly accountable to Parliament for delivering healthcare services, they are held to account by the same regulators as NHS trusts. Roles and responsibilities for cyber-security as at September 2017 are set out in **Figure 4** on pages 22 and 23. In particular:

- NHS Improvement holds trusts and NHS foundation trusts to account for delivering value for money; and
- the Care Quality Commission (CQC) regulates health and social care providers for safety and quality of their services.

3.2 Both bodies can mandate local NHS organisations to improve their performance. They also have a role in ensuring that local bodies have appropriate cyber-security arrangements, but neither are primarily concerned with cyber or information technology issues. NHS Digital provides guidance, alerts and support to local organisations on cyber-security, and can visit organisations to evaluate cyber-security arrangements if asked to do so, as part of CareCERT Assure.[5] However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of that organisation.

5 Prior to the WannaCry attack, NHS Digital offered an on-site inspection to hospitals to assess their cyber-security. This was known as 'CareCERT Assure' and was voluntary. NHS national bodies are currently revising this system.

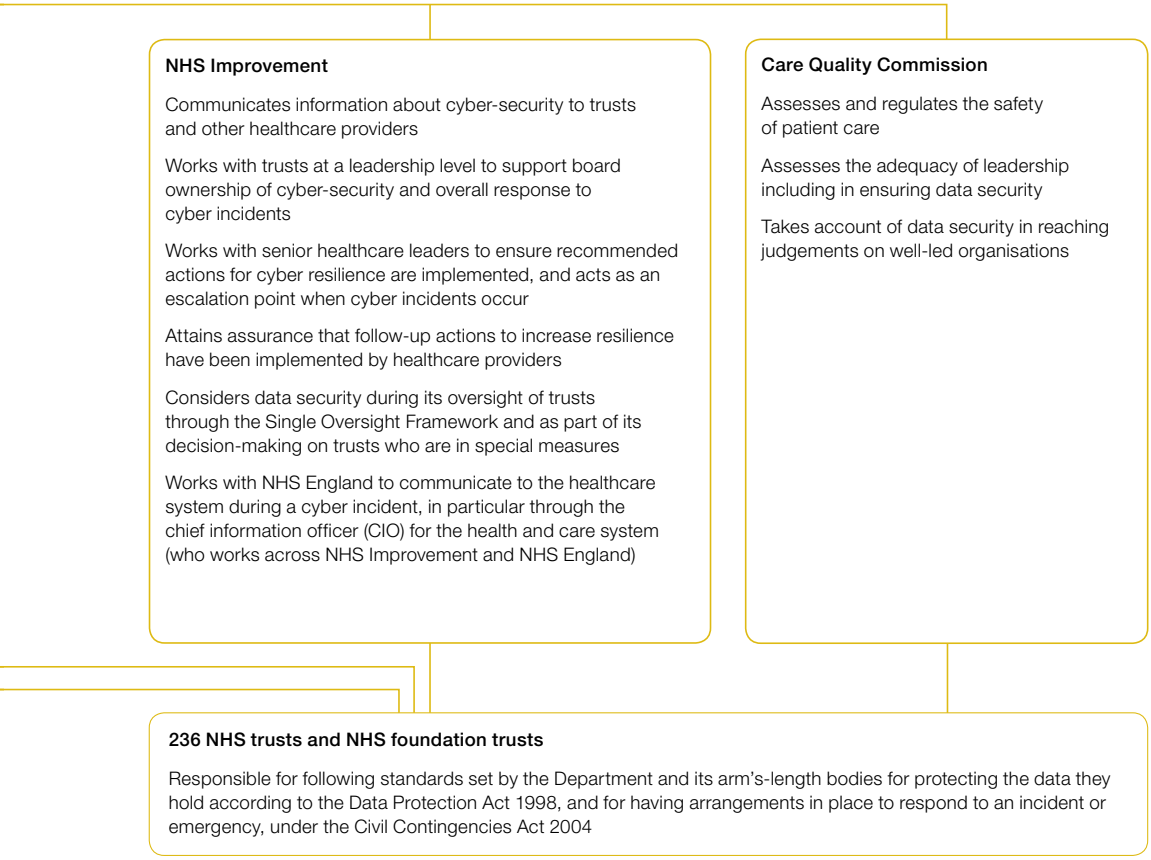
Figure 4

Roles and responsibilities for cyber-security in the NHS as at September 2017

National and local bodies share responsibility for cyber-security in the health sector



Source: National Audit Office analysis of Department of Health and NHS England data


NHS Improvement
Communicates information about cyber-security to trusts and other healthcare providers
Works with trusts at a leadership level to support board ownership of cyber-security and overall response to cyber incidents
Works with senior healthcare leaders to ensure recommended actions for cyber resilience are implemented, and acts as an escalation point when cyber incidents occur
Attains assurance that follow-up actions to increase resilience have been implemented by healthcare providers
Considers data security during its oversight of trusts through the Single Oversight Framework and as part of its decision-making on trusts who are in special measures
Works with NHS England to communicate to the healthcare system during a cyber incident, in particular through the chief information officer (CIO) for the health and care system (who works across NHS Improvement and NHS England)
Care Quality Commission
Assesses and regulates the safety of patient care
Assesses the adequacy of leadership including in ensuring data security
Takes account of data security in reaching judgements on well-led organisations
236 NHS trusts and NHS foundation trusts
Responsible for following standards set by the Department and its arm's-length bodies for protecting the data they hold according to the Data Protection Act 1998, and for having arrangements in place to respond to an incident or emergency, under the Civil Contingencies Act 2004

How the cyber attack was managed

3.3 Before the WannaCry attack the Department had developed a plan for responding to a cyber attack, which included roles and responsibilities of national and local organisations. However, the Department had not tested the plan at a local level. This meant the NHS was not clear what actions it should take when affected by WannaCry, including how it should respond at a local level. On 12 May 2017, NHS England determined that it should declare a national major incident and decided that it would lead the response, coordinating with NHS Digital and NHS Improvement. NHS England treated the attack as a major operational incident through its existing Emergency Preparedness, Resilience and Response (EPRR) processes. However, as NHS England had not rehearsed its response to a cyber attack it faced a number of challenges. The cyber attack was less visible than other types of incident and not confined to local areas or regions in the way a major transport accident would have been, for example. This meant that it took more time to determine the cause of the problem, the scale of the problem and the number of people and organisations affected.

3.4 Without clear guidelines on responding to a national cyber attack, organisations reported the attack to different sources including the local police, NHS England and NHS Digital. For the same reason communications to patients and local organisations also came from a number of sources. These included the National Cyber Security Centre, which was providing support to all UK organisations affected by the attack, NHS England and NHS Digital. In addition, the use of email for communication was limited, although NHS Improvement did communicate with trusts' chief executive officers by telephone. Affected trusts shut down IT systems, including some trusts disconnecting from NHS email and the N3 network as a precautionary measure.[6] The Department coordinated the response with the centre of government, briefing ministers, liaising with the National Cyber Security Centre and National Crime Agency, and overseeing NHS England's and NHS Digital's operational response.

3.5 Affected trusts were triaged through the EPRR route and, where necessary, received assistance from national bodies, including advice and physical technical support from NHS Digital, which sent 54 staff out to hospitals to provide direct support. Staff at the Department, NHS England, NHS Improvement and NHS Digital, as well as large numbers of staff in other organisations across the NHS, worked through the weekend to resolve the problem and avoid further problems on Monday. NHS England's IT team did not have on-call arrangements in place, but staff came in voluntarily to help resolve the issue. Front-line NHS staff adapted to communication challenges and shared information through personal mobile devices, including using the encrypted WhatsApp application. NHS national bodies and trusts told us that this worked well on the day although is not an official communication channel.

6 N3 is the broadband network connecting all NHS sites in England.

The risk of a cyber attack had been identified before WannaCry

3.6 The Secretary of State for Health asked the National Data Guardian and CQC to undertake reviews of data security. These reports were published in July 2016 and warned the Department about the cyber threat and the need for the Department to respond to it. They noted the threat of cyber attacks not only put patient information at risk of loss or compromise but also jeopardised access to critical patient record systems by clinicians. They recommended that all health and care organisations needed to provide evidence that they were taking action to improve cyber-security, such as through the 'Cyber Essentials' scheme.[7]

3.7 Although WannaCry was the largest cyber-security incident to affect the NHS, individual NHS organisations had been victims of other attacks in recent years (**Figure 5** overleaf). WannaCry infected one of England's biggest trusts, Barts Health NHS Trust. This was the second cyber attack to affect the trust in six months. A ransomware attack had also affected Northern Lincolnshire and Goole NHS Foundation Trust in October 2016, which had led to it cancelling 2,800 appointments.

Lessons learned

3.8 The NHS has accepted that there are lessons to learn from WannaCry and is already taking action. The NHS has identified the need to improve the protection of services from future cyber attacks. These include the need to:

- develop a response plan setting out what the NHS should do in the event of a cyber attack and establish the roles and responsibilities of local and national NHS bodies and the Department;
- ensure organisations implement critical CareCERT alerts, including applying software patches and keeping anti-virus software up to date;
- ensure essential communications are getting through during an incident when systems are down; and
- ensure that organisations, boards and their staff are taking the cyber threat seriously, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise the impact on patient care.

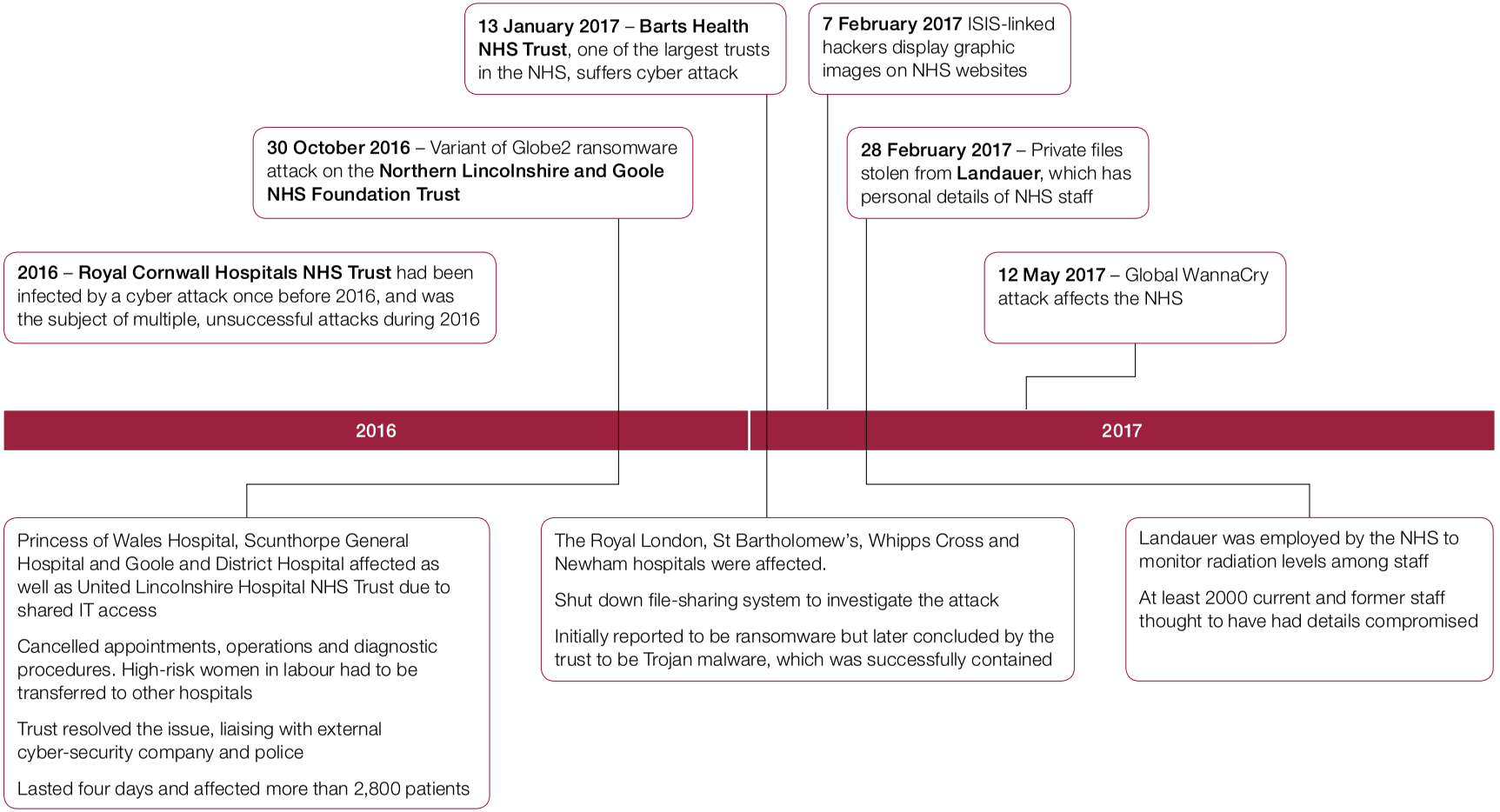
3.9 Following the WannaCry attack, NHS England and NHS Improvement wrote to every trust, clinical commissioning group and commissioning support unit asking boards to ensure that they had implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and had taken essential action to secure local firewalls.

7 Cyber Essentials is a government-designed cyber-security certification scheme that sets out a baseline of cyber-security and can be used by any organisation in any sector, see: www.cyberaware.gov.uk/cyberessentials/

Figure 5

Cyber attacks on the NHS in 2016 and 2017 before 12 May 2017

The NHS had experienced a number of cyber attacks prior to the WannaCry attack



Source: National Audit Office

3.10 NHS England and NHS Improvement are talking to every major trauma centre and ambulance trust, and will reprioritise £21 million in capital funding from existing IT budgets to improve cyber-security in major trauma centres. NHS Digital has built a new CareCERT Collect portal to provide assurance that trusts have implemented cyber alerts and to collect central data on IT and digital assets in the NHS. Since 2015, the Department has made £50 million available to provide central support to the health and care system through the CareCERT suite of services.

