PRIVACY INTERNATIONAL

Submitted to the Home Office

Privacy International's Submission to the Home Office Investigatory Powers Act 2016 Consultation on the Draft Codes of Practice

6 April 2017

PRIVACY INTERNATIONAL'S SUBMISSION TO THE HOME OFFICE INVESTIGATORY POWERS ACT 2016 CONSULTATION ON THE DRAFT CODES OF PRACTICE

6 APRIL 2017

Submitted to the Home Office

investigatorypowers@homeoffice.gsi.gov.uk

1. Introduction

1.1. Thank you for the opportunity to provide comments on the Draft Codes of Practice for:

- 1.1.1. Interception of communications
- 1.1.2. Equipment interference
- 1.1.3. Bulk communications data acquisition
- 1.1.4. Bulk Personal Datasets
- 1.1.5. National Security Notices

1.2. Privacy International was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, focuses on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

1.3. We have previously made submissions in relation to the Investigatory Powers Act.[1] We maintain our positions as set out in those submissions. We have, for example, stated that bulk powers are contrary to law and should be removed from the Investigatory Powers Act. Whilst we maintain this position, given that the Government appears likely to enact the bulk powers, we make the following observations and recommendations in relation to the proposed accompanying Codes of Practice, including as they address the bulk powers.

[1] Privacy International Submissions to the Joint Committee on the Investigatory Powers Bill
https://www.privacyinternational.org/node/724
Also at: Privacy International—written evidence (IPB0120) https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf
Privacy International Submissions to the Science and Technology Committee
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html
https://www.privacyinternational.org/node/833

1.4. Our response is set out in two sections. **Section A** deals with submissions that relate to a number or all of the Codes. **Section B** deals with submissions specific to a particular Code.

Concerns about the consultation process

1.5. The consultation states that in preparing the drafts the Government has engaged with representatives of civil liberties organisations. We confirm that we have not been consulted by the Government nor contacted for 'engagement' in relation to these versions of the Codes.

1.6. We have written to the Home Office during the consultation period asking for various points of clarification. We have received no response.

1.7. The consultation purports to *'set out the processes and safeguards governing the use of investigatory powers'* to *'give detail on how the relevant powers should be used, including examples of best practice'*. They are *'intended to provide additional clarity and to ensure the highest standards of professionalism and compliance'*. Each Code fails to achieve these aims. We submit that rather than clarify powers in the Act, the Codes have reduced certain safeguards and removed language that limits powers.

1.8. We have three primary concerns in relation to the Codes:

1.8.1. They undermine transparency in relation to surveillance powers in the Investigatory Powers Act;

1.8.2. They expand powers in the Investigatory Powers Act;

1.8.3. They undermine the limited oversight as set out in the Investigatory Powers Act.

1.9. Our response is limited in scope given the short timeline for the consultation on five very large Codes of Practice. These Codes contain many fundamental changes to previous versions published in Autumn 2016. These changes have not been identified by the Home Office and instead had to be identified by painstaking comparison of the documents. We are thus concerned that certain key changes may not have been picked up.

1.10. We have also been severely limited by:

1.10.1. The lack of explanation behind any of the examples provided and deficiencies in many of those examples which purport to justify powers granted by the Investigatory Powers Act.

1.10.2. The lack of material to explain changes to the Codes.

1.11. We refer to the joint letter signed by Privacy International and Open Rights Group.[2]

1.12. We recommend that a further consultation take place following review of submissions in relation to the current Draft Codes of Practice.

[2] https://www.openrightsgroup.org/ourwork/letters/letter-to-home-secretary-on-investigatory-powers-act-codes-consultation

1.13. We recommend that at the time the Codes are laid before Parliament sufficient time is given for debate, discussion and amendment.

1.14. A number of recommendations and concerns relate to oversight. We believe oversight needs to be comprehensive and suggest, among other things, an informed review of the resources and funding available to the oversight bodies on an annual basis, with involvement of Parliament.

1.15. In relation to terminology used in this submission:

1.15.1. Unless otherwise specified, reference to the Codes of Practice or the Codes refer to the current Draft February 2017 versions as opposed to the Autumn 2016 versions.

1.15.2. We may abbreviate Equipment Interference as "EI".

Concerns Regarding the Role of Codes of Practice

1.16. We note that as per the judgment of the Court of Justice of the EU (Grand Chamber) of 21 December 2016 ("the Watson CJEU judgment") in 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 & others (ORG and PI intervening)* (the "Watson Proceedings"), the Code of Practice is not the appropriate place to provide additional rules regarding the government's surveillance powers, as the Code of Practice is not legally binding. Instead, primary legislation must serve this purpose:

'117. Further, since the legislative measure referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.'

1.17. Codes are an important tool for clarification of existing authorizations and obligations conferred by law. As all the Codes note is is the Act that provides the "statutory framework" for authorising the powers enumerated therein. The Code thus merely provides guidance for authorities, but cannot replace the law or be used to generate new powers that were not otherwise provided by Parliament.

SECTION A

2. **Definitions General**

2.1. Telecommunication operators

2.2. The Investigatory Powers Act expands the definition of a telecommunications operator. The Codes fail to provide any clarity on what is meant by a telecommunications operator and instead adds to the confusion. We believe the term 'telecommunications operator' is so broad as to be meaningless.

2.3. The Codes refer to a communication service provider ('CSP'). The Bulk Acquisition Code of Practice has removed reference to postal operator from the definition of a communication service provider ('CSP'). Whereas previously a CSP was used to refer to both a postal operator and telecommunications operator, it is now stated that *'CSP refers only to a telecommunications operator'.* This is consistent with the EI Code of Practice [§2.8]. The Interception Code of Practice, however, uses CSP to refer to '*a telecommunications operator or postal operator*' [§2.3].'

2.4. This inconsistency only adds confusion regarding who will be subject to the powers the Codes describe.

2.5. **Recommendation**: **Remove all references to communication service provider and maintain consistent references to telecommunications operator and postal operator as appropriate.**

2.6. As stated above, the Act expands the powers of the Government in respect of whom it can require to comply with surveillance powers. Prior to the Investigatory Powers Act, legislation[3] referred to 'public' telecommunications operators. The Investigatory Powers Act has dropped the 'public' and refers simply to telecommunications operators. A telecommunications operator is defined at section 261(10) of the Act as a person who "(a) offers or provides a telecommunications service to persons in the UK, or (b) controls or provides a telecommunications system" in or controlled from UK.