3.11 Following the WannaCry attack, in July 2017 the Department published its response to the National Data Guardian and CQC recommendations. The response built on existing work to strengthen cyber-security in the NHS, involving the Department and its arm's-length bodies. For example, NHS Digital was developing its existing services to support local organisations, including broadcasting alerts about cyber threats, providing a hotline for dealing with incidents, sharing best practice across the health system and carrying out on-site assessments to help protect against future cyber attacks; and NHS England had embedded the 10 Data Security Standards, recommended by the National Data Guardian, in the standard NHS contract for 2017-18, and was providing training to its Board and local teams to raise awareness of cyber threats. The Department also told us that a revised version of the Information Governance Toolkit is being developed for use in 2018-19, and that the inspection framework used by the CQC will be updated to incorporate the data standards.[8]

8 The Information Governance Toolkit draws together the legal rules and central guidance issued by the Department of Health, and presents them in a single standard as a set of information governance requirements. All health and social care providers, commissioners and suppliers are required to carry out self-assessments of their compliance against these requirements. The Toolkit is commissioned by the Department and is maintained by NHS Digital. See www.igt.hscic.gov.uk/

Appendix One

Our investigative approach

Scope

1 We conducted an investigation into the WannaCry cyber attack that affected the NHS in England on 12 May 2017. We investigated:

- the WannaCry attack's impact on the NHS and its patients;
- why some parts of the NHS were affected; and
- how the Department, NHS national bodies (NHS England, NHS Digital and NHS Improvement) and other national bodies, such as the National Cyber Security Centre and National Crime Agency, responded to the incident.

Methods

2 In examining the issues in paragraph one, we drew on a variety of evidence sources.

3 We conducted semi-structured interviews with officials from:

- Department of Health
- NHS England
- NHS Digital
- NHS Improvement
- Care Quality Commission
- National Cyber Security Centre
- National Crime Agency
- Cabinet Office.

4 We visited four local trusts to examine their roles and responsibilities in relation to cyber-security; the impact of WannaCry on the trust and its patients; and how the trust responded to the incident:

- Barts Health NHS Trust;
- Bedford Hospital NHS Trust;
- Northern Lincolnshire and Goole NHS Foundation Trust; and
- the Royal Marsden NHS Foundation Trust.

5 We reviewed documents relating to the WannaCry ransomware attack including documents setting out roles and responsibilities for cyber-security in the NHS and across the wider public sector. We also reviewed published and unpublished research and reports relating to the NHS and WannaCry and cyber-security more generally.

6 We carried out analysis of data provided by NHS England, NHS Digital and the Care Quality Commission.

Appendix Two

Trusts infected or disrupted by WannaCry

Figure 6

Trusts infected, or affected, by the WannaCry attack

Trusts infected by WannaCry, and locked out of devices

Barts Health NHS Trust

Birmingham Community Healthcare NHS Foundation Trust

Blackpool Teaching Hospitals NHS Foundation Trust

Bradford District Care NHS Foundation Trust

Bridgewater Community Healthcare NHS Foundation Trust

Central Manchester University Hospitals NHS Foundation Trust

Colchester Hospital University NHS Foundation Trust

Cumbria Partnership NHS Foundation Trust

East and North Hertfordshire NHS Trust

East Cheshire NHS Trust

East Lancashire Teaching Hospitals NHS Trust

Essex Partnership University NHS Foundation Trust

George Eliot Hospital NHS Trust

Hampshire Hospitals NHS Foundation Trust

Hull and East Yorkshire Hospitals NHS Trust

Humber NHS Foundation Trust

James Paget University Hospitals NHS Foundation Trust

Lancashire Care NHS Foundation Trust

Lancashire Teaching Hospital NHS Trust

Mid Essex Hospital Services NHS Trust

North Cumbria University Hospitals NHS Trust

Northern Lincolnshire and Goole NHS Foundation Trust

Northumbria Healthcare NHS Foundation Trust

Nottinghamshire Healthcare NHS Foundation Trust

Plymouth Hospitals NHS Trust

Royal Berkshire Hospital NHS Foundation Trust

Shrewsbury and Telford Hospital NHS Trust

Solent NHS Trust

Southport and Ormskirk Hospital NHS Trust

The Dudley Group NHS Foundation Trust

United Lincolnshire Hospitals NHS Trust

University Hospitals of Morecambe Bay NHS Foundation Trust

Wrightington, Wigan and Leigh NHS Foundation Trust

York Teaching Hospitals NHS Foundation Trust

Source: NHS England

Trusts not infected by WannaCry but known to have experienced disruption

Airedale NHS Foundation Trust

Ashford and St Peters Hospitals NHS Foundation Trust

Barking, Havering and Redbridge University Hospitals NHS Trust

Barnsley Hospital NHS Foundation Trust

Bedford Hospital NHS Trust

Bradford Teaching Hospitals NHS Foundation Trust

Brighton and Sussex University Hospitals NHS Trust

Buckinghamshire Healthcare NHS Foundation Trust

Calderdale and Huddersfield NHS Foundation Trust

Central London Community Healthcare NHS Trust

Chelsea and Westminster Hospital NHS Foundation Trust

Doncaster and Bassetlaw Hospitals NHS Foundation Trust

Dorset Healthcare NHS Foundation Trust

East Kent Hospitals University NHS Foundation Trust

Great Ormond Street Hospital NHS Foundation Trust

Greater Manchester Mental Health NHS Foundation Trust

Guy's and St Thomas' NHS Foundation Trust

Harrogate and District NHS Foundation Trust

Kettering General Hospital NHS Foundation Trust

Kingston Hospital NHS Trust

Leeds and York Partnership NHS Foundation Trust

Leeds Community Healthcare NHS Trust

Leeds Teaching Hospitals NHS Trust

Leicestershire Partnership NHS Trust

Lincolnshire Community Health Services NHS Trust

Lincolnshire Partnership NHS Trust

London North West Healthcare NHS Trust

Luton and Dunstable NHS Trust

Mid Yorkshire Hospitals NHS Trust

Moorfields Eye Hospital NHS Foundation Trust

Norfolk and Norwich University Hospital NHS Foundation Trust

North West Ambulance Service NHS Trust

Northampton General Hospital NHS Trust

Northamptonshire Healthcare NHS Foundation Trust

Rotherham, Doncaster and South Humber NHS Foundation Trust

Salford Royal NHS Foundation Trust

Sheffield Children's NHS Foundation Trust

Sheffield Health and Social Care NHS Foundation Trust

Sheffield Teaching Hospitals NHS Foundation Trust

South West Yorkshire Partnership NHS Foundation Trust

South Western Ambulance Service NHS Foundation Trust

The Rotherham NHS Foundation Trust

University Hospitals of Leicester NHS Trust

West Hertfordshire Hospitals NHS Trust

West London Mental Health NHS Trust

Yorkshire Ambulance Service NHS Trust

Source: NHS England

This report has been printed on Evolution Digital Satin and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.



National Audit Office

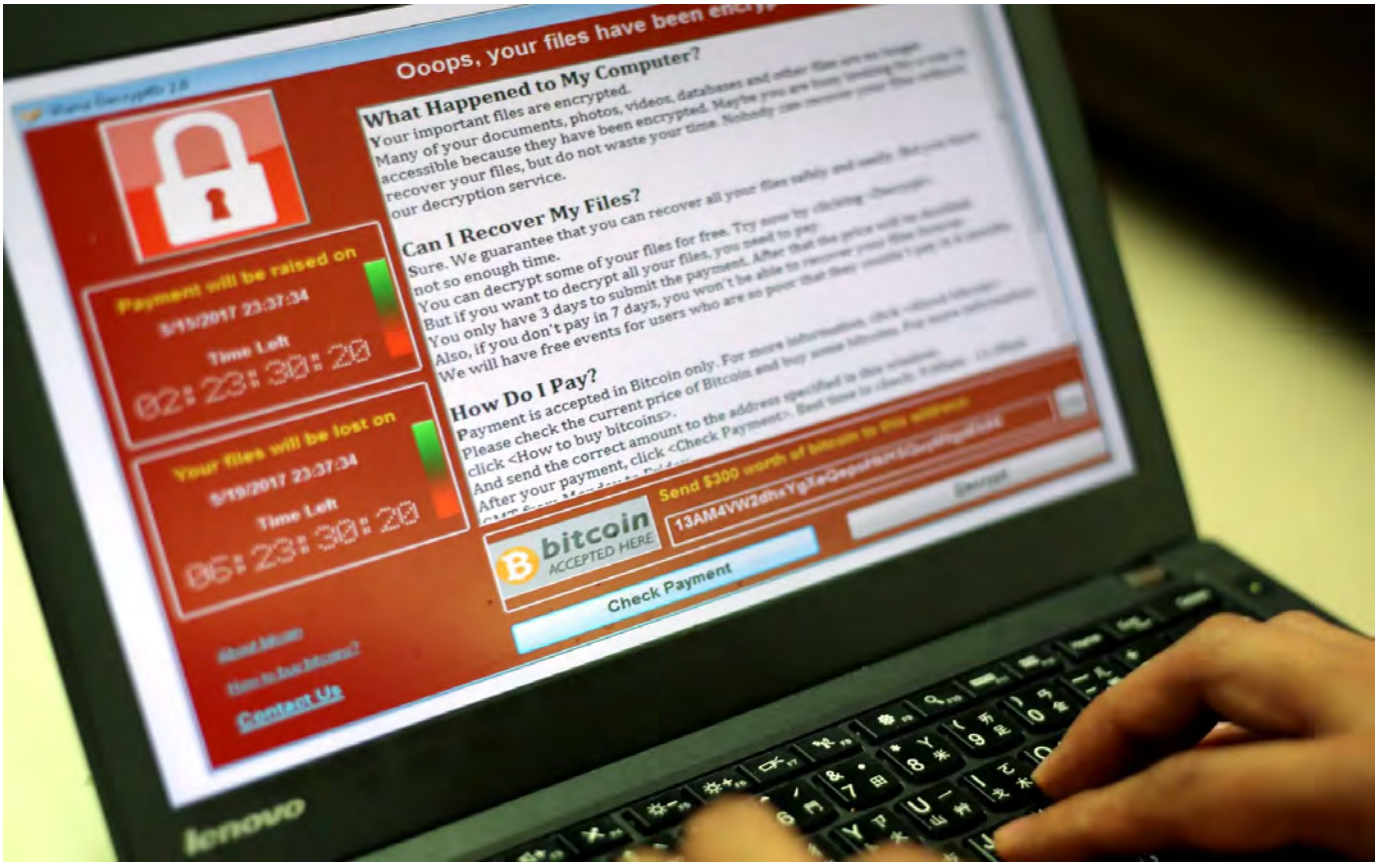
£10.00

ISBN 978-1-78604-147-0



Design and Production by NAO External Relations
DP Ref: 11594-001

NHS cyber chaos hits thousands of patients



A 'WannaCry' ransomware cyber attack hit thousands of computers in 99 countries. CREDIT: EPA

By **Patrick Sawer**, SENIOR REPORTER ; **Robert Mendick**, CHIEF REPORTER ; **Stephen Walter** and **Nicola Harley**

13 MAY 2017 • 9:50PM

Follow

Thousands of operations and other appointments will be cancelled as NHS bosses admitted it will take several weeks to fix ageing computer systems hit by Friday's cyber attack.

The NHS admitted vital equipment, such as MRI scanners and X-ray machines, have now been taken offline as they cannot be repaired immediately.

Thousands of NHS staff are now bracing themselves for further problems (https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/)when they arrive at work on Monday and attempt to log onto their computer terminals.

Staff have been reduced to reverting to pen and paper and ferrying messages around hospital using runners, according to NHS England sources – despite ministers insisting things had returned to normal.

Senior sources told the Telegraph that as many as "tens of thousands" of procedures could be "disrupted" and many thousands of appointments cancelled.

Senior British Medical Association sources said they did not recognise the picture painted by the Government.

Dr Mark Porter, the BMA council chairman, said the attack was "extremely worrying" and that a lack of investment in computer security may have left the NHS vulnerable.

Lister Hospital Stevenage tells patients it has been hacked. CREDIT: FIONA HANSON

In May 2015, the Government ended its annual £5.5 million deal with Microsoft to provide ongoing security support for Windows XP.

Norman Lamb, the Liberal Democrats' health spokesman and former minister, said: "This is potentially the worst NHS crisis for decades. It is going to take some time before the full scale of this becomes clear."

NHS Digital admitted it would take several weeks to restore some key equipment, such as MRI scanners, which run on the affected Windows XP programme.

It said: "Some expensive hardware (such as MRI scanners) cannot be updated immediately, and in such instances organisations will take steps to mitigate any risk, such as by isolating the device from the main network."

MalwareTech has plotted the countries affected by the hack

Some 48 health service organisations in England and Scotland – almost a fifth of the NHS – were infiltrated (https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/) by Friday's ransomware attack, leaving dozens of hospitals and GP surgeries with a backlog of appointments.

On Saturday the country's biggest NHS trust said it had cancelled all non-urgent appointments on Saturday and more would be cancelled on Sunday. Ambulances were being diverted to neighbouring hospitals and Barts – which serves 2.5 million people – had activated its major incident plan.

There were also questions over the failure of both Jeremy Hunt, the Health Secretary, and Simon Stevens, the NHS's chief executive, to appear during the crisis. Instead the

NHS's director of operations, Anne Rainsberry, was left to explain its response.

Amber Rudd, the Home Secretary, insisted that the NHS was coping. Writing exclusively for the Telegraph, she warns that Britain should be braced for future hacking attacks on an even greater scale in the future. The cyber attack has now spread to more than 100 countries, including Germany, France, Spain, the US and China, infecting more than 130,000 IT systems.

A woman points to the website of the NHS: East and North Hertfordshire notifying users of a problem in its network. CREDIT: AFP

British intelligence agencies have been drawn into the international hunt for the masterminds behind the biggest cyber attack in history.

Security services said analysts from the three main spy agencies – MI5, MI6 and GCHQ – were being deployed in the search for those responsible.

It also emerged that the spread of the virus was slowed at 7pm on Friday, when a young British cyber expert discovered and accidentally activated a "kill switch" hidden in the software code.

The Government said that by Saturday afternoon of the 48 trusts which were affected, all bar six were now running a "normal service" and every A&E in England was operating as normal.

However, a senior NHS source admitted that there would still be cancellations of non-urgent operations at a number of trusts.

“This will still affect hundreds of people. There will be cancellations. This is not a good thing,” said the source. But it is not a crisis. The NHS has coped.

“In more than 200 trusts engineers went in to ensure patches to counter this malware were put in place or were already in place.”

The cyber attack took down the computer systems at Blackpool Victoria. CREDIT: WARREN SMITH

On top of any postponement to treatment trusts still face weeks of administrative delays as systems engineers get computers back online following the attack.

NHS England was last night refusing to say how many patients would be affected by delays over the coming days, but on any given day the health service deals with 31,000 non-emergency operations, 61,000 attendances at A&E, 750 people starting treatment for cancer and 8,600 emergency ambulance journeys.

Computer security experts said it could take weeks for the NHS to unlock or replace every computer systems that were frozen by the virus attack.

It emerged on Saturday that one in 20 of the NHS's thousands of computers – five per cent of the total – are still fitted with the Windows XP programme susceptible to the virus used in Friday's attack.

Sean Sullivan, security adviser to F-Secure, an international cyber security company, said: "This is going to be a real problem for the NHS for months.

"You can expect a lot of cancelled operations in the course of the next week at least. We can expect cancelled operations for quite some time.

"The NHS will have to have systems up and running to handle critical patients straight away but non-critical stuff will take a long time to clear up."

While ministers tried to reassure the public that patient data had not been compromised and lives were not at risk, stories have begun to emerge of clinical staff being unable to do their jobs.

Contact us

About us (https://corporate.telegraph.co.uk/)

Rewards

Archive (https://www.telegraph.co.uk/archive/)

Reader Prints (http://telegraph.newsprints.co.uk/)

Branded Content

Syndication and Commissioning

Guidelines

Privacy

Terms and Conditions

Advertising terms (http://spark.telegraph.co.uk/toolkit/advertising/terms-and-conditions/)

Fantasy Sport (https://fantasyfootball.telegraph.co.uk)

Black Friday

LAWFARE

CYBERSECURITY

Hackers Leaked Sensitive Government Data in Argentina—and Nobody Cares

By **Eugenia Lostri** Wednesday, August 21, 2019, 9:00 AM

DayZero: Cybersecurity Law and Policy

On Monday, Aug. 12, hackers leaked 700 GB of data obtained from the government of Argentina, including confidential documents, wiretaps and biometric information from the Argentine Federal Police, along with the personal data of police officers. The Twitter account of the Argentine Naval Prefecture was hacked as well, and used not only to share links to the stolen information but also to spread fake news about a nonexistent British attack on Argentine ships.

An operation combining the hacking of law enforcement agencies, an attempt to spread misinformation through social media and the leaking of large amounts of sensitive data on the "Deep Web" would seem to check all the boxes for a major news story. But you most likely have not heard about any of this.

The relative lack of media coverage about the hack is not actually surprising, considering the news dominating the discussion about Argentina this past week. Primary elections were held on Aug. 11, the night before the leak. Due to heavy polarization, most predicted that the election would be a tight race between the current president, Mauricio Macri, and his challengers, Alberto Fernandez and former President Cristina Fernandez de Kirchner (the latter running as Fernandez's vice-presidential pick). By the end of the night, however, the opposition ticket had claimed a landslide victory: Macri received 32 percent of the vote, compared to the 47 percent boasted by the opposition. This past election does not formally change anything for either party. The purpose of the primaries is to filter out low-polling candidates and to settle internal primaries, and the general elections in October will see the same candidates face each other again. But the results signal that October will likely bring Kirchner back to power. While it is unclear whether Alberto Fernandez's economic plan would mark a return to the populist measures that characterized Kirchner's administration, the market's reaction to these results was chaotic. On Aug. 12, Argentine bonds and stocks plunged, the value for the Argentine peso dropped sharply and companies lost $18.144 million in a day. Throughout the week, the political and economic aftermath of the election was what most Argentinians had on their minds.

In the midst of the ensuing turmoil, it is understandable that not much attention was initially paid to the short-lived hack of the Naval Prefecture Twitter account. However, allowing the story to fade in the background would be a disservice. What happened on Aug. 12 in Argentina not only has implications for the country's own security but also serves as another data point for the ongoing discussion about how hacking and leaking operations should be understood and addressed.

On the night of Aug. 11, a public Telegram chat group appeared. A Twitter account would soon be compromised, the group's founders announced. By noon on Aug. 12, it became clear what the message was referring to: The official Twitter account of the Argentine Naval Prefecture began posting a sequence of disconcerting messages, evidence that it had been hacked. The hackers had around 10 minutes to publish several tweets before the government regained control over the account; one of them shared some of the "LaGorraLeaks" ("La Gorra" is an Argentinian term used to refer to the police), a set of links that allegedly contained police officers' personal data along with wiretaps, biometric information and classified documents, among other information. Another concerning message falsely informed the public about a British attack on Argentine ships.

"LaGorraLeaks" is the handle for the Twitter account that made the hacked documents known. And this is not their first rodeo. Back in 2017, the profile claimed to have hacked into the Argentine security minister's account—although the consequences of such action were limited to posting unflattering messages about the minister. A few months later, the same profile leaked emails with information regarding the Organized Crime Division of the Argentine police. On Aug. 12, 2019, the account was busy retweeting news reports about its hack and sharing links to leaked data. A pinned tweet made public "#LaGorraLeaks2.0." The user or users, who go by "[S]," claimed to have published 700 GB of information to the "Deep Web"—which, they assured, contained sensitive data relating to the Argentine Federal Police and the Buenos Aires City Police. It is worth pointing out that it is most likely that the hacker was actually referring to what is usually known as the "dark web," the portion of the web accessible only through anonymizing tools; the dark web is contained within the deep web, referring to content not indexed by search engines.

The account has now been suspended, but this has not deterred the group. A new Telegram public group was set up and further menacing texts sent out, hinting at future activity. Its founders posted obscure references to how "September will have a very amusing start," argued that banking institutions are taking advantage of the state of the country and hinted at the preparation of something "very large" set to affect Argentina's cybersecurity as never seen before. The chat also seemed to work as a recruiting

space, where the self-described "Team" announced it was looking for people with specific capabilities and informed those reading the channel about a selection process to participate in the project. Whether this is actually an established organization or just banter among hackers is not clear.

On Aug. 12, the stolen data was shared both through [S]'s twitter account and the Naval Prefecture's profile, although it has not been confirmed whether the hacks and the leak were carried out by the same person or organization. Even as of now, there does not seem to be a consensus regarding how precisely the leak of information occurred—some have even suggested that the whole thing might have been an inside job, rather than an actual exploitation of security vulnerabilities. A spokesperson for the Federal Police assured the press that the organization's database has not been compromised; the data accessed was in the cloud, uploaded by what the spokesman vaguely called "peripheral dependencies." There also seems to be some confusion about the relevance of the leaked information. Some news outlets reported that confidential information regarding ongoing investigations is now public, with some of the leaked information dated as recently as a month ago; others wrote that the hackers are publishing old data. Authorities from the Buenos Aires City Police, however, have denied that their databases were breached.

Local media was able to establish contact with the alleged hacker via email. Whoever was behind the screen responded under the alias Nicolái Lobachevski—the name of a 19th century Russian mathematician—and provided his side of the story. In terms of the methodology used to access the stolen data, "Lobachevski" replied that the process had taken months of silently accessing the police's network, relying partly on his own knowledge and abilities and partly on the naivete of police agents and employees. Further, he assured that he is the same hacker from 2017 and claimed responsibility for the hacks both past and present. Finally, the hacker dismissed the chances of being caught, arguing that there was no risk and no margin of error.

"Lobachevski"/[S] claims that the intent behind his actions was to demonstrate the security flaws in the system and was motivated by the technical challenge it presented. This seems consistent with some of the content posted in his now-suspended account. Prior to the bulk of the leak, messages on the Twitter account made calls for the government to improve its security and even mentioned the possibility of reporting security vulnerabilities to the Security Ministry before brushing the idea aside.

Both the Federal Police and the Naval Prefecture have informed the press that there are already investigations underway to figure out what occurred, and that judicial procedures have been initiated.

These events should bring attention to three sets of concerns. First, the hacking and leaking of sensitive information could endanger the safety of law enforcement agents and affect the Argentine national security strategy. Second, the events provide an opportunity to explore the consequences of fake news being published through trusted channels such as official social media accounts of government institutions and authorities. Lastly, events of this nature should push forward the conversation about digital literacy and the portrayal of such issues in the media.

In the exchange between "Lobachevski" and the press, reporters raised the question of the risk that this leak poses for law enforcement—though the issue seemed to hold little significance for the alleged hacker. After acknowledging that the release of the data had created risks for these people, he went on to say that he did not care given that he does not like the police. In fact, the website hosting the leaked information also contained a manifesto proclaiming the oppressive nature of the police force and declaring that it should no longer exist.

The 700 GB leak contains an extensive list of data, allegedly including confidential documents, wiretaps, scanned documents, biometric information and files with personal information of police officers and their families. The scope and extent of the information that is now accessible presents serious security concerns, both for the country's ability to conduct security operations and for the safety of the agents themselves. Local press reported that, indeed, files on 70 police officers comprised some of the leaked information, including the officers' personal phone numbers, their addresses and the names of their partners and children. This breach of privacy exposes the officers to targeted attacks from both criminal organizations or reprisals for their work from those who do not like the police.

The fact that someone accessed and published such a great amount of information is in itself a grave concern. But there is a different threat to be considered as well, related to the proliferation of fake news.

The tweets sent out by the hacked Naval Prefecture account were more than just a way of informing the public about the leaked data or insulting law enforcement agencies. Before the government regained control over the account, the hackers posted that three Argentine ships had been attacked by British missiles, that Argentina had successfully responded to the breach of the country's territory and that the president was on his way. They also stated that 27 officers had died.

To be fair, the tweet was not public for long, because authorities resumed their control over the account relatively quickly. It also doesn't hurt that the Argentine Naval Prefecture's account, with less than 100,000 Twitter followers, could hardly boast of a following that could make such a tweet have an impact. And it was hardly the intention of whoever was managing the account at that point to set in motion a proper misinformation campaign destined to wreak havoc—between the links to the data and the foul

references to the security minister, the posts were clearly a result of the hacker's activity rather than a convincing imitation of the Naval Prefecture. Nevertheless, the use of an authoritative channel to spread fake news over an issue as sensitive as a British attack on Argentina raises the possibility that a more carefully and well executed campaign with that purpose could be conducted.

The Naval Prefecture's Twitter account reportedly did not have two-factor authentication, aiding in the hacker's ability to gain access. If social media accounts belonging to other governmental agencies or even political figures also lack such security measures, the possibilities for exploitation are high. Recall that in 2013, a week after the Boston marathon bombing, a fake AP tweet claiming that an explosion at the White House had injured then-President Obama briefly caused a stock market crash. The use of trusted profiles to spread misinformation could have far-reaching effects, particularly during a delicate time. This does not, of course, mean that a malicious tweet will cause war or the collapse of society. But this kind of misinformation is a tool that can be exploited by those with bad intentions.

There are a range of pressing issues that rank higher in Argentina than the hacking of the Naval Prefecture's Twitter. However, it is telling how the hack and leak were reported and discussed. A first group of reports basically replicated each other, providing a brief description of the facts and attaching several screenshots of both the hacked accounts and [S]'s own Twitter account. Most also included a superficial explanation of the "Deep Web." Those reporters who put in the extra work provided a line describing the TOR browser, needed to access the leaked data.

Subsequently, there has been further reporting and explanation on the hacking and leaking, with outlets reaching out to security experts and unnamed sources within the government in order to paint a more detailed picture of what happened. Regardless, the considerations presented, at least on the public record, have barely scratched the surface of the national security concerns that should be taken into account now that sensitive information is available. Nor has there been any conversation about the infrastructure vulnerabilities that allowed this to happen in the first place.

Given that investigations into the hack are ongoing, it may be too early to assign blame for this particular incident. But many different elements contributed to this situation. On the one hand, according to "Lobachevski," accessing the Federal Police's database took months; this signals some level of proper cyber protection. How exactly did this breach happen, and how was a months-long intrusion not detected? Comparatively, hacking the Naval Prefecture's Twitter was no problem at all, if the media reports on the account's low security settings are accurate. Simple fixes such as establishing two-factor authentication and password protocols could go a long way if implemented in a systematic and institutionalized fashion across Argentine government agencies.

Ultimately, this is not only a question of improving technical cybersecurity in some areas. After all, governments across the world struggle with similar issues—even those that can boast of advanced defenses. What should cause concern in this case is the apathetic response with which these events were met. If 700 GB of government information can be leaked without any response or outcry—not even the beginnings of a conversation on cybersecurity—this is indicative of an underlying problem. Not much can be fixed if no one cares.

Topics: Cybersecurity

Tags: Latin America, hacking, data breach, leaks

Eugenia Lostri recently earned an LLM in International Law from The Fletcher School of Law and Diplomacy, and holds a First Degree in Law from the Pontifical Catholic University of Argentina. She is the Tufts Cybersecurity Policy Summer Fellow at Lawfare.

The Intercept_

THE NSA AND GCHQ CAMPAIGN AGAINST GERMAN SATELLITE COMPANIES

Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer, Christian Grothoff

September 14 2014, 11:00 a.m.