2.7. At 261(11) a "Telecommunications service" is "*any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system"* and at 261(13) a "Telecommunications system" is *"a system . . . that exists . . . for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy"*

2.8. We do not agree that it is justifiable to use such *'intentionally broad'* definitions, solely on the basis that *'it remain[s] relevant for new technologies.'*

[3] E.g. Regulation of Investigatory Powers Act 2000, Data Retention and Investigatory Powers Act 2014

2.9. We submit that the use of such broad definitions undermines transparency and effective oversight.

2.10. The EI Code demonstrates the broad reach of the definition stating that "telecommunications operator" also includes:

2.10.1. *"application and website providers . . . insofar as they provide a telecommunication service. For example an online marketplace may be a telecommunications operator if it provides a connection to an application/website"*. [§2.12]

2.10.2. *"a telecommunications operator if and in so far as it provides a messaging service."* [§2.12]

2.10.3. *"those persons who provide services where customers, guests or members of the public are provided with access to communications services . . . ancillary to the provision of another service . . . for example in commercial premises such as hotels or public premises such as airport lounges or public transport."* [§2.13]

2.11. The Bulk Acquisition Code adds that:

2.11.1. *'...any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included with the meaning of 'telecommunication service'. Internet-based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.'* [§2.4]

2.12. The Autumn 2016 version of the Bulk Acquisition Code had other examples. It is not clear why these have been deleted:

2.12.1. *"In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally circumstances may necessitate the acquisition of communications data for example where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room."* [§2.7]

2.13. In light of the above it is misleading for the Bulk Acquisition Code, for example, to give the impression that those to whom obligations apply, is limited - *'The obligations … apply to telecommunications operators only…'*

2.14. **Recommendation**:

- **To provide clarification on who is a telecommunications operator.**
- **To maintain a central list of telecommunications operators on whom the powers of the IPA have been exercised, which is reviewed by the Investigatory Powers Commissioner and provided to Parliament.**

2.15. Serious crime

2.15.1. The Codes refer to the justification of serious crime for utilising powers in the Act. Serious crime is defined in broad terms in section 263(1) of the Act. Further explanation is required on the meaning of serious crime. Such explanation is not provided in the Codes.

2.15.2. The types of offences which fall under 'serious crime' should be subject to independent review.

2.16. Less intrusive means

2.16.1. The Codes refer to the use of 'less intrusive means'. Whilst this is in theory a positive statement, it is meaningless without an analysis or explanation as to what constitutes 'less intrusive means', how a determination of intrusiveness is conducted, who conducts the assessment and what oversight exists to scrutinise whether less intrusive in theory is less intrusive in practice.

2.16.2. To illustrate our concern, the Bulk Acquisition Code refers to the use of less intrusive means [§3.10] however it also refers to the request filter as less intrusive. See below our concerns about this statement given the paucity of information on the request filter and its potential to be quite intrusive.

2.16.3. Similarly, the Interception Code declares the collection of 'secondary data' to be less intrusive than the collection of content. This conclusion is not necessarily correct as context matters in assessing intrusiveness, and indeed the bulk collection of secondary data might be very intrusive indeed, as has been recognised in the Watson CJEU judgment.

2.17. Non-content data: Systems data / identifying data / communications data / secondary data

2.18. The subdivision of what was previously referred to as communications data creates a confusing array of terminologies.

2.19. The EI Code refers to 'systems data' and 'identifying data' as part of equipment data [§2.4]. It states that *'identifying data'* can be '*comprised in the communication'* but *'does not, once separated, reveal anything of what might reasonably be considered the meaning … of any communication.'*

2.20. The Interception Code uses the term 'secondary data', which encompasses 'system data' and 'identifying data' [§2.12]. 'Secondary data' is vaguely described as '*a broader category of data than communications data*'.

2.21. The Bulk Acquisition Code refers to 'systems data', 'communications data' and 'identifying data' [§2.6]. It states that communications can be separated into systems data and content. Anything which is systems data is not content.

2.22. Identifying data: The Bulk Acquisition Code repeats the EI Code stating that identifying data is certain data *'separated from the remainder of a communication in circumstances where, if it were so separated it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication.'*

2.23. Communications data is a subset of systems data: *'communications data is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication, except any meaning arising from the fact of the communication or transmission of the communication.'*

2.24. The Bulk Acquisition Code provides further sub-categories of communications data:

2.24.1. 'entity data; [§2.14 - 2.17] which includes *'information about any person to whom a service is provided, whether a subscriber or guest user, and whether or not they have ever used that service'* and is *'limited to data held or obtained by the CSP in relation to the provision of a telecommunications service'*

2.24.2. Data that facilitates the transmission of a communication [§2.18 - 2.10]

2.24.3. Service or system data [§2.21]

2.24.4. Architecture of a telecommunication system [§2.22 - 2.23]

2.25. The above sub-categories are merely examples of the many ways in which what may be obtained or accessed under the powers are being described. This lack of consistency undermines transparency regarding how the powers will be used.

2.26. Compounding this problem, the Bulk Acquisition Code refers, as stated above, to data 'held by a CSP about the architecture of the telecommunications system (sometimes referred to as reference data). Whilst it gives examples of what may be included - location of cell masts or WI-FI hotspots - this is not an exhaustive list. Yet despite providing limited clarity on what this applies to, the Code states that *'This information itself does not contain any information relating to specific persons and its acquisition in its own right does not interfere with the privacy of any customers'.*

2.27. Not only does the negation of the right to privacy undermine safeguards in relation to an unspecified type of communications data, it does not address the impact on the right to privacy of the combination of this with other data.

2.28. We are concerned that the Bulk Acquisition Code then excludes [§2.23] *'publicly or commercially available communications data. A Part 3 authorisation is not mandatory to obtain reference data, such as mobile phone mast locations, from a CSP, as there is no intrusion with an individual's human rights.'*

2.29. We are concerned that the Bulk Acquisition Code appears to allow content to be defined as systems data without independent oversight:

'2.28 ...systems data cannot be content. In practice this means that a SIA should first determine whether the data enables or otherwise facilitates the functioning of a system or service. If the answer to this is yes, then the data is systems data regardless of whether it may reveal anything of what might be reasonably considered to be the meaning (if any) of the communication.'

2.30. Looking at the powers applicable to non-content data, there is a real concern that definitions will develop in secret with little or no independent oversight and arbitrarily delineate what is and it not intrusive, and what does or does not fall under the Investigatory Powers Act or within an oversight regime. This raises the risk of abuse, misuse and errors. There is a need for regular scrutiny and transparency.

2.31. **Recommendations**:

2.31.1. **The Codes must not be used to exclude the collection or use of any data from the application of safeguards and independent oversight.**
2.31.2. **Clarity is required in relation to non-content data.**
2.31.3. **Oversight is required as to the classification of information as communications data, content or a third category.**
2.31.4. **The intrusive nature of systems data, identifying data and communications data should not be predetermined as low.**

3. Status of the Code

3.1. Each of the Codes of Practice were previously accompanied by the statement that the guidance in the Code *'takes precedence over any contrary content'* of a *'public authority's internal advice or guidance'* [Autumn BA:1.10] or *'of an equipment interference agency's internal advice or guidance.'* [Autumn EI: 1.5].

3.2. However, this statement has been amended in the February 2017 draft Codes of Practice in a manner which adds a layer of obfuscation to the role of the Codes.