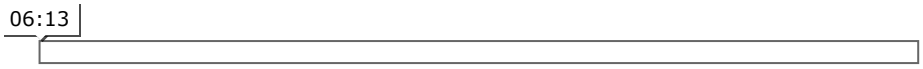
“Fuck!” That is the word that comes to the mind of Christian Steffen, the CEO of German satellite communications company Stellar PCS. He is looking at classified documents laying out the scope of something called Treasure Map, a top secret NSA program. Steffen’s firm provides internet access to remote portions of the globe via satellite, and what he is looking at tells him that the company, and some of its customers, have been penetrated by the U.S. National Security Agency and British spy agency GCHQ.

385

Stellar's visibly shaken chief engineer, reviewing the same documents, shares his boss' reaction. "The intelligence services could use this data to shut down the internet in entire African countries that are provided access via our satellite connections," he says.

Treasure Map is a vast NSA campaign to map the global internet. The program doesn't just seek to chart data flows in large traffic channels, such as telecommunications cables. Rather, it seeks to identify and locate every single device that is connected to the internet somewhere in the world – every smartphone, tablet, and computer – "anywhere, all the time," according to NSA documents. Its internal logo depicts a skull superimposed onto a compass, the eyeholes glowing demonic red.

The breathtaking mission is described in a document from the archive of NSA whistleblower Edward Snowden provided to *The Intercept* and *Der Spiegel*. Treasure Map's goal is to create an "interactive map of the global internet" in "almost real time." Employees of the so-called "Five Eyes" intelligence alliance – England, Canada, Australia, and New Zealand – can install and use the program on their own computers. It evokes a kind of Google Earth for global data traffic, a bird's eye view of the planet's digital arteries.



(The short film above, *Chokepoint*, by filmmaker Katy Scoggin and *Intercept* co-founder Laura Poitras, documents the reactions of Stellar engineers when confronted with evidence that their company – and they themselves – had been surveilled by GCHQ.)

The New York Times reported on the existence of Treasure Map last November. Though the NSA documents indicate that it can be used to monitor "adversaries," and for "computer attack/exploit planning" – offering a kind of battlefield map for cyber warfare – they also clearly show that Treasure Map monitors traffic and devices inside the United States. Unnamed intelligence officials told the *Times* that the program didn't have the capacity to monitor *all* internet-connected devices, and was focused on foreign networks, as well as the U.S. Defense Department's own computer systems.

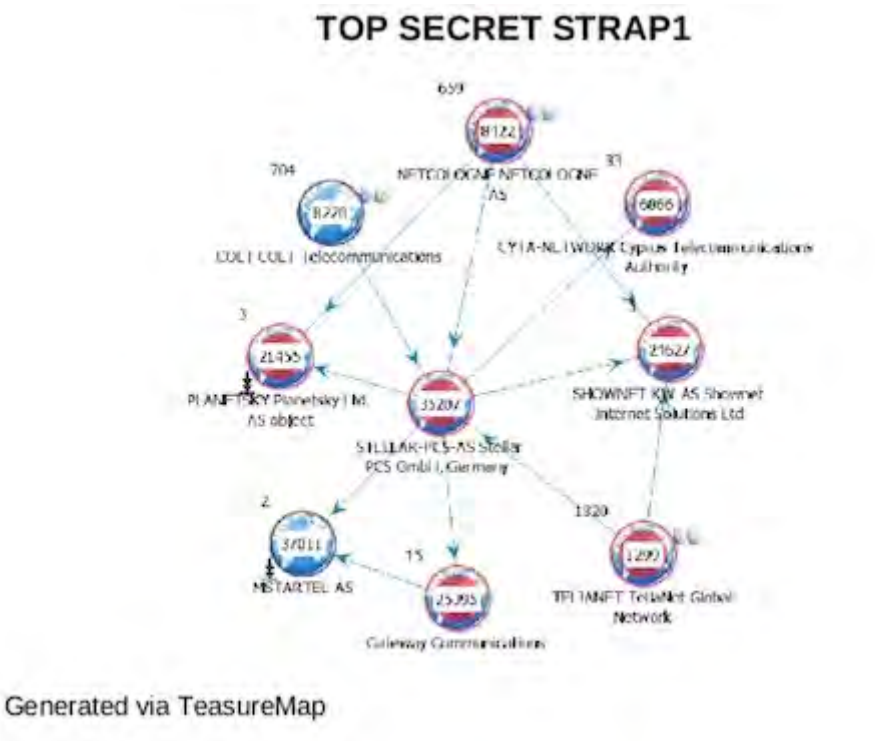


A slide from an NSA presentation explaining Treasure Map

The Treasure Map graphics contained in the Snowden archive don't just provide detailed views of global networks – they also note which carriers and internal service provider networks Five Eyes agencies

claim to have already penetrated. In graphics generated by the program, some of the "autonomous systems" – basically, networks of routers all controlled by one company, referred to by the shorthand "AS" – under Treasure Map's watchful eye are marked in red. An NSA legend explains what that means: "Within these AS, there are access points for technical monitoring." In other words, they are under observation.

In one GCHQ document, an AS belonging to Stellar PCS is marked in red, as are networks that belong to two other German firms, Deutsche Telekom AG and Netcologne, which operates a fiber-optic network and provides telephone and internet services to 400,000 customers.



A Treasure Map image from a GCHQ document shows Stellar PCS and other companies marked red, meaning their networks have been penetrated

Deutsche Telekom, of which the German government owns more than 30 percent, is one of the dozen or so international telecommunications companies that operate global networks – so-called Tier 1 providers. In Germany alone, Deutsche Telekom claims

to provide mobile phone services, internet, and land lines to 60 million customers.

It's not clear from the documents how or where the NSA gained access to the networks. Deutsche Telekom's autonomous system, marked in red, includes several thousand routers worldwide. It has operations in the U.S. and England, and is part of a consortium that operates the TAT14 transatlantic cable system, which stretches from England to the east coast of the U.S. "The accessing of our network by foreign intelligence agencies," said a Telekom spokesperson, "would be completely unacceptable."

The fact that Netcologne is a regional provider, with no international operations, would seem to indicate that the NSA or one of its partners accessed the network from within Germany. If so, that would be a violation of German law and potentially another NSA-related case for German prosecutors, who have been investigating the monitoring of Chancellor Angela Merkel's mobile phone.

Reporters for *Der Spiegel*, working in collaboration with *The Intercept,* contacted both companies several weeks ago in order to give them an opportunity to look into the alleged security breaches themselves. The security departments of both firms say they launched intensive investigations, but failed to find any suspicious equipment or data streams leaving the network. The NSA declined to comment for this story, and GCHQ offered no response beyond its boilerplate claim that all its activities are lawful.

Deutsche Telekom and Netcologne are not the first German companies to be pinpointed by Snowden documents as having been successfully hacked by intelligence agencies. In March, *Der Spiegel* reported on a large-scale attack by GCHQ on German satellite operators Stellar, Cetel, and IABG, all of which offer satellite internet connections to remote regions of the world. All three companies operate their own autonomous systems. And all three are marked red in Treasure Map graphics.

Der Spiegel also contacted 11 of the international providers listed in the Treasure Map document. Four answered, all saying they examined their systems and were unable to find any irregularities. “We would be extremely concerned if a foreign government were to seek unauthorized access to our global networks and infrastructure,” said a spokesperson for the Australian telecommunications company Telstra.

The case of Stellar illustrates the lengths to which GCHG and NSA have gone in making their secret map of the internet, and its users.

One document, from GCHQ’s Network Analysis Center, lays out what appears to be an attack on Stellar. The document lists “central employees” at the company, and states that they should be identified and “tasked.” To “task” somebody, in signals intelligence jargon, is to engage in electronic surveillance. In addition to Stellar CEO Christian Steffen, nine other employees are named in the document.

The attack on Stellar has notable similarities with the GCHQ surveillance operation targeting the Belgian provider Belgacom, which *Der Spiegel* reported last year. There too, the GCHQ Network Analysis department penetrated deeply into the Belgacom network and that of its subsidiary BICS by hacking employee computers. They then prepared routers for cyber attacks.

Der Spiegel reporters visited Stellar at its headquarters in Hürth, near Cologne, and presented the documents to Steffen and three of his “tasked” employees. They were able to recognize, among other things, a listing for their central server as well as the company’s mail server, which the GCHQ attackers appear to have hacked.

The document also lays out the intelligence gathered from the spying efforts, including an internal table that shows which Stellar customers are being served by which specific satellite transponders. “Those are business secrets and sensitive information,” said Stellar’s

visibly shocked IT chief, Ali Fares, who is himself cited in the document as an employee to be "tasked."

The Stellar officials expressed alarm when they saw the password for the central server of an important customer. The significance of the theft is immense, Fares said. "This is really disturbing."

Steffen, after spitting out his four-letter assessment, said he considers the documents to constitute proof that his company's systems were breached illegally. "The hacked server has always stood behind our company's own firewall," he said. "The only way of accessing it is if you first successfully break into our network." The company in question is no longer a customer with Stellar.

When asked if there are any reasons that would prompt England, a European Union partner country, to take such an aggressive approach to Stellar, Steffen shrugged his shoulders, perplexed. "Our customer traffic doesn't run across conventional fiber optic lines," he said. "In the eyes of intelligence services, we are apparently seen as difficult to access." Still, he said, "that doesn't give anyone the right to break in."

"A cyber attack of this nature is a clear criminal offense under German law," he continued. "I want to know why we were a target and exactly how the attack against us was conducted – if for no other reason than to be able to protect myself and my customers from this happening again." Steffen wrote a letter to the British ambassador in Berlin asking for an explanation, but says he never received an answer.

Meanwhile, Deutsche Telekom's security division has conducted a forensic review of important routers in Germany, but has yet to detect anything. Volker Tschersich, who heads the security division, says it's possible the red dots in Treasure Map can be explained as access to the TAT14 cable, in which Telekom occupies a frequency band in England and the U.S. At the end of last week, the company

informed Germany's Federal Office for Information Security of the findings of *Der Speigel*'s reporting.

The classified documents also indicate that other data from Germany contributes to keeping the global treasure map up to date. Of the 13 servers the NSA operates around the world in order to track current data flows on the open Internet, one is located somewhere in Germany.

Like the other servers, this one, which feeds data into the secret NSA network, is "covered" in an inconspicuous "data center."

WAIT! BEFORE YOU GO about your day, ask yourself: How likely is it that the story you just read would have been produced by a different news outlet if The Intercept hadn't done it?

Consider what the world of media would look like without The Intercept. Who would hold party elites accountable to the values they proclaim to have? How many covert wars, miscarriages of justice, and dystopian technologies would remain hidden if our reporters weren't on the beat?

The kind of reporting we do is essential to democracy, but it is not easy, cheap, or profitable. The Intercept is an independent nonprofit news outlet. We don't have ads, so we depend on our members — 35,000 and counting — to help us hold the powerful to account. Joining is simple and doesn't need to cost a lot: You can become a sustaining member for as little as $3 or $5 a month. That's all it takes to support the journalism you rely on.

Become a Member →

The Intercept_

THE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO

Ryan Gallagher

December 13 2014, 6:26 a.m.



When the incoming emails stopped arriving, it seemed innocuous at first. But it would eventually become clear that this was no routine technical problem. Inside a row of gray office buildings in Brussels, a major hacking attack was in progress. And the perpetrators were British government spies.

It was in the summer of 2012 that the anomalies were initially detected by employees at Belgium's largest telecommunications provider, Belgacom. But it wasn't until a year later, in June 2013, that

the company's security experts were able to figure out what was going on. The computer systems of Belgacom had been infected with a highly sophisticated malware, and it was disguising itself as legitimate Microsoft software while quietly stealing data.

Last year, documents from National Security Agency whistleblower Edward Snowden confirmed that British surveillance agency Government Communications Headquarters was behind the attack, codenamed Operation Socialist. And in November, *The Intercept* revealed that the malware found on Belgacom's systems was one of the most advanced spy tools ever identified by security researchers, who named it "Regin."

The full story about GCHQ's infiltration of Belgacom, however, has never been told. Key details about the attack have remained shrouded in mystery – and the scope of the attack unclear.

Now, in partnership with Dutch and Belgian newspapers *NRC Handelsblad* and *De Standaard*, *The Intercept* has pieced together the first full reconstruction of events that took place before, during, and after the secret GCHQ hacking operation.

Based on new documents from the Snowden archive and interviews with sources familiar with the malware investigation at Belgacom, *The Intercept* and its partners have established that the attack on Belgacom was more aggressive and far-reaching than previously thought. It occurred in stages between 2010 and 2011, each time penetrating deeper into Belgacom's systems, eventually compromising the very core of the company's networks.

"a breathtaking example of the state-sponsored hacking problem."

Snowden told *The Intercept* that the latest revelations amounted to unprecedented "smoking-gun attribution for a governmental cyber attack against critical infrastructure."

The Belgacom hack, he said, is the "first documented example to show one EU member state mounting a cyber attack on another…a breathtaking example of the scale of the state-sponsored hacking problem."

Publicly, Belgacom has played down the extent of the compromise, insisting that only its internal systems were breached and that customers' data was never found to have been at risk. But secret GCHQ documents show the agency gained access far beyond Belgacom's internal employee computers and was able to grab encrypted and unencrypted streams of private communications handled by the company.

Belgacom invested several million dollars in its efforts to clean-up its systems and beef-up its security after the attack. However, *The Intercept* has learned that sources familiar with the malware investigation at the company are uncomfortable with how the clean-up operation was handled – and they believe parts of the GCHQ malware were never fully removed.

The revelations about the scope of the hacking operation will likely alarm Belgacom's customers across the world. The company operates a large number of data links internationally (see interactive map below), and it serves millions of people across Europe as well as officials from top institutions including the European Commission, the European Parliament, and the European Council. The new details will also be closely scrutinized by a federal prosecutor in Belgium, who is currently carrying out a criminal investigation into the attack on the company.