3.2.1. Bulk Acquisition: [§1.9] *'For the avoidance of doubt, the duty to have regard to the code when exercising functions to which the code relates exists regardless of any contrary content of a SIA's internal advice or guidance.'*
3.2.2. Equipment Interference: [§1.4] *'the information commissioner **may** take the provisions of the codes of practice into account.'*
3.2.3. National Security Notices: [§1.3] *'For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an intercepting agency's internal advice or guidance.*
3.2.4. Interception of Communications: [§1.3] *'For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an intercepting agency's internal advice or guidance.'*

3.3. **Recommendation: The Codes of Practice must all contain the statement that each one takes precedence over any contrary content of a public authority's /**

equipment interference agency's internal advice or guidance. It is unacceptable that secret internal guidance or advice can override publicly available guidance.

3.4. We note that throughout the Codes of Practice there are also references to additional guidance and handbooks, for example:

3.4.1. *'The Home Office may issue further guidance to CSPs or SIAs on how the definitions in the Act apply.'* [§2.29 Bulk Acquisition Code]

3.4.2. *'...handbook provided to all CSPs required to provide communications data in bulk.'* [§7.8 Bulk Acquisition Code]

3.4.3. *'The person or company to whom a notice is given will be provided with a handbook which will contain the basic information they will require to respond to requests for reasonable assistance in relation to the interception of communications.*' [§8.18 Interception Code]

3.4.4. *'Further details with respect to cost recovery will be available in the handbook provided to all communications service providers who maintain an interception capability.'* [§8.51 Interception Code]

3.4.5. *'Further details with respect to cost recovery will be available in the handbook provided to all communication service providers who maintain an equipment interference capability.'* [§7.20 EI Code]

3.4.6. *'The person or company to whom a notice is given will be provided with a handbook which will contain the basic information they will require to respond to requests for reasonable assistance in relation to the acquisition of material.'* [§8.18 EI Code]

3.4.7. *'The Secretary of State may issue further guidance to assist law enforcement chiefs and appropriate delegates in considering whether it is proportionate to issue an equipment interference warrant.'* [§5.49 EI Code]

3.5. **Recommendation**: **Any additional handbooks, guides, or policy positions must be published. Any information that is redacted must be subject to independent review.**

4. Use of automated systems

4.1. The Codes refer to the use of automated systems:

4.1.1. Bulk Acquisition Code refers to the use of automated systems for selection for examination [§6.13]

4.1.2. EI Code refers to the use of automated systems to *'effect the selection for examination'* [§6.71]

4.1.3. Interception Code refers to *'the use of automated systems, to reduce the extent of collateral intrusion.'* [§5.45] and that *'automated systems should, where technically possible, be used to effect the selection for examination in accordance with section 142 of the Act'.* [§6.71]

4.2. **Recommendation: There is no explanation in the Act or in the Codes as to what is meant by automated systems. Clarification is required and it is not accepted that conclusions can be made about whether or not they reduce collateral intrusion without further transparency**.

5. Thematic Warrants

5.1. The Interception and EI Codes refer to the use of thematic warrants.

5.2. **Thematic warrants as general warrants**

5.3. Privacy International maintains, and has explained in numerous submissions, that thematic warrants are unlawful because they constitute classic general warrants.[4] This is because thematic warrants permit law enforcement and the security and intelligence agencies to intercept content or interfere with equipment within the United Kingdom without needing to specify the target of the interference.

5.4. The EI Code confirms this lack of specification, describing thematic warrants at §5.15 as falling two categories: "*those where it is reasonably practicable to include additional details and those where it is not*".

5.5. The EI Code provides that, for the latter category, hacking targets are entirely at the discretion of the agency: *"There is no requirement to modify warrants . . . during the currency of the warrant providing any additional names or descriptions already fall within the subject-matter of the warrant and the description of the persons."* [§5.16]

5.6. The Code allows that even the determination of whether to provide individual names or descriptions is entirely at the discretion of the agency: *"The practicability of providing individual names or descriptions will need to be assessed on a case by case basis by the . . . agency . . . ."* [§5.17]

5.7. The requirements for an interception thematic warrant are essentially identical [§5.13-5.17].

[4] See Privacy International, Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill ("Joint Committee") (IPB0120), 7 Jan. 2016, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26371.html; Privacy International and Open Rights Group, Written Evidence to the Joint Committee on Human Rights, 7 Dec. 2015; Privacy International, Written Evidence to the Science and Technology Committee (IPB0040), 1 Dec. 2015, available at http://data.parliament.uk/writtenevidence/ committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html.

5.8. The additional detail provided in the Codes regarding thematic warrants only heighten Privacy International's concerns that such warrants do not comply with either UK law or the ECHR.

5.9. **Promotion of Thematic Warrants**

5.10. These concerns regarding the breadth of thematic warrants were not only expressed by Privacy International and other civil society groups, but also by some of the Parliamentary committees that reviewed the Investigatory Powers Bill.

5.11. For instance, the Joint Committee on the Draft Investigatory Powers Bill ("Joint Committee") expressed deep concerns regarding thematic warrants, concluding that "the current wording . . . is too broad". It recommended that "the language of the Bill be amended so that targeted interception and targeted equipment interference warrants cannot be used in a way to issue thematic warrants concerning a very large number of people."[5]

5.12. Given these concerns, the use of thematic warrants should, at the very least, be extremely rare. The Codes, however, appear to promote their use, particularly because they are easier to modify than more traditional targeted warrants. In the Interception Code for example:

5.12.1. The first example of thematic warrant given, at §5.15, describes the use of the warrant for the investigation of three people, with the possibility that more people of interest could be added to the warrant as they are discovered during the course of the investigation.

5.12.2. It is not at all clear in the example why three targeted, non-thematic interception warrants could not be issued in the circumstances described, with additional targeted warrants being obtained as additional suspects are identified. Indeed, the only apparent reason for the use of a thematic warrant in such circumstances seems to be that it makes it easier to add further targets to the warrant since, as the Code later states, '*[t]he ability to modify the names or descriptions [in a warrant] apply only to thematic warrants*' [§5.21].

5.12.3. The modification of a thematic warrant does not require the approval of a judicial commissioner, only that he be notified, thus bypassing a safeguard that would otherwise apply to non-thematic targeted warrants [Interception Code at §5.71-5.72]. The comparison of non-thematic and thematic warrants in the Interception Code §5.74 illustrates this disparity.

5.13. **Recommendation: While Privacy International maintains that thematic warrants are not lawful under UK law or the ECHR, if they are to be used, they should be seen only as a last resort. The Codes should reflect this disapproval of**

[5] Joint Committee Report, Draft Investigatory Powers Bill, para. 468.

thematic warrants instead of, as they currently do, seeming to tout their flexibility and usefulness

6. Technical Capability Notices ("TCN") / Maintenance of Technical Capability

6.1. *Lack of Clarity*: TCNs are referred to in the Bulk Acquisition, Equipment Interference and Interception Codes. Referring to TCNs across all three Codes creates confusion regarding the full scope of this power. In addition, the definition of the obligations required under TCNs is much too vague for the public to adequately foresee the circumstances in which they would be used and the scope of its application:

6.1.1. The Code describes the purpose of "*maintaining a technical capability*" as ensuring that "*when a warrant . . . is served, companies can give effect to it securely and quickly*" and that "*[i]n practice, [TCN]s will only be given to communication service providers that are likely to be required to give effect to warrants . . . on a recurrent basis*." It is not sufficiently clear exactly what companies would fall with the characterization of "likely to be required" and "on a recurrent basis" – would a company that might be required to effect a warrant once or twice a year, for example, fall within this scope?