Sophia in 't Veld, a Dutch politician who chaired the European Parliament's recent inquiry into mass surveillance exposed by

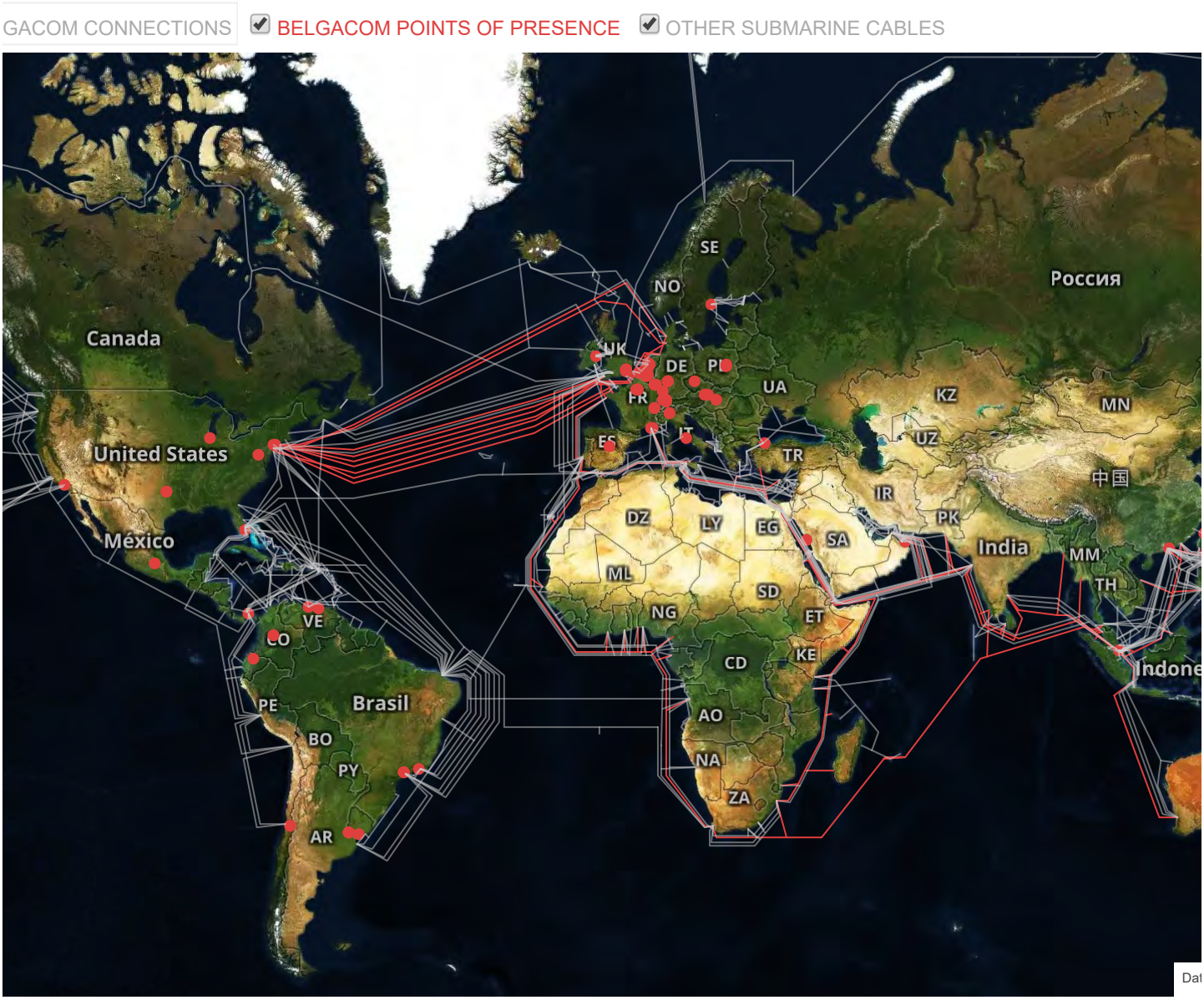
Snowden, told *The Intercept* that she believes the British government should face sanctions if the latest disclosures are proven.

"Compensating Belgacom should be the very least it should do," in 't Veld said. "But I am more concerned about accountability for breaking the law, violating fundamental rights, and eroding our democratic systems."

Other similarly sophisticated state-sponsored malware attacks believed to have been perpetrated by Western countries have involved Stuxnet, a bug used to sabotage Iranian nuclear systems, and Flame, a spy malware that was found collecting data from systems predominantly in the Middle East.

What sets the secret British infiltration of Belgacom apart is that it was perpetrated against a close ally – and is backed up by a series of top-secret documents, which *The Intercept* is now publishing.

GCHQ declined to comment for this story, and insisted that its actions are "necessary legal, and proportionate."



The beginning

The origins of the attack on Belgacom can be traced back to 2009, when GCHQ began developing new techniques to hack into telecommunications networks. The methods were discussed and developed during a series of top-secret "signals development" conferences, held annually by countries in the so-called "Five Eyes" surveillance alliance: the United States, the United Kingdom, Australia, New Zealand, and Canada.

Between 2009 and 2011, GCHQ worked with its allies to develop sophisticated new tools and technologies it could use to scan global

networks for weaknesses and then penetrate them. According to top-secret GCHQ documents, the agency wanted to adopt the aggressive new methods in part to counter the use of privacy-protecting encryption – what it described as the "encryption problem."

When communications are sent across networks in encrypted format, it makes it much harder for the spies to intercept and make sense of emails, phone calls, text messages, internet chats, and browsing sessions. For GCHQ, there was a simple solution. The agency decided that, where possible, it would find ways to hack into communication networks to grab traffic *before* it's encrypted.

The British spies identified Belgacom as a top target to be infiltrated. The company, along with its subsidiary Belgacom International Carrier Services, plays an important role in Europe, and has partnerships with hundreds of telecommunications companies across the world – in Africa, Asia, Europe, the Middle East, and the United States. The Belgacom subsidiary maintains one of the world's largest "roaming" hubs, which means that when foreign visitors traveling through Europe on vacation or a business trip use their cellphones, many of them connect to Belgacom's international carrier networks.

The Snowden documents show that GCHQ wanted to gain access to Belgacom so that it could spy on phones used by surveillance targets travelling in Europe. But the agency also had an ulterior motive. Once it had hacked into Belgacom's systems, GCHQ planned to break into data links connecting Belgacom and its international partners, monitoring communications transmitted between Europe and the rest of the world. A map in the GCHQ documents, named "Belgacom_connections," highlights the company's reach across Europe, the Middle East, and North Africa, illustrating why British spies deemed it of such high value.

Attack planning

Before GCHQ launched its attack on Belgacom's systems, the spy agency conducted in-depth reconnaissance, using its powerful surveillance systems to covertly map out the company's network and identify key employees "in areas related to maintenance and security."

GCHQ documents show that it maintains special databases for this purpose, storing details about computers used by engineers and system administrators who work in the nerve center, or "network operations center," of computer networks worldwide. Engineers and system administrators are particularly interesting to the spies because they manage networks – and hold the keys that can be used to unlock large troves of private data.

GCHQ developed a system called NOCTURNAL SURGE to search for particular engineers and system administrators by finding their IP addresses, unique identifiers that are allocated to computers when they connect to the internet. In early 2011, the documents show, GCHQ refined the NOCTURNAL SURGE system with the help of its Canadian counterparts, who had developed a similar tool, named PENTAHO.

GCHQ narrowed down IP addresses it believed were linked to the Belgacom engineers by using data its surveillance systems had collected about internet activity, before moving into what would be the final stages prior to launching its attack. The documents show that the agency used a tool named HACIENDA to scan for vulnerable potential access points in the Belgacom's networks; it then went hunting for particular engineers or administrators that it could infect with malware.



The infection

The British spies, part of special unit named the Network Analysis Center, began trawling through their vast repositories of intercepted Internet data for more details about the individuals they had identified as suspected Belgacom engineers.

The spies used the IP addresses they had associated with the engineers as search terms to sift through their surveillance troves, and were quickly able to find what they needed to confirm the employees' identities and target them individually with malware.

The confirmation came in the form of Google, Yahoo, and LinkedIn "cookies," tiny unique files that are automatically placed on computers to identify and sometimes track people browsing the Internet, often for advertising purposes. GCHQ maintains a huge repository named MUTANT BROTH that stores billions of these intercepted cookies, which it uses to correlate with IP addresses to

400

determine the identity of a person. GCHQ refers to cookies internally as "target detection identifiers."

Top-secret GCHQ documents name three male Belgacom engineers who were identified as targets to attack. *The Intercept* has confirmed the identities of the men, and contacted each of them prior to the publication of this story; all three declined comment and requested that their identities not be disclosed.

GCHQ monitored the browsing habits of the engineers, and geared up to enter the most important and sensitive phase of the secret operation. The agency planned to perform a so-called "Quantum Insert" attack, which involves redirecting people targeted for surveillance to a malicious website that infects their computers with malware at a lightning pace. In this case, the documents indicate that GCHQ set up a malicious page that looked like LinkedIn to trick the Belgacom engineers. (The NSA also uses Quantum Inserts to target people, as *The Intercept* has previously reported.)

A GCHQ document reviewing operations conducted between January and March 2011 noted that the hack on Belgacom was successful, and stated that the agency had obtained access to the company's systems as planned. By installing the malware on the engineers' computers, the spies had gained control of their machines, and were able to exploit the broad access the engineers had into the networks for surveillance purposes.

The document stated that the hacking attack against Belgacom had penetrated "both deep into the network and at the edge of the network," adding that ongoing work would help "further this new access."

By December 2011, as part of a second "surge" against Belgacom, GCHQ identified other cellphone operators connecting to company's network as part of international roaming partnerships, and successfully hacked into data links carrying information over a

protocol known as GPRS, which handles cellphone internet browsing sessions and multimedia messages.

The spy agency was able to obtain data that was being sent between Belgacom and other operators through encrypted tunnels known as "virtual private networks." GCHQ boasted that its work to conduct "exploitation" against these private networks had been highly productive, noting "the huge extent of opportunity that this work has identified." Another document, dated from late 2011, added: "Network Analysis on BELGACOM hugely successful enabling exploitation."

GCHQ had accomplished its objective. The agency had severely compromised Belgacom's systems and could intercept encrypted and unencrypted private data passing through its networks. The hack would remain undetected for two years, until the spring of 2013.



Inside the Belgacom network control center in Brussels.

The discovery

In the summer 2012, system administrators detected errors within Belgacom's systems. At the company's offices on Lebeau Street in Brussels, a short walk from the European Parliament's Belgian offices, employees of Belgacom's BICS subsidiary complained about problems receiving emails. The email server had malfunctioned, but Belgacom's technical team couldn't work out why.

The glitch was left unresolved until June 2013, when there was a sudden flare-up. After a Windows software update was sent to Belgacom's email exchange server, the problems returned, worse than before. The administrators contacted Microsoft for help, questioning whether the new Windows update could be the reason for the fault. But Microsoft, too, struggled to identify exactly what was going wrong. There was still no solution to be found. (Microsoft declined to comment for this story.)

Belgacom's internal security team began to suspect that the systems had been infected with some sort of virus, and the company decided it was time to call in outside experts. It hired Dutch computer security firm Fox-IT to come and scan the systems for anything suspicious.

Sources familiar with the investigation described the malware as the most advanced they had ever seen.

Before long, Fox-IT discovered strange files on Belgacom's email server that appeared to be disguised as legitimate Microsoft software. The suspicious files had been enabling a highly sophisticated hacker to circumvent automatic Microsoft software

updates of Belgacom's systems in order to continue infiltrating the company's systems.

About a month after Belgacom had identified the malicious software, or malware, it informed Belgian police and the country's specialist federal computer crime unit, according to sources familiar with the incident. Belgian military intelligence was also called in to investigate the hack, together with Fox-IT.

The experts from Fox IT and military intelligence worked to dissect the malware on Belgacom's systems, and were shocked by what they found. In interviews with *The Intercept* and its reporting partners, sources familiar with the investigation described the malware as the most advanced they had ever seen, and said that if the email exchange server had not malfunctioned in the first place, the spy bug would likely have remained inside Belgacom for several more years.

A deep breach

While working to assess the extent of the infection at Belgacom, the team of investigators realized that the damage was far more extensive than they first thought. The malware had not only compromised Belgacom's email servers, it had infected more than 120 computer systems operated by the company, including up to 70 personal computers.

The most serious discovery was that the large routers that form the very core of Belgacom's international carrier networks, made by the American company Cisco, were also found to have been compromised and infected. The routers are one of the most closely guarded parts of the company's infrastructure, because they handle large flows of sensitive private communications transiting through its networks.

Earlier Snowden leaks have shown how the NSA can compromise routers, such as those operated by Cisco; the agency can remotely hack them, or physically intercept and bug them before they are installed at a company. In the Belgacom case, it is not clear exactly which method was used by GCHQ—or whether there was any direct NSA assistance. (The NSA declined to comment for this story.)

Either way, the malware investigators at Belgacom never got a chance to study the routers. After the infection of the Cisco routers was found, the company issued an order that no one could tamper with them. Belgacom bosses insisted that only employees from Cisco could handle the routers, which caused unease among some of the investigators.

"You could ask many security companies to investigate those routers," one of the investigators told *The Intercept*. By bringing in Cisco employees to do the investigation, "you can't perform an independent inspection," said the source, who spoke on condition of anonymity because he was not authorized to speak to the media

A spokesman for Cisco declined to comment on the Belgacom investigation, citing company policy. "Cisco does not comment publicly on customer relationships or specific customer incidents," the spokesman said.

Shortly after the malware was found on the routers, Fox-IT was told by Belgacom to stop its investigation. Researchers from the Dutch security company were asked to write-up a report about their findings as soon as possible. Under the conditions of a non-disclosure agreement, they could not speak about what they had found, nor could they publicly warn against the malware. Moreover, they were not allowed to remove the malware.

Between late August and mid-Sept. 2013, there was an intense period of activity surrounding Belgacom.

On August 30, some parts of the malware were remotely deleted from the company's infected systems – apparently after the British spies realized that it had been detected. But the malware was not completely removed, according to sources familiar with the investigation.

Two weeks later, on Sept. 14, employees from Belgacom, investigators, police and military intelligence services began an intensive attempt to completely purge the spy bug from the systems.

During this operation, journalists were tipped off for the first time about the malware investigation. *The Intercept*'s Dutch and Belgian partners *NRC Handelsblad* and *De Standaard* reported the news, disclosing that sources familiar with the investigation suspected NSA or GCHQ may have been responsible for the attack.

The same day the story broke, on Sept. 16, Belgacom issued a press release. "At this stage there is no indication of any impact on the customers or their data," it said. "At no point in time has the delivery of our telecommunication services been compromised. "

Then, on Sept. 20, German news magazine *Der Spiegel* published documents from Snowden revealing that British spies were behind the hack, providing the first confirmation of the attacker's identity.



Significant resources

In the aftermath of the revelations, Belgacom refused to comment on GCHQ's role as the architect of the intrusion. Top officials from the company were called to appear before a European Parliamentary committee investigating the extent of mass surveillance revealed by Snowden.

The Belgacom bosses told the committee that there were no problems with Belgacom's systems after a "meticulous" clean-up operation, and again claimed that private communications were not compromised. They dismissed media reports about the attack, and declined to discuss anything about the perpetrator, saying only that "the hackers [responsible] have considerable resources behind them."

People with knowledge of the malware investigation watched Belgacom's public statements with interest. And some of them have questioned the company's version of events.

"There was only a partial clean-up," said one source familiar with the malware investigation. "I believe it is still there. It is very hard to

remove and, from what I've seen, Belgacom never did a serious attempt to remove it."

Belgacom declined to comment for this story, citing the ongoing criminal investigation in Belgium.

Last month, *The Intercept* confirmed Regin as the malware found on Belgacom's systems during the clean-up operation.

The spy bug was described by security researchers as one of the most sophisticated pieces of malware ever discovered, and was found to have been targeting a host of telecommunications networks, governments, and research organizations, in countries such as Germany, Iran, Brazil, Russia, and Syria, as well as Belgium.

GCHQ has refused to comment on Regin, as has the NSA, and Belgacom. But Snowden documents contain strong evidence, which has not been reported before, that directly links British spies to the malware.

Aside from showing extensive details about how the British spies infiltrated the company and planted malware to successfully steal data, GCHQ documents in the Snowden archive contain codenames that also appear in samples of the Regin malware found on Belgacom's systems, such as "Legspin" and "Hopscotch."

One GCHQ document about the use of hacking methods references the use of "Legspin" to exploit computers. Another document describes "Hopscotch" as part of a system GCHQ uses to analyze data collected through surveillance.

Ronald Prins, director of the computer security company Fox-IT, has studied the malware, and played a key role in the analysis of Belgacom's infected networks.

"Documents from Snowden and what I've seen from the malware can only lead to one conclusion," Prins told *The Intercept*. "This was used

by GCHQ."

– – –

Documents published with this article:

- Automated NOC detection
- Mobile Networks in My NOC World
- Making network sense of the encryption problem
- Stargate CNE requirements
- NAC review – October to December 2011
- GCHQ NAC review – January to March 2011
- GCHQ NAC review – April to June 2011
- GCHQ NAC review – July to September 2011
- GCHQ NAC review – January to March 2012
- GCHQ Hopscotch
- Belgacom connections

– – –

Photo: Belgacom headquarters: Paul O'Driscoll/Getty; Map: Ingrid Burrington and Josh Begley; Belgacom operations center, Paul O'Driscoll/Bloomberg via Getty.

The Intercept_

HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE

Jeremy Scahill, Josh Begley

February 19 2015, 7:25 p.m.



AMERICAN AND BRITISH spies hacked into the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden.

The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the

potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

The company targeted by the intelligence agencies, Gemalto, is a multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards. Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world. The company operates in 85 countries and has more than 40 manufacturing facilities. One of its three global headquarters is in Austin, Texas and it has a large factory in Pennsylvania.

In all, Gemalto produces some 2 billion SIM cards a year. Its motto is "Security to be Free."

With these stolen encryption keys, intelligence agencies can monitor mobile communications without seeking or receiving approval from telecom companies and foreign governments. Possessing the keys also sidesteps the need to get a warrant or a wiretap, while leaving no trace on the wireless provider's network that the communications were intercepted. Bulk key theft additionally enables the intelligence agencies to unlock any previously encrypted communications they had already intercepted, but did not yet have the ability to decrypt.

As part of the covert operations against Gemalto, spies from GCHQ — with support from the NSA — mined the private communications of unwitting engineers and other company employees in multiple countries.

Gemalto was totally oblivious to the penetration of its systems — and the spying on its employees. "I'm disturbed, quite concerned that this has happened," Paul Beverly, a Gemalto executive vice president, told *The Intercept*. "The most important thing for me is to understand exactly how this was done, so we can take every measure to ensure that it doesn't happen again, and also to make sure that there's no impact on the telecom operators that we have served in a very

trusted manner for many years. What I want to understand is what sort of ramifications it has, or could have, on any of our customers." He added that "the most important thing for us now is to understand the degree" of the breach.

Leading privacy advocates and security experts say that the theft of encryption keys from major wireless network providers is tantamount to a thief obtaining the master ring of a building superintendent who holds the keys to every apartment. "Once you have the keys, decrypting traffic is trivial," says Christopher Soghoian, the principal technologist for the American Civil Liberties Union. "The news of this key theft will send a shock wave through the security community."

The massive key theft is "bad news for phone security. Really bad news."

Beverly said that after being contacted by *The Intercept*, Gemalto's internal security team began on Wednesday to investigate how their system was penetrated and could find no trace of the hacks. When asked if the NSA or GCHQ had ever requested access to Gemalto-manufactured encryption keys, Beverly said, "I am totally unaware. To the best of my knowledge, no."

According to one secret GCHQ slide, the British intelligence agency penetrated Gemalto's internal networks, planting malware on several computers, giving GCHQ secret access. We "believe we have their entire network," the slide's author boasted about the operation against Gemalto.

Additionally, the spy agency targeted unnamed cellular companies' core networks, giving it access to "sales staff machines for customer

information and network engineers machines for network maps." GCHQ also claimed the ability to manipulate the billing servers of cell companies to "suppress" charges in an effort to conceal the spy agency's secret actions against an individual's phone. Most significantly, GCHQ also penetrated "authentication servers," allowing it to decrypt data and voice communications between a targeted individual's phone and his or her telecom provider's network. A note accompanying the slide asserted that the spy agency was "very happy with the data so far and [was] working through the vast quantity of product."

The Mobile Handset Exploitation Team (MHET), whose existence has never before been disclosed, was formed in April 2010 to target vulnerabilities in cellphones. One of its main missions was to covertly penetrate computer networks of corporations that manufacture SIM cards, as well as those of wireless network providers. The team included operatives from both GCHQ and the NSA.

While the FBI and other U.S. agencies can obtain court orders compelling U.S.-based telecom companies to allow them to wiretap or intercept the communications of their customers, on the international front this type of data collection is much more challenging. Unless a foreign telecom or foreign government grants access to their citizens' data to a U.S. intelligence agency, the NSA or CIA would have to hack into the network or specifically target the user's device for a more risky "active" form of surveillance that could be detected by sophisticated targets. Moreover, foreign intelligence agencies would not allow U.S. or U.K. spy agencies access to the mobile communications of their heads of state or other government officials.

"It's unbelievable. Unbelievable," said Gerard Schouw, a member of the Dutch Parliament, when told of the spy agencies' actions. Schouw, the intelligence spokesperson for D66, the largest opposition

party in the Netherlands, told *The Intercept*, "We don't want to have the secret services from other countries doing things like this." Schouw added that he and other lawmakers will ask the Dutch government to provide an official explanation and to clarify whether the country's intelligence services were aware of the targeting of Gemalto, whose official headquarters is in Amsterdam.

Last November, the Dutch government proposed an amendment to its constitution to include explicit protection for the privacy of digital communications, including those made on mobile devices. "We have, in the Netherlands, a law on the [activities] of secret services. And hacking is not allowed," Schouw said. Under Dutch law, the interior minister would have to sign off on such operations by foreign governments' intelligence agencies. "I don't believe that he has given his permission for these kind of actions."

The U.S. and British intelligence agencies pulled off the encryption key heist in great stealth, giving them the ability to intercept and decrypt communications without alerting the wireless network provider, the foreign government or the individual user that they have been targeted. "Gaining access to a database of keys is pretty much game over for cellular encryption," says Matthew Green, a cryptography specialist at the Johns Hopkins Information Security Institute. The massive key theft is "bad news for phone security. Really bad news."



AS CONSUMERS BEGAN to adopt cellular phones en masse in the mid-1990s, there were no effective privacy protections in place. Anyone could buy a cheap device from RadioShack capable of intercepting calls placed on mobile phones. The shift from analog to digital networks introduced basic encryption technology, though it was still crackable by tech savvy computer science graduate students, as well as the FBI and other law enforcement agencies, using readily available equipment.

Today, second-generation (2G) phone technology, which relies on a deeply flawed encryption system, remains the dominant platform globally, though U.S. and European cellphone companies now use 3G, 4G and LTE technology in urban areas. These include more secure, though not invincible, methods of encryption, and wireless carriers throughout the world are upgrading their networks to use these newer technologies.

It is in the context of such growing technical challenges to data collection that intelligence agencies, such as the NSA, have become interested in acquiring cellular encryption keys. “With old-fashioned [2G], there are other ways to work around cellphone security without those keys,” says Green, the Johns Hopkins cryptographer. “With

newer 3G, 4G and LTE protocols, however, the algorithms aren't as vulnerable, so getting those keys would be essential."

The privacy of all mobile communications — voice calls, text messages and Internet access — depends on an encrypted connection between the cellphone and the wireless carrier's network, using keys stored on the SIM, a tiny chip smaller than a postage stamp, which is inserted into the phone. All mobile communications on the phone depend on the SIM, which stores and guards the encryption keys created by companies like Gemalto. SIM cards can be used to store contacts, text messages, and other important data, like one's phone number. In some countries, SIM cards are used to transfer money. As *The Intercept* reported last year, having the wrong SIM card can make you the target of a drone strike.

SIM cards were not invented to protect individual communications — they were designed to do something much simpler: ensure proper billing and prevent fraud, which was pervasive in the early days of cellphones. Soghoian compares the use of encryption keys on SIM cards to the way Social Security numbers are used today. "Social security numbers were designed in the 1930s to track your contributions to your government pension," he says. "Today they are used as a quasi national identity number, which was never their intended purpose."

Because the SIM card wasn't created with call confidentiality in mind, the manufacturers and wireless carriers don't make a great effort to secure their supply chain. As a result, the SIM card is an extremely vulnerable component of a mobile phone. "I doubt anyone is treating those things very carefully," says Green. "Cell companies probably don't treat them as essential security tokens. They probably just care that nobody is defrauding their networks." The ACLU's Soghoian adds, "These keys are so valuable that it makes sense for intel agencies to go after them."

As a general rule, phone companies do not manufacture SIM cards, nor program them with secret encryption keys. It is cheaper and more efficient for them to outsource this sensitive step in the SIM card production process. They purchase them in bulk with the keys pre-loaded by other corporations. Gemalto is the largest of these SIM "personalization" companies.

After a SIM card is manufactured, the encryption key, known as a "Ki," is burned directly onto the chip. A copy of the key is also given to the cellular provider, allowing its network to recognize an individual's phone. In order for the phone to be able to connect to the wireless carrier's network, the phone — with the help of the SIM — authenticates itself using the Ki that has been programmed onto the SIM. The phone conducts a secret "handshake" that validates that the Ki on the SIM matches the Ki held by the mobile company. Once that happens, the communications between the phone and the network are encrypted. Even if GCHQ or the NSA were to intercept the phone signals as they are transmitted through the air, the intercepted data would be a garbled mess. Decrypting it can be challenging and time-consuming. Stealing the keys, on the other hand, is beautifully simple, from the intelligence agencies' point of view, as the pipeline for producing and distributing SIM cards was never designed to thwart mass surveillance efforts.

One of the creators of the encryption protocol that is widely used today for securing emails, Adi Shamir, famously asserted: "Cryptography is typically bypassed, not penetrated." In other words, it is much easier (and sneakier) to open a locked door when you have the key than it is to break down the door using brute force. While the NSA and GCHQ have substantial resources dedicated to breaking encryption, it is not the only way — and certainly not always the most efficient — to get at the data they want. "NSA has more mathematicians on its payroll than any other entity in the U.S.," says the ACLU's Soghoian. "But the NSA's hackers are way busier than its mathematicians."

GCHQ and the NSA could have taken any number of routes to steal SIM encryption keys and other data. They could have physically broken into a manufacturing plant. They could have broken into a wireless carrier's office. They could have bribed, blackmailed or coerced an employee of the manufacturer or cellphone provider. But all of that comes with substantial risk of exposure. In the case of Gemalto, hackers working for GCHQ remotely penetrated the company's computer network in order to steal the keys in bulk as they were en route to the wireless network providers.

SIM card "personalization" companies like Gemalto ship hundreds of thousands of SIM cards at a time to mobile phone operators across the world. International shipping records obtained by *The Intercept* show that in 2011, Gemalto shipped 450,000 smart cards from its plant in Mexico to Germany's Deutsche Telekom in just one shipment.

In order for the cards to work and for the phones' communications to be secure, Gemalto also needs to provide the mobile company with a file containing the encryption keys for each of the new SIM cards. These master key files could be shipped via FedEx, DHL, UPS or another snail mail provider. More commonly, they could be sent via email or through File Transfer Protocol, FTP, a method of sending files over the Internet.

The moment the master key set is generated by Gemalto or another personalization company, but before it is sent to the wireless carrier, is the most vulnerable moment for interception. "The value of getting them at the point of manufacture is you can presumably get a lot of keys in one go, since SIM chips get made in big batches," says Green, the cryptographer. "SIM cards get made for lots of different carriers in one facility." In Gemalto's case, GCHQ hit the jackpot, as the company manufactures SIMs for hundreds of wireless network providers, including all of the leading U.S. — and many of the largest European — companies.

But obtaining the encryption keys while Gemalto still held them required finding a way into the company's internal systems.