6.1.2. The Act provides only examples of the types of obligations that might be imposed by TCNs, which are exceedingly broad. The Code provides no additional clarity, simply reiterating the examples in the Act, which include such vague statements as *"[o]bligations to provide facilities or services of a specified description*," "*relating to apparatus owned or operated by a relevant operator*," and "*relating to the security of any telecommunications services provided by the relevant operator*." [§8.4 EI Code]

6.1.3. ***Recommendation*: The provisions for TCNs should be provided for in a single Code to ensure consistency and clarity.**

6.1.4. ***Recommendation*: The Code should bring greater clarity to the circumstances in which the government will seek a TCN and the obligations that might be imposed under a TCN, including concrete examples.**

6.2. *Significant Interference with Business Operations of Telecommunications Operators*: TCNs authorise the government to significantly interfere with the business operations of telecommunications operators.

6.2.1. For example, the Code observes that TCNs will "*often . . . require the creation of dedicated systems*," without elaborating further on what types of systems these might entail and how they might interact with the company's existing systems. [§8.19 EI Code]

6.2.2. Relatedly, we are concerned by the Secretary of State's power under TCNs "*to develop compliance systems*," for example "*to develop consistent systems for use by communication service providers to acquire material*."

[§§8.8-8.10 Bulk Acquisition Code, §8.57 EI Code, §8.57 Interception Code] In both scenarios, the IPA regime essentially permits the government to force government-developed systems onto companies.

6.2.3. Finally, a TCN will require the subject of the notice to "*notify the Secretary of State of changes to existing telecommunications services and the development of new services and relevant products in advance of their launch*." [§8.32 EI Code] This requirement permits the government to delay, interfere with, or alter core business and strategic decisions undertaken by telecommunications operators.

6.2.4. **Recommendation: The Code must provide greater transparency as to the types of dedicated and compliance systems that may be required under TCNs. It should also not require companies adopt such systems where they would compromise the security and integrity of the company's existing systems. The Code must further remove the requirement that companies must notify the government of changes to existing services or the development of new ones.**

6.3. *Undermining Encryption:* We are concerned by the continued requirements relating to undermining encryption, which the government had suggested during the debate over the Act that it would not seek to pursue. The Codes now make clear that TCNs can be used to remove encryption. These measures would weaken internet security as they would force telecommunications providers to create "backdoors" to encrypted systems, leaving them open to breaches. The EI Code, for example, states that "*[a]n obligation imposed by a [TCN] . . . requires that provider to maintain the capability to remove encryption when subsequently served with a warrant* . . ." [§8.6 EI Code] In other words, a TCN would require companies to fundamentally alter their systems by building in the permanent capability to undermine encryption on any individual customer's communications.

6.3.1. ***Recommendation*: Clarify that the "removal of electronic protection" obligation does not operate to require that companies "*maintain the capability to remove encryption when subsequently served with a warrant*."**

6.4. ***Insufficient Process to Challenge TCNs*:** The subject of a TCN may request review by the Secretary of State. While the Technical Advisory Board and a Judicial Commissioner provide views on the challenge, the Secretary of State makes the decision "to vary, withdraw or confirm the effect of the notice." That decision is then subject to approval by the Investigatory Powers Commissioner. [§§8.43-8.47 EI Code]

6.4.1. ***Recommendation*: The subject of a TCN should be able to challenge the TCN before an independent authority, preferably a judge. The review of that challenge should not be undertaken by the Secretary of State with approval by the IPC.**

7. Intelligence Sharing

7.1. Across all of the Codes, very little attention is paid to intelligence sharing and the safeguards that must attached when data is shared. This is a deficiency in the Codes, and indeed in the Act itself. Without robust safeguards, intelligence sharing may not be compliant with the UK law and the ECHR. The following are a few examples of where the Codes fall short in regulating sharing and cooperation, often by making any safeguards that may apply to that sharing optional instead of mandatory.

7.2. <u>EI Code</u>

7.2.1. Intelligence Cooperation: The Government cannot ask an international partner to undertake EI where it would deliberately circumvent the Act but it is not "*deliberate circumvention where, for example, the . . . agency does not have the required access to a piece or multiple pieces of equipment and it is not therefore technically feasible for the . . . agency to obtain the data under the Act*" [§4.3]. This provision would appear to contain a significant loophole to the prohibition against deliberate circumvention of the Act.

7.2.2. Intelligence Sharing:

7.2.3. The EI Code contains a number of safeguards relating to the dissemination of material obtained under an EI warrant. For example, disclosure is prohibited "*to persons who have not been appropriately vetted and also by the need-to-know principle*" and "*only so much of the material may be disclosed as the recipient needs*" [§9.21]. The EI Code states that these obligations apply "*to anyone to whom the material is subsequently disclosed*", in some cases by "*requiring the latter to obtain the original agency's permission before disclosing the material further*", in other cases through explicit safeguards. [§9.22]

7.2.4. It is not clear, however, if these safeguards also apply to material disseminated to foreign governments. For example, the EI Code also states that where material obtained under an EI warrant is "*disclosed to*" foreign authorities, retention, copying, dissemination, and minimization requirements "*will apply to the extent (if any) that the issuing authority considers appropriate*". [§9.23]. Moreover, where "*unselected data obtained under a bulk [EI] warrant" is disclosed to foreign authorities, examination safeguards "will apply . . . to the extent (if any) that the issuing authority considers appropriate*". [§9.23]. In the latter instance, foreign access to unselected data could potentially permit foreign governments access - with few safeguards - to an enormous pool of data.

7.3. <u>Bulk Acquisition</u>

7.3.1. The Bulk Acquisition Code states that an application form for acquisition should (not must) contain *'Consideration of whether the data acquired*

under the warrant may be available to any other security and intelligence agency or an international partner, where it is necessary and proportionate to do so' [§4.5].

7.3.2. The Bulk Acquisition Code further refers to sharing bulk communications data:

> *'6.18 Section 171 provides for the giving of any communications data acquired under a bulk acquisition warrant, or a copy of any such data, to any overseas authorities. For this to happen, the Secretary of State must first ensure that the overseas authority has in place retention, disclosure, and examination safeguards corresponding to those specified in the Act, to the extent the Secretary of State considers appropriate.'*

7.4. Interception

7.4.1. Similarly, in the Interception Code safeguards are only applied when intercepted content and secondary data, including unselected data, is shared with overseas partners to the extent the Secretary of State of issuing authority 'considers appropriate' [§9.18].

7.5. Bulk Personal Datasets

7.5.1. The Code states that consideration should be given to whether a BPD may be made available to an access by an international partner: *'4.5 … The review of the application should ensure that consideration has been given as to whether access to the dataset, whilst it is retained under the warrant may be made available to any other SIA or an international partner were it is necessary and proportionate to do so.;*

7.5.2. The Code states that §§7.5-7.6 apply to access to BPD via the electronic analysis systems.

7.5.3. Entire Bulk Personal Datasets may be given to foreign intelligence agencies:

> *'7.49 For the purposes of this paragraph, disclosure means providing a copy of a BPD or information held in a BPD to a third party. It does not cover third party access to BPD via the electronic analysis systems of the Security and Intelligence Agency which holds the warrant.'*

7.5.4. Not even the minimal safeguards apply where datasets are shared (*"…while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets")* (§163).