Diagram from a top-secret GCHQ slide.

TOP-SECRET GCHQ documents reveal that the intelligence agencies accessed the email and Facebook accounts of engineers and other employees of major telecom corporations and SIM card manufacturers in an effort to secretly obtain information that could give them access to millions of encryption keys. They did this by utilizing the NSA's X-KEYSCORE program, which allowed them access to private emails hosted by the SIM card and mobile companies' servers, as well as those of major tech corporations, including Yahoo and Google.

In effect, GCHQ clandestinely cyberstalked Gemalto employees, scouring their emails in an effort to find people who may have had access to the company's core networks and Ki-generating systems. The intelligence agency's goal was to find information that would aid in breaching Gemalto's systems, making it possible to steal large quantities of encryption keys. The agency hoped to intercept the files

containing the keys as they were transmitted between Gemalto and its wireless network provider customers.

GCHQ operatives identified key individuals and their positions within Gemalto and then dug into their emails. In one instance, GCHQ zeroed in on a Gemalto employee in Thailand who they observed sending PGP-encrypted files, noting that if GCHQ wanted to expand its Gemalto operations, "he would certainly be a good place to start." They did not claim to have decrypted the employee's communications, but noted that the use of PGP could mean the contents were potentially valuable.

The cyberstalking was not limited to Gemalto. GCHQ operatives wrote a script that allowed the agency to mine the private communications of employees of major telecommunications and SIM "personalization" companies for technical terms used in the assigning of secret keys to mobile phone customers. Employees for the SIM card manufacturers and wireless network providers were labeled as "known individuals and operators targeted" in a top-secret GCHQ document.

According to that April 2010 document, "PCS Harvesting at Scale," hackers working for GCHQ focused on "harvesting" massive amounts of individual encryption keys "in transit between mobile network operators and SIM card personalisation centres" like Gemalto. The spies "developed a methodology for intercepting these keys as they are transferred between various network operators and SIM card providers." By that time, GCHQ had developed "an automated technique with the aim of increasing the volume of keys that can be harvested."

The PCS Harvesting document acknowledged that, in searching for information on encryption keys, GCHQ operatives would undoubtedly vacuum up "a large number of unrelated items" from the private communications of targeted employees. "[H]owever an

analyst with good knowledge of the operators involved can perform this trawl regularly and spot the transfer of large batches of [keys]."

The document noted that many SIM card manufacturers transferred the encryption keys to wireless network providers "by email or FTP with simple encryption methods that can be broken … or occasionally with no encryption at all." To get bulk access to encryption keys, all the NSA or GCHQ needed to do was intercept emails or file transfers as they were sent over the Internet — something both agencies already do millions of times per day. A footnote in the 2010 document observed that the use of "strong encryption products … is becoming increasingly common" in transferring the keys.

In its key harvesting "trial" operations in the first quarter of 2010, GCHQ successfully intercepted keys used by wireless network providers in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan. But, the agency noted, its automated key harvesting system failed to produce results against Pakistani networks, denoted as "priority targets" in the document, despite the fact that GCHQ had a store of Kis from two providers in the country, Mobilink and Telenor. "[I]t is possible that these networks now use more secure methods to transfer Kis," the document concluded.

From December 2009 through March 2010, a month before the Mobile Handset Exploitation Team was formed, GCHQ conducted a number of trials aimed at extracting encryption keys and other personalized data for individual phones. In one two-week period, they accessed the emails of 130 people associated with wireless network providers or SIM card manufacturing and personalization. This operation produced nearly 8,000 keys matched to specific phones in 10 countries. In another two-week period, by mining just six email addresses, they produced 85,000 keys. At one point in March 2010, GCHQ intercepted nearly 100,000 keys for mobile phone users in Somalia. By June, they'd compiled 300,000. "Somali providers are

not on GCHQ's list of interest," the document noted. "[H]owever, this was usefully shared with NSA."

The GCHQ documents only contain statistics for three months of encryption key theft in 2010. During this period, millions of keys were harvested. The documents stated explicitly that GCHQ had already created a constantly evolving automated process for bulk harvesting of keys. They describe active operations targeting Gemalto's personalization centers across the globe, as well as other major SIM card manufacturers and the private communications of their employees.

A top-secret NSA document asserted that, as of 2009, the U.S. spy agency already had the capacity to process between 12 and 22 million keys per second for later use against surveillance targets. In the future, the agency predicted, it would be capable of processing more than 50 million per second. The document did not state how many keys were actually processed, just that the NSA had the technology to perform such swift, bulk operations. It is impossible to know how many keys have been stolen by the NSA and GCHQ to date, but, even using conservative math, the numbers are likely staggering.

GCHQ assigned "scores" to more than 150 individual email addresses based on how often the users mentioned certain technical terms, and then intensified the mining of those individuals' accounts based on priority. The highest-scoring email address was that of an employee of Chinese tech giant Huawei, which the U.S. has repeatedly accused of collaborating with Chinese intelligence. In all, GCHQ harvested the emails of employees of hardware companies that manufacture phones, such as Ericsson and Nokia; operators of mobile networks, such as MTN Irancell and Belgacom; SIM card providers, such as Bluefish and Gemalto; and employees of targeted companies who used email providers, such as Yahoo and Google. During the three-month trial, the largest number of email addresses harvested were those belonging to Huawei employees, followed by MTN Irancell. The

third largest class of emails harvested in the trial were private Gmail accounts, presumably belonging to employees at targeted companies.

"People were specifically hunted and targeted by intelligence agencies, not because they did anything wrong, but because they could be used."

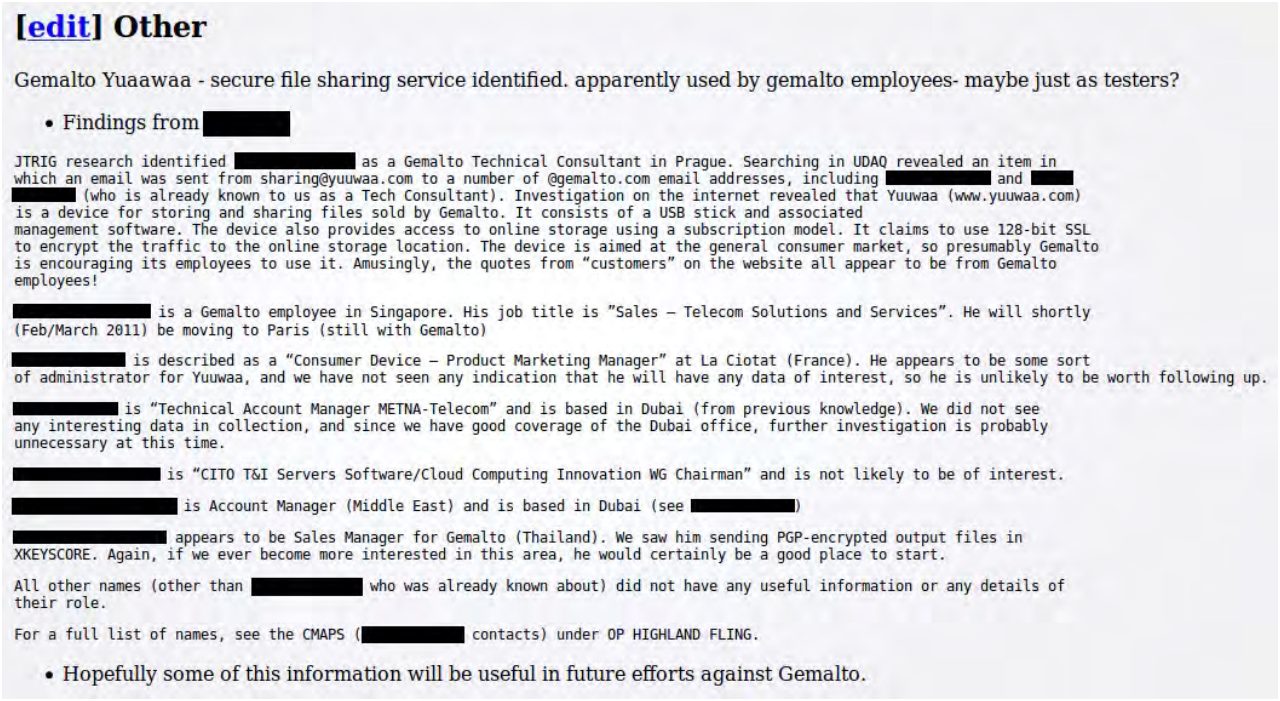
The GCHQ program targeting Gemalto was called DAPINO GAMMA. In 2011, GCHQ launched operation HIGHLAND FLING to mine the email accounts of Gemalto employees in France and Poland. A top-secret document on the operation stated that one of the aims was "getting into French HQ" of Gemalto "to get in to core data repositories." France, home to one of Gemalto's global headquarters, is the nerve center of the company's worldwide operations. Another goal was to intercept private communications of employees in Poland that "could lead to penetration into one or more personalisation centers" — the factories where the encryption keys are burned onto SIM cards.

As part of these operations, GCHQ operatives acquired the usernames and passwords for Facebook accounts of Gemalto targets. An internal top-secret GCHQ wiki on the program from May 2011 indicated that GCHQ was in the process of "targeting" more than a dozen Gemalto facilities across the globe, including in Germany, Mexico, Brazil, Canada, China, India, Italy, Russia, Sweden, Spain, Japan and Singapore.

The document also stated that GCHQ was preparing similar key theft operations against one of Gemalto's competitors, Germany-based SIM card giant Giesecke and Devrient.

On January 17, 2014, President Barack Obama gave a major address on the NSA spying scandal. “The bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don’t threaten our national security and that we take their privacy concerns into account in our policies and procedures,” he said.

The monitoring of the lawful communications of employees of major international corporations shows that such statements by Obama, other U.S. officials and British leaders — that they only intercept and monitor the communications of known or suspected criminals or terrorists — were untrue. “The NSA and GCHQ view the private communications of people who work for these companies as fair game,” says the ACLU’s Soghoian. “These people were specifically hunted and targeted by intelligence agencies, not because they did anything wrong, but because they could be used as a means to an end.”



[edit] Other

Gemalto Yuaawaa - secure file sharing service identified. apparently used by gemalto employees- maybe just as testers?

- Findings from [redacted]

JTRIG research identified [redacted] as a Gemalto Technical Consultant in Prague. Searching in UDAQ revealed an item in which an email was sent from sharing@yuuwaa.com to a number of @gemalto.com email addresses, including [redacted] and [redacted] (who is already known to us as a Tech Consultant). Investigation on the internet revealed that Yuuwaa (www.yuuwaa.com) is a device for storing and sharing files sold by Gemalto. It consists of a USB stick and associated management software. The device also provides access to online storage using a subscription model. It claims to use 128-bit SSL to encrypt the traffic to the online storage location. The device is aimed at the general consumer market, so presumably Gemalto is encouraging its employees to use it. Amusingly, the quotes from “customers” on the website all appear to be from Gemalto employees!

[redacted] is a Gemalto employee in Singapore. His job title is "Sales – Telecom Solutions and Services". He will shortly (Feb/March 2011) be moving to Paris (still with Gemalto)

[redacted] is described as a “Consumer Device – Product Marketing Manager” at La Ciotat (France). He appears to be some sort of administrator for Yuuwaa, and we have not seen any indication that he will have any data of interest, so he is unlikely to be worth following up.

[redacted] is “Technical Account Manager METNA-Telecom” and is based in Dubai (from previous knowledge). We did not see any interesting data in collection, and since we have good coverage of the Dubai office, further investigation is probably unnecessary at this time.

[redacted] is “CITO T&I Servers Software/Cloud Computing Innovation WG Chairman” and is not likely to be of interest.

[redacted] is Account Manager (Middle East) and is based in Dubai (see [redacted])

[redacted] appears to be Sales Manager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in XKEYSCORE. Again, if we ever become more interested in this area, he would certainly be a good place to start.

All other names (other than [redacted] who was already known about) did not have any useful information or any details of their role.

For a full list of names, see the CMAPS ([redacted] contacts) under OP HIGHLAND FLING.

- Hopefully some of this information will be useful in future efforts against Gemalto.

THERE ARE TWO basic types of electronic or digital surveillance: passive and active. All intelligence agencies engage in extensive passive surveillance, which means they collect bulk data by

424

intercepting communications sent over fiber-optic cables, radio waves or wireless devices.

Intelligence agencies place high-power antennas, known as "spy nests," on the top of their countries' embassies and consulates, which are capable of vacuuming up data sent to or from mobile phones in the surrounding area. The joint NSA/CIA Special Collection Service is the lead entity that installs and mans these nests for the United States. An embassy situated near a parliament or government agency could easily intercept the phone calls and data transfers of the mobile phones used by foreign government officials. The U.S. embassy in Berlin, for instance, is located a stone's throw from the Bundestag. But if the wireless carriers are using stronger encryption, which is built into modern 3G, 4G and LTE networks, then intercepted calls and other data would be more difficult to crack, particularly in bulk. If the intelligence agency wants to actually listen to or read what is being transmitted, they would need to decrypt the encrypted data.

Active surveillance is another option. This would require government agencies to "jam" a 3G or 4G network, forcing nearby phones onto 2G. Once forced down to the less secure 2G technology, the phone can be tricked into connecting to a fake cell tower operated by an intelligence agency. This method of surveillance, though effective, is risky, as it leaves a digital trace that counter-surveillance experts from foreign governments could detect.

Stealing the Kis solves all of these problems. This way, intelligence agencies can safely engage in passive, bulk surveillance without having to decrypt data and without leaving any trace whatsoever.

"Key theft enables the bulk, low-risk surveillance of encrypted communications," the ACLU's Soghoian says. "Agencies can collect all the communications and then look through them later. With the keys, they can decrypt whatever they want, whenever they want. It's

like a time machine, enabling the surveillance of communications that occurred before someone was even a target."