7.5.5. The Code states that: *'7.50 Disclosure of BPDs, or information in BPDs held by a SIA is not generally regulated by the IP Act.'*

7.5.6. Both the Codes and the Act lack effective safeguards in respect of both forms of sharing with third parties and do not set out who these could be (other government departments, industry partners, foreign governments).

7.5.7. **Recommendation: At the least, any safeguards relating to the dissemination of materials obtained under any of the powers governed by the Codes should apply equally when that material is shared with foreign governments.**

8. Extraterritorial Reach

8.1. In accordance with international law, the enforcement jurisdiction of a state to investigate, prosecute, or apprehend an offender extraterritorially is limited by the territorial sovereignty of the foreign state.[6] A state exercises what is called enforcement jurisdiction when it undertakes some form of executive action.[7] In the criminal context, the U.K. exercises enforcement jurisdiction extraterritorially when its law enforcement affects legal process coercively, such as to arrest someone, or to undertake searches and seizures abroad. It has been argued that "the customary international law rule against one state conducting investigative activities in another state's territory provides a strong basis for states to object to remote cross-border searches of data within their territory".[8]

8.2. The Codes adopt an expansive approach whereby U.K. law enforcement and intelligence agencies are provided with significant powers to engage in or facilitate extraterritorial searches and seizures. For example:

8.2.1. Technical Capability Notices: can be given to *"persons located outside the UK and may require things to be done or not done outside the UK"* [§7.27 Bulk Acquisition Code & §8.17 EI Code]

8.3. **Recommendation: UK government agencies should not be granted powers to conduct unilateral extraterritorial surveillance activities.**

9. Privileged Communications and Professional Protections

[6] *S.S. Lotus (France v. Turkey)*, 1927 P.C.I.J. (Ser. A), No. 10, pp. 18-19 ("Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention"); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW IN THE UNITED STATES §432(2) (1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); INTERNATIONAL BAR ASSOCIATION, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION, p. 10 (2009) (noting that a "state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial process in another state's territory without the latter state's permission").

[7] A state can exercise three types of jurisdiction: (1) prescriptive ("i.e. to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things"), (2) adjudicative ("i.e. to subject persons or things to the process of its courts"), or (3) enforcement ("i.e. to induce or compel compliance . . . with its laws or regulations"). Restatement (Third), supra, at §401.

[8] Patricia L. Bellia, *Chasing Bits Across Borders*, U. Chi. Legal F. 35, 77-80 (2001).

9.1. The Investigatory Powers Act offers an already limited set of protections for those who are involved in protected communications as part of their professional engagements.

9.2. The Codes of Practice continue this route by further limiting or providing disjointed protections for such communications. For example:

9.2.1. National Security Notices [3.8]: The NSN Code only references "journalistic information" and "data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information". With regards to both the Code notes that "it is not necessary to include more detailed safeguards" and refers to other codes of practice. The Code ignores other relevant professions (including medical and psychological professionals, welfare professionals, legislators, and the clergy).

9.2.2. EI [9.68, 9.76]: The EI Code clarifies that "equipment data may not be sufficient to identify a source", e.g. "identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship". This is not necessarily accurate, especially when you combine an address with time, location, and frequency of contact. Given the specific importance of maintaining the integrity of journalistic sources, it is crucial that the Code provides the highest level of protection when journalists' sources or journalistic material are involved.

9.3. **Recommendation: Re-evaluate the manner in which the Codes describe and elaborate on protections for privileged communications. The Codes should bring additional clarity, not confusion, to these protections and should in no way lower the level of protection mandated by the Act.**

10. Necessity and proportionality

10.1. At various points the Codes attempt to explain the concepts of necessity and proportionality. While an understanding of these concepts is crucial to ensuring that privacy is respected when a warrant or authorisation is issued, the attempts at definition do not necessarily facilitate that understanding.

10.2. For instance, the Interception Code at §4.10 declares the '*interception of communications, and the obtaining of secondary data from communications, is likely to involve an interference with a person's rights under the European Convention on Human Rights (ECHR)*.' Such interference is not only "likely" but almost a certainty.

10.3. The interception of communications constitutes an interference with the right to privacy of those communications under Article 8(1) of the European Convention on Human Rights, whether made via email, phone, text message, or on social media[9].

[9] See e.g. Klass v Germany, 6 September 1978, Series A No 28 at §41; Weber and Saravia v Germany, ECHR 2006 XI at §77; Kennedy v United Kingdom 26839/05 18 May 2010 at §118.

The same is true with respect to accessing communications data or 'metadata'[10]. Further interferences arise from the collection and retention of such material - especially on a searchable database - and its transmission to other authorities[11].

10.4. The European Court of Human Rights (ECtHR) has made no distinction as to the severity of the interference when the interception is effected by an automated system or computer. Indeed, the Court has found that the interception and/or storage of a communication constitutes the interference, and that the subsequent use of the stored information has no bearing on that finding[12].

10.5. In Liberty and Others v United Kingdom the ECtHR reiterated that the mere existence of powers "permitting the examination, use and storage of intercepted communications constituted an interference with Article 8 rights of the applicants" (at §57). This sentiment has been echoed by the United Nations High Commissioner of Human Rights who, in her report on the right to privacy in the digital age, noted that "[t]he very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.[13]"

10.6. We have also previously called for the inclusion of the test requiring consideration of whether other less invasive techniques have been exhausted. Whilst this has been included to a degree, we express concerns above regarding how 'less intrusive' has been interpreted in the Act and Code and the lack of transparency about how those exercising surveillance powers will interpret what is or is not less or more intrusive.

10.7. Compounding concerns regarding the guidance the Codes are providing on necessity and proportionality, in the context of National Security Notices, telecommunications operators may only express concerns about "reasonableness, cost, or technical feasibility of requirements" [4.4]. As such the operators may not raise any concerns about the necessity or proportionality of the measure.

10.8. **Recommendation: To the extent the Codes address the parameters of necessity and proportionality, those descriptions should be revisited to assure they are consistent with human rights obligations, and do not preclude additional, potentially helpful input into whether the exercise of any particular power is necessary and proportionate.**

11. Role of Judicial Commissioners

11.1. We have previously made submissions on the parameters of the 'judicial review' standard. The Codes fails to clarify this test and we maintain our position that Judicial

[10] See e.g. Malone v United Kingdom, 2 Aug 1984, Series A No 82 at §84

[11] See e.g. Amann v Switzerland [GC] ECHR 2000-II; and Weber and Saravia v Germany at §79.

[12] See e.g. Amann v Switzerland [GC] ECHR 2000-II at §69 ("The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding.")

[13] Report of the UN High Commissioner for Human Rights, the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014.

Commissioners should have the power to fully and completely assess whether a warrant is necessary and proportionate. We have noted in this submission our concern that the Codes refer to a review of the Secretary of State's conclusions rather than a full and complete assessment of the warrant.

11.2. We have set out in this submission in separate sections our concerns with limitations to the role of the Judicial Commissioners specific to certain Codes. We have also set out our concerns with the ineffective nature of the oversight role in respect of bulk powers, and our continuing objection that the bulk powers are unlawful. Further, we have noted the need to review the record keeping requirements for each Code to ensure the Investigatory Powers Commissioner has oversight of all aspects of the powers in the Act and the Codes. There are significant limitations on the scrutiny the Judicial Commissioners can currently exercise.

11.3. While the limited timeframe of this consultation has not permitted us to identify every instance in which the Codes evidences limitations on the Judicial Commissioners' role, we provide some further illustrative examples below.

11.4. In the Interception Code at §5.47, the Judicial Commissioner is allowed to 'seek clarification' from the agency seeking the warrant. It is unclear what seeking clarification encompasses. For instance, can the Judicial Commissioner require additional details in the warrant to circumscribe its scope or justify its necessity or proportionality? Can the Judicial Commissioner require additional people to be named in a thematic warrant? Can the Judicial Commissioner insist on a better description of the subject of the warrant or the selectors to be used? Can the Judicial Commissioner require additional protections for the "Integrity and security" of public telecommunications systems? What about protections for other security concerns unrelated to a public telecommunications system? The Code does not provide an answer to any of these questions.

11.5. The Bulk Acquisition Code has removed reference to certain duties of the Judicial Commissioner as follows:

11.5.1. Previously in sections §4.7 & §4.8 in the Autumn Code, authorisation of a bulk acquisition warrant required the Judicial Commissioner to consider whether the warrant is necessary for one or more of the statutory purposes; and whether the selection for examination of BCD obtained under the warrant is necessary for one or more of the specified operational purposes.

11.5.2. The updated Code has removed reference to the Judicial Commissioner being satisfied that the conduct authorised by the warrant is proportionate to what is sought to be achieved and considering whether the information sought could be obtained by other means.

11.5.3. The role of the Judicial Commissioner appears to have been limited to solely considering the Secretary of State's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved [§4.14]. Whether the Judicial

Commissioner can make an independent inquiry into these requirements, as was suggested by the previous language of the Autumn Code, is now less clear.

11.6. The Bulk Acquisition Code states that a minor modification may be made by the Secretary of State or by a senior official and does not require Judicial Commissioner approval. Included within minor modifications are the renewal of a bulk acquisition warrant that focuses solely on examination of bulk communications data.

11.6.1. We note the concerns we have about the existing breadth of bulk communications data that can be acquired under bulk acquisition warrants and the inadequate safeguards in relation to examination of bulk communications data, where the operational purposes are prospective and there is no requirement for a warrant at the point at which examination is carried out.

11.6.2. The Code states that *'...it may no longer be necessary, or possible, to continue the bulk acquisition of communications data ...it may continue to be necessary and proportionate to select for examination the data obtained under the warrant. The Act therefore provides that* ***a bulk acquisition warrant can be modified such that it no longer authorises the acquisition of communications data in bulk, but continues to authorise selection for examination of data already obtained*** *under the warrant.'* [§5.12]. *'Such a modification is a* ***minor modification*** *and may be made by the Secretary of State or by a senior official acting on their behalf.'*

11.7. The Bulk Acquisition Code includes further amendment powers that are not subject to judicial scrutiny. It states *'In accordance with section 164(12), a SIA is permitted to amend a warrant as long as as such an amendment does not alter the conduct that is authorised by the warrant.'* This appears a broad and unspecific power which should be further clarified in the Code.

11.8. The Bulk Personal Datasets Code states, at §5.16, that bulk personal datasets may be aggregated to allow for pattern identification and profiling. However, this is not accompanied by any additional scrutiny or oversight, despite its potential to be highly intrusive:

> *'The analysis of bulk systems data and identifying data (referred to hereafter as non-protected data, which comprises the majority of data in BPD) is one of the key means by which the Security and Intelligence Agencies are able to discover and assess threats to the UK. This generally involves the aggregation of non-protected data from a wide variety of sources acquired under multiple bulk warrants. Such analysis allows the Agencies to draw together fragments of information into coherent patterns which allow for the identification of those threats while at the same time minimising intrusion into privacy.'*

12. **Inadequacy of safeguards for bulk powers**

12.1. The Codes refer to the safeguards in place for bulk powers and in particular the role of the Judicial Commissioners. However, we question whether these can ever really be classed as safeguards given that the warrants largely authorise broad, prospective powers without any of the specificity of a traditional warrant based on individualised suspicion. In this context the safeguards, even as explored in the Codes, appear illusory.

12.2. Bulk warrants subvert the traditional investigative process, by which the Government has reason to suspect someone and applies for a warrant to surveil that person. Bulk warrants permit the intelligence agencies to surveil everyone. The broad scope of bulk warrants means the authorisation process falls short of what is required under international human rights law. In particular it leaves the authorities unable to verify *"the existence of reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."*[14]

12.3. Given that bulk warrants do not specify the nature of the offence each individual whose data will be acquired and examined is alleged to have committed, the powers by nature place large groups of people under surveillance without suspicion. This in admitted in the case of Bulk Personal Datasets.

12.4. The requirements of some of the warrants are so vaguely formulated that they will make it next to impossible to assess the necessity and proportionality of the envisaged measure.

12.5. The EI Code admits that the Secretary of State and the Judicial Commissioner, cannot effectively assess necessity and proportionality in authorising bulk hacking:

> §6.5 (bulk): "*To determine whether a thematic or bulk warrant is appropriate, regard must be given . . . to whether the Secretary of State is able to foresee the extent of all the interferences to a sufficient degree to properly and fully assess necessity and proportionality at the time of issuing the warrant. This includes consideration of interferences in relation to all those individuals affected . . . . Where this can be done . . . a thematic warrant is likely to be most appropriate.* ***This is because the additional access controls of the bulk regime are not required if a greater degree of targeting . . . can limit interference such that the Secretary of State and the [JC] can adequately address all of those considerations (e.g. necessity and proportionality, purpose, protection for UK persons' content) from the outset***."

12.6. Bulk hacking – whether carried out under a thematic warrant or under the explicit "bulk" power – destroys the ability of the authorising authority to assess necessity and proportionality. How can the authorising authority properly make such an assessment

[14] Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 260.

without knowing which computer is to be hacked, what information might be contained on that computer, who else might be using it, or the level of suspicion that attaches to the individuals using the computer? Indeed, the Home Office has admitted as much, noting in its operational case for bulk powers:

> A bulk EI warrant is likely to be required in circumstances where the Secretary of State or Judicial Commissioner is not be able [sic] to assess the necessity and proportionality to a sufficient degree at the time of issuing the warrant.

12.7. The procedure to be followed for examining, sharing, retaining and deleting material or data obtained through 'bulk' warrants do nothing to alleviate the concerns caused by such insufficient authorisation. These "safeguards" are too broad and vague to provide sufficient guidance and prevent abuse. In particular, the disclosure and copying of information obtained under a 'bulk' warrant is broadly permitted so long as the information is or is likely to become necessary in the interests of national security or other relevant grounds.