Neither the NSA nor GCHQ would comment specifically on the key theft operations. In the past, they have argued more broadly that breaking encryption is a necessary part of tracking terrorists and other criminals. "It is longstanding policy that we do not comment on intelligence matters," a GCHQ official stated in an email, adding that the agency's work is conducted within a "strict legal and policy framework" that ensures its activities are "authorized, necessary and proportionate," with proper oversight, which is the standard response the agency has provided for previous stories published by *The Intercept*. The agency also said, "[T]he UK's interception regime is entirely compatible with the European Convention on Human Rights." The NSA declined to offer any comment.

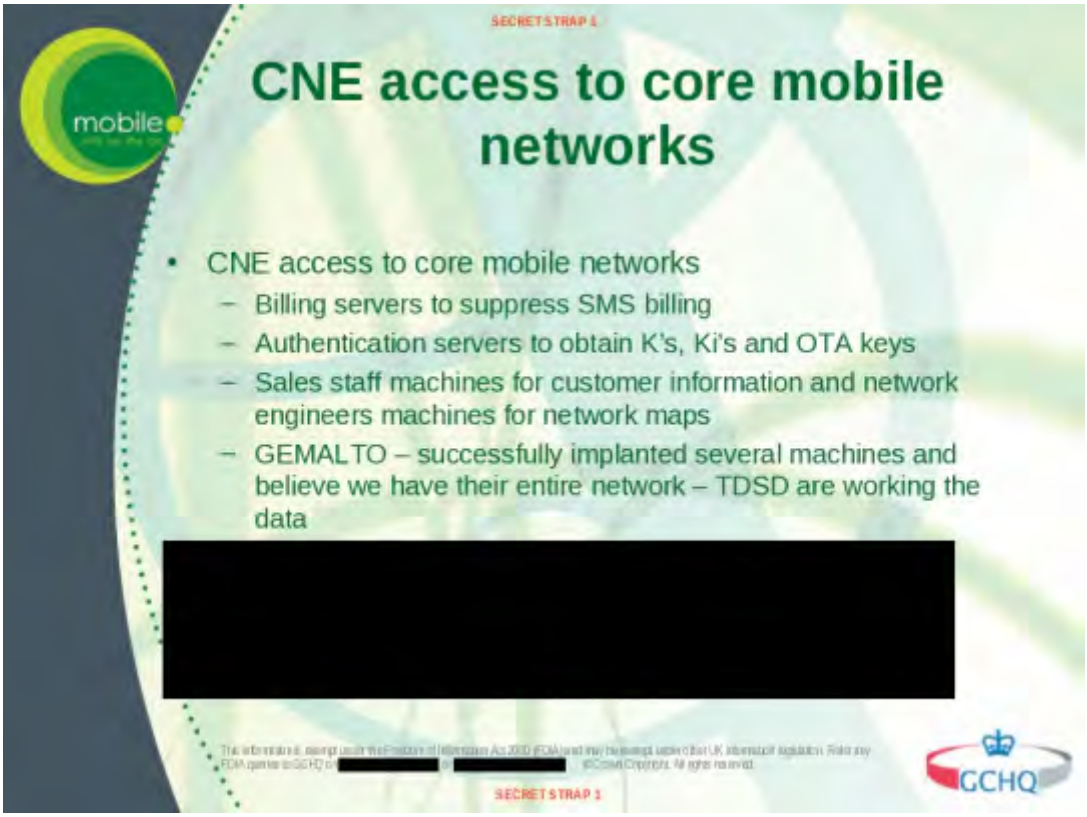
It is unlikely that GCHQ's pronouncement about the legality of its operations will be universally embraced in Europe. "It is governments massively engaging in illegal activities," says Sophie in't Veld, a Dutch member of the European Parliament. "If you are not a government and you are a student doing this, you will end up in jail for 30 years." Veld, who chaired the European Parliament's recent inquiry into mass surveillance exposed by Snowden, told *The Intercept*: "The secret services are just behaving like cowboys. Governments are behaving like cowboys and nobody is holding them to account."

The Intercept's Laura Poitras has previously reported that in 2013 Australia's signals intelligence agency, a close partner of the NSA, stole some 1.8 million encryption keys from an Indonesian wireless carrier.

A few years ago, the FBI reportedly dismantled several transmitters set up by foreign intelligence agencies around the Washington, D.C. area, which could be used to intercept cellphone communications. Russia, China, Israel and other nations use similar technology as the NSA across the world. If those governments had the encryption keys

for major U.S. cellphone companies' customers, such as those manufactured by Gemalto, mass snooping would be simple. "It would mean that with a few antennas placed around Washington, D.C., the Chinese or Russian governments could sweep up and decrypt the communications of members of Congress, U.S. agency heads, reporters, lobbyists and everyone else involved in the policymaking process and decrypt their telephone conversations," says Soghoian.

"Put a device in front of the U.N., record every bit you see going over the air. Steal some keys, you have all those conversations," says Green, the Johns Hopkins cryptographer. And it's not just spy agencies that would benefit from stealing encryption keys. "I can only imagine how much money you could make if you had access to the calls made around Wall Street," he adds.



GCHQ slide.

THE BREACH OF Gemalto's computer network by GCHQ has far-reaching global implications. The company, which brought in $2.7 billion in revenue in 2013, is a global leader in digital security,

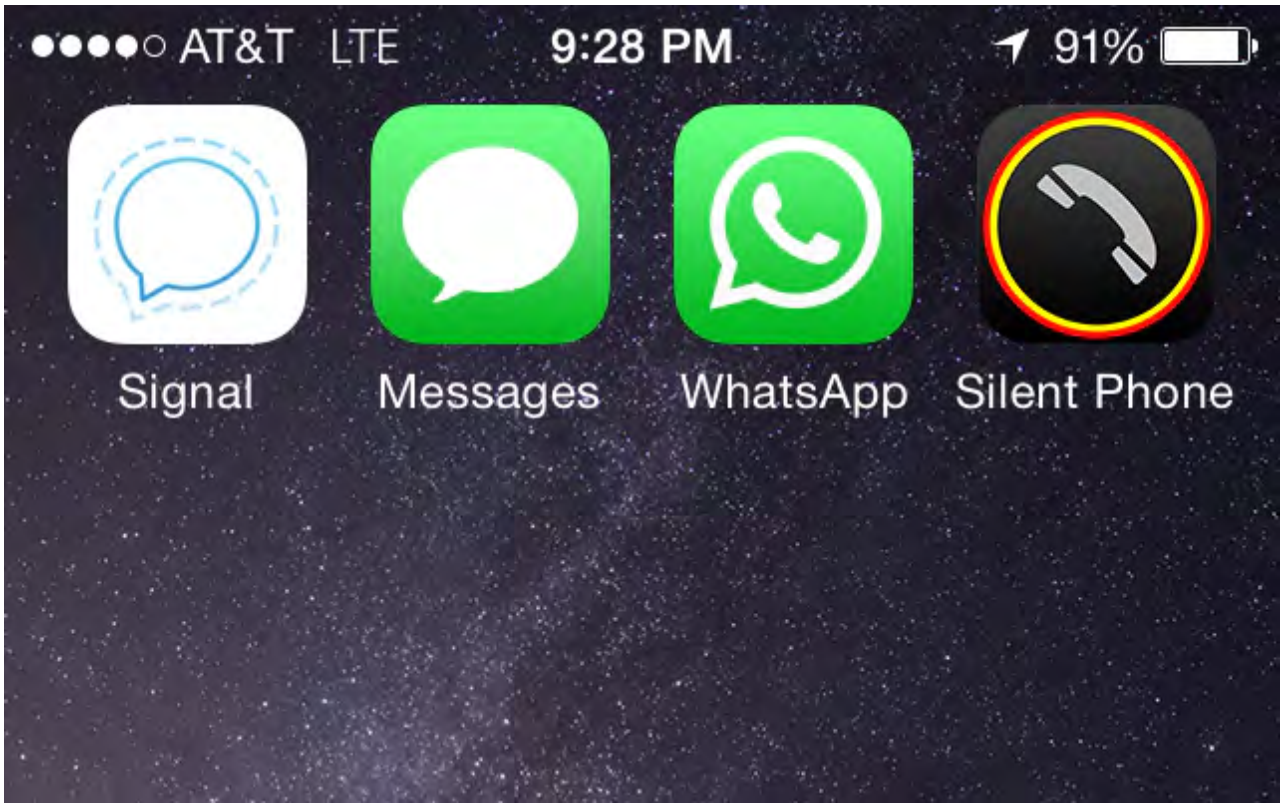
producing banking cards, mobile payment systems, two-factor authentication devices used for online security, hardware tokens used for securing buildings and offices, electronic passports and identification cards. It provides chips to Vodafone in Europe and France's Orange, as well as EE, a joint venture in the U.K. between France Telecom and Deutsche Telekom. Royal KPN, the largest Dutch wireless network provider, also uses Gemalto technology.

In Asia, Gemalto's chips are used by China Unicom, Japan's NTT and Taiwan's Chungwa Telecom, as well as scores of wireless network providers throughout Africa and the Middle East. The company's security technology is used by more than 3,000 financial institutions and 80 government organizations. Among its clients are Visa, Mastercard, American Express, JP Morgan Chase and Barclays. It also provides chips for use in luxury cars, including those made by Audi and BMW.

In 2012, Gemalto won a sizable contract, worth $175 million, from the U.S. government to produce the covers for electronic U.S. passports, which contain chips and antennas that can be used to better authenticate travelers. As part of its contract, Gemalto provides the personalization and software for the microchips implanted in the passports. The U.S. represents Gemalto's single largest market, accounting for some 15 percent of its total business. This raises the question of whether GCHQ, which was able to bypass encryption on mobile networks, has the ability to access private data protected by other Gemalto products created for banks and governments.

As smart phones become smarter, they are increasingly replacing credit cards and cash as a means of paying for goods and services. When Verizon, AT&T and T-Mobile formed an alliance in 2010 to jointly build an electronic pay system to challenge Google Wallet and Apple Pay, they purchased Gemalto's technology for their program, known as Softcard. (Until July 2014, it previously went by the unfortunate name of "ISIS Mobile Wallet.") Whether data relating to

that, and other Gemalto security products, has been compromised by GCHQ and the NSA is unclear. Both intelligence agencies declined to answer any specific questions for this story.



Signal, iMessage, WhatsApp, Silent Phone.

PRIVACY ADVOCATES and security experts say it would take billions of dollars, significant political pressure, and several years to fix the fundamental security flaws in the current mobile phone system that NSA, GCHQ and other intelligence agencies regularly exploit.

A current gaping hole in the protection of mobile communications is that cellphones and wireless network providers do not support the use of Perfect Forward Secrecy (PFS), a form of encryption designed to limit the damage caused by theft or disclosure of encryption keys. PFS, which is now built into modern web browsers and used by sites like Google and Twitter, works by generating unique encryption keys for each communication or message, which are then discarded. Rather than using the same encryption key to protect years' worth of data, as the permanent Kis on SIM cards can, a new key might be

generated each minute, hour or day, and then promptly destroyed. Because cellphone communications do not utilize PFS, if an intelligence agency has been "passively" intercepting someone's communications for a year and later acquires the permanent encryption key, it can go back and decrypt all of those communications. If mobile phone networks were using PFS, that would not be possible — even if the permanent keys were later stolen.

The only effective way for individuals to protect themselves from Ki theft-enabled surveillance is to use secure communications software, rather than relying on SIM card-based security. Secure software includes email and other apps that use Transport Layer Security (TLS), the mechanism underlying the secure HTTPS web protocol. The email clients included with Android phones and iPhones support TLS, as do large email providers like Yahoo and Google.

Apps like TextSecure and Silent Text are secure alternatives to SMS messages, while Signal, RedPhone and Silent Phone encrypt voice calls. Governments still may be able to intercept communications, but reading or listening to them would require hacking a specific handset, obtaining internal data from an email provider, or installing a bug in a room to record the conversations.

"We need to stop assuming that the phone companies will provide us with a secure method of making calls or exchanging text messages," says Soghoian.

— — —

Documents published with this article:

- CNE Access to Core Mobile Networks
- Where Are These Keys?
- CCNE Successes Jan10-Mar10 Trial
- DAPINO GAMMA CNE Presence Wiki

- DAPINO GAMMA Gemalto Yuaawaa Wiki
- DAPINO GAMMA Target Personalisation Centres Gemalto Wiki
- IMSIs Identified with Ki Data for Network Providers Jan10-Mar10 Trial
- CCNE Stats Summaries Jan10-Mar10 Trial
- CCNE Email Harvesting Jan10-Mar10 Trial
- CCNE Email Addresses Jan10-Mar10 Trial
- PCS Harvesting at Scale

– – –

Additional reporting by Andrew Fishman and Ryan Gallagher. Sheelagh McNeill, Morgan Marquis-Boire, Alleen Brown, Margot Williams, Ryan Devereaux and Andrea Jones contributed to this story. Erin O'Rourke provided additional assistance.

Top photo: Shutterstock

WAIT! BEFORE YOU GO about your day, ask yourself: How likely is it that the story you just read would have been produced by a different news outlet if The Intercept hadn't done it?

Consider what the world of media would look like without The Intercept. Who would hold party elites accountable to the values they proclaim to have? How many covert wars, miscarriages of justice, and dystopian technologies would remain hidden if our reporters weren't on the beat?

The kind of reporting we do is essential to democracy, but it is not easy, cheap, or profitable. The Intercept is an independent nonprofit news outlet. We don't have ads, so we depend on our members — 35,000 and counting — to help us hold the powerful to account. Joining is simple and doesn't need to cost a lot: You can become a sustaining member for as little as $3 or $5 a month. That's all it takes to support the journalism you rely on.

Become a Member →

CNE Access to BELGACOM GRX Operator: (GREEN) Following the successful NAC MyNOC OP SOCIALIST to provide CNE access to the BELGACOM GRX Operator (MERION ZETA), the NAC have continued to provide assistance in mapping out the internal network and providing direction to the CNE operator on the best internal devices to have a presence on. The goal being to enable access to internal GRX routers that can then be used to conduct MitM operations against Mobile Handsets that are roaming.