12.8. Further, with regard to Bulk Personal Datasets and Bulk Acquisition, there are no provisions for a 'targeted examination warrant' in the Act. The Code does nothing to provide safeguards to remedy this deficiency despite this being highlighted in submissions relating to the Act itself.

12.9. **Recommendation: In view of the nature of the bulk powers and the inherent inadequacies of authorisation, it is impossible to recommend an effective safeguard other than the removal of bulk surveillance powers and replacement with targeted powers.**

13. Problems with the IPC's role in oversight

13.1. While we have not had time to provide a full assessment of the Investigatory Powers Commissioner's role as defined in the Code, we highlight an area of particular concern which is the inability of the Commissioner to allow for public scrutiny of secret interpretations of the Act and Codes.

13.2. A large number of powers in the Investigatory Powers Act will operate in secret. There is no provision in the Act or Codes for review of secret law and secret interpretations of certain words, phrases and powers. This review should be undertaken by the Investigatory Powers Commissioner.

13.3. Further, there must be a process to make such the interpretations of the Act and Codes available for public and Parliamentary scrutiny.

13.4. To provide a specific example, with regard to National Security Notices [§5.3]: While the Code establishes that the IPC will have "*unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties*", and while the Code further clarifies that "*telecommunications operators may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit*", at the same time the Code establishes harsh gag

provisions and prohibitions on disclosures, giving all the power to the Secretary of State [§§4.6-4.7].

14. Record keeping

14.1. We are concerned that the record keeping required in the Codes, which is a key aspect of oversight, is inadequate.

14.2. **Recommendation: The record keeping section of every Code should be reviewed on an annual basis as an additional part of the Commissioner's' functions to ensure that gaps in record keeping are prevented and areas do not fall outside of oversight.**

14.3. The Codes contain insufficient requirements for recording the sharing of data with foreign partners, industry and other government departments.

14.4. In the Bulk Acquisition Code, there seems to be insufficient requirements for record keeping in relation to the actual examination of bulk communications data (see concerns raised in relation to examination below) and the use of bulk communications data for 'authorised purposes'.

14.5. In the EI Code, there is no requirement to keep an audit trail for each EI operation. As use of EI develops there are a number of records that should be kept, which may develop over time, such as the number of exploits used, the number of exploits disclosed for patching and so on.

14.6. In relation to the Bulk Personal Datasets Code, we submit that further consideration should be give to this section and it should include a number of matters we have raised in submissions on Bulk Personal Datasets. There are references to being able to make oral decisions, such as by the Judicial Commissioner. This is unacceptable. All decisions must be recorded.

15. Error reporting

15.1. There must be a requirement for notification in the Act and Codes. The reference to notification in the Codes is inadequate.

15.2. We note that as per the judgment of the Court of Justice of the EU (Grand Chamber) of 21 December 2016 ("the Watson CJEU judgment") in 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 & others (ORG and PI intervening)* (the "Watson Proceedings"):

> *"121. Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigation being undertaken by those authorities. That*

notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to legal remedy."

15.3. The current error reporting provisions in the Codes are insufficient to fulfill this requirement. For instance, in the EI Code:

15.3.1. According to the EI Code, an "*error can only occur*" after interference or selection for examination has "*commenced*," thereby excluding other types of errors or the mere fact that an EI operation has commenced from this definition. [§10.13 EI Code]

15.3.2. Moreover, errors are only reported to the Investigatory Powers Commissioner if it is considered to be a "*relevant error*," which is a narrow band of errors, including EI without lawful authority and failure to adhere to certain safeguards and restrictions on disclosure. [§§10.14-10.15 EI Code]

15.3.3. Finally, errors are only reported to a person subjected to EI if it constitutes a "*serious error*." A "*serious error*" requires that there be "*significant prejudice or harm*" although these terms are not further defined in the Code. A breach of a person's rights under the European Convention on Human Rights "*is not sufficient by itself for an error to be a serious error*." [§10.26 EI Code]

16. **Urgent Authorizations of Warrants**

16.1. The Codes define urgency, for the purposes of allowing the urgent authorisation of warrants without prior approval from a Judicial Commissioner, in too broad a fashion. This applies equally to both targeted and bulk warrants.

16.1.1. Urgency "*is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the time available to meet an operational and investigative need*." Urgent warrants fall into one of two categories: (1) imminent threat to life or serious harm; or (2) an intelligence-gathering or investigative opportunity with limited time to act" [§§5.61, 6.27 EI Code; §5.52 Interception Code]

16.1.2. The Codes provide varying examples of what category 2 warrants might look like. These include "*a consignment of Class A drugs is about to enter the UK and law enforcement agencies want to have coverage of the perpetrators of serious crime in order to effect arrests*" and "*a suspect is believed to be involved in the illegal sale of military grade weapons and is planning to visit the UK on business. Their travel plans are uncovered at short notice as their passport allows visa-free travel to the UK and they made a late booking. It is a brief visit, only 2 days, beginning in 24 hours time. This will present a unique opportunity to intercept their communications to learn more about their associates here in the UK*" [*Id.*]

16.1.3. Insofar as the test is, as defined in the Codes, whether it would be "*reasonably practicable*" to seek approval from a Judicial Commissioner, it is hard to see why in either of the two examples provided in the Codes such approval could not be sought. The first example does not indicate the timeframe for seeking the approval and the second suggests approval would be needed within 24 hours. With proper resourcing, it is unclear why approval could not be sought from a Judicial Commissioner within 24 hours. No explanation is provided as to why this is too short a timeframe.

16.1.4. ***Recommendation*: Provide a narrower definition of what category 2 urgency means ("investigative opportunity with limited time to act") explaining what type of situations might limit the ability to seek JC approval ahead of time.**

SECTION B

17. We set out below our concerns that are specific to a particular code. These are the most significant concerns we have identified in the short space of time we have had to consider the Codes. It is not a comprehensive review, as a result of the limitations identified in the introduction.

18. **Equipment Interference Code of Practice**

18.1. *Scope of Application*: The EI Code permits a warrant to be obtained for "*communications, equipment and other information*" [§2.3]. There is no detail as to what "*other information*" means in practice. Furthermore, the definition of "equipment" is so broad as to permit EI against virtually any connected device, which increasingly not only includes our phones, laptops and tablets, but just about any other physical object, including cars, refrigerators, thermostats, pacemakers and toys.

18.1.1. ***Recommendation*: Define what "Other Information" means. Limit the scope of EI to well-defined and bounded categories of information and "equipment".**

18.2. *Methods of EI*: EI can be carried out "*remotely*" or by "*physically interacting with the equipment*" [§3.2]. "*At the lower end . . . an agency may use someone's login credentials to gain access to data*" and "*complex [EI] operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device*" [§3.3]. The Code entirely glosses over distinctions between techniques, despite the fact that different techniques (for example a bulk "waterhole" attack compared to a tailored social engineering attack) may present varying privacy and security implications and require tailored safeguards. It also ignores the fact that certain techniques - such as the use of software vulnerabilities that haven't been disclosed to manufacturers - should perhaps be prohibited altogether due to their overarching security ramifications.

18.2.1. ***Recommendation*: Define and issue specific guidelines for each method of EI proposed to be utilised.**

18.3. *Hacking against Non-Suspects*: The Code determines that it is lawful to conduct EI against devices used by individuals who are not themselves "*suspected of direct or culpable involvement in the overall matter being investigated*," but surveillance of whom might nonetheless assist the overall investigation. The example provided in the Code is of an associate of a target of an investigation, and who could assist the identification of the location of that target. [§5.53] This runs counter to the basic principle laid down by the European Court of Human Rights whereby "*reasonable suspicion*" must be verified before it is found lawful that a person may be targeted by surveillance measures (see, e.g., Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment, para. 260 (4 December 2015)). As the Court noted in Weber v. Germany, App. No. 54934/00 (29 June 2006): "*the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications*."

18.3.1. **Recommendation: prohibit any form of EI against individuals against whom there is no reasonable suspicion for being complicit in the overall matter being investigated.**

18.4. *EI Assistance Not Requiring Service of a Warrant*: The Code clarifies that the process of issuing EI warrants "*does not prevent equipment interference agencies and providers working co-operatively together (without the need for service of a copy of an equipment interference warrant in accordance with section 127)*" [§7.6]. Thus the Code suggests that in certain circumstances, the process required before a company is compelled to assist in effecting a warrant is dispensed with altogether. We maintain that that process itself is inadequate. Regardless of whether a private provider is willing to engage in cooperation with governmental authorities, such cooperation should nonetheless be judicially reviewed and authorized by a Court.

18.4.1. ***Recommendation*: Remove any reference to EI assistance that does not require service of a warrant.**

18.5. *Discrepancies in Safeguards for Law Enforcement and Intelligence Agencies*: Sections 128(2) and 128(5) of the Act establish a discrepancy in the level of safeguards for EI warrants issued by law enforcement and those by intelligence agencies. The Code of Practice reiterates this discrepancy: for security and intelligence agencies there is a "*requirement on providers served with a warrant . . . to take all reasonably practicable steps for giving effect to the warrant*" [§7.7] and for law enforcement there is a "*requirement on providers to take all such steps for giving effect to the warrant as were approved by the Secretary of State . . . steps that are required to take are limited to those that the Secretary of State has expressly approved as necessary and proportionate*" [§7.8]. Another example of a discrepancy exists in the modification of a warrants. Whereas warrants issued by the Secretary of State to intelligence agencies can be unilaterally modified without JC approval

[§§5.74, 5.80] warrants issued by law enforcement chiefs or delegates must receive JC approval prior to modification [§5.82].

18.5.1. ***Recommendation*: Ensure that equivalent, and highest, safeguards are maintained for EI for law enforcement purposes and EI for intelligence agencies' purposes.**

18.6. *Specificity of Assistance to Effect a Warrant*: The Code establishes that EI assistance "*will typically comprise (but may not be limited to) the provision of infrastructure by a relevant communication service provider, or details about the technical specification of relevant equipment*." [§7.9] The definition as currently provided lacks sufficient detail.

18.6.1. ***Recommendation*: Provide better clarification of the types of categories of assistance envisioned including more robust examples to meet the requirement of foreseeability.**

18.7. *Disclosures*: The Code elaborates on what "*expected disclosure*" as required under Section 133 of the Act entails. The Code notes that "*in accordance with regulations made by the Secretary of State*," telecommunications operators may publish "*statistics relating to the number of warrants to which they have given effect*" [§9.9]. The Code is vague, leaving open the question of whether the Secretary's regulations will be made public and the extent to which they would infringe on the practice of telecommunications operators to publish transparency reports that contain adequate information regarding the assistance they have provided. Of particular concern is the extent to which the regulations will demand that any disclosures be made in overly generalized terms.

18.7.1. ***Recommendation:* Provide more clarity and specific instructions as to the regulation of disclosures, and require such regulations, once completed, to be made public and open to scrutiny.**

18.8. *Warrant laundering*: The Code allows for one agency to approach another agency and ask it to obtain an EI warrant on its behalf. The Code gives the example "*where a police force considers that there is not sufficient resources available to ensure the protection of a sensitive technique, it may approach the NCA to obtain the warrant*". [§5.124] This in essence authorises the laundering of warrant applications. Consider for example a situation where the scope of powers or mandate of one agency differs from another (e.g. extraterritorial hacking powers) - in that case would the powers of the agency obtaining the warrant also transfer over to the implementing agency?

18.8.1. ***Recommendation*: Remove any reference in the Code to the ability of one agency to request another seek an EI warrant on its behalf.**

18.9. *Review of Warrants*: The Code provides that "*unless specified by issuing authority, the frequency of reviews should be determined by the equipment interference agency who made the application. This should be as frequently as is considered necessary and proportionate*" [§9.19]. Agencies should not make this determination. The

decision should be left with the Judicial Commissioner, who should also determine the length of warrants.

18.9.1. ***Recommendation*: Assign mandated responsibility for decision on length of warrants and frequency of reviews to the Judicial Commissioner.**

18.10. *Non-IPA Hacking not Subject to Judicial Review*: The Code still leaves open the possibility for EI to be conducted without judicial review, as long as it is permitted under other authorities. The ability for government agencies to conduct EI under other statutes is inherently confusing and defeats one of the core purposes of the Act. An example of this is provided in the Code: "*A security and intelligence agency wishes to conduct an operation which involves property interference (provided for under section 5 of the Intelligence Services Act) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications . . . In approving the decision to issue the warrant, the Judicial Commissioner would only consider the application for targeted equipment interference*" [§5.110].

18.10.1. ***Recommendation*: The Code must clarify that no EI operation should ever be authorised without judicial review.**

18.11. *International Cooperation*: The Code establishes that "*where an [EI] agency requires an international partner . . . to undertake an action authorized by an [EI] warrant, this must be specified in the warrant application, including why the assistance of an international partner is required*" [5.119]. Furthermore the Code confirms that "*in cases where it is necessary and proportionate for material obtained under the warrant to be made available to another of the security and intelligence agencies or an international partner, the operational purposes specified in the warrant may include operational purposes relating to that third party providing*" that the section 178(1)(d) test is met [§6.15]. To ground these activities in the Act the Code relies on Section 99(5)(b). In essence this language in the Code authorises the conduct of joint EI operations and sharing of information collected through EI with foreign agencies, by relying on a section of the Act which was not originally designated for that purpose. The U.K. is under an obligation to ensure that "*robust oversight systems*" exist over "*intelligence-sharing of personal communications*" (Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)). This begins by clearly specifying in primary legislation any form of intelligence cooperation of the kind envisioned in the Code. This is particularly true in the context of EI which poses greater risks to the security and integrity of networks and systems and poses potentially greater interferences with the privacy of individuals.

18.11.1. ***Recommendation*: The Code should not introduce any new intelligence sharing powers beyond those expressly stated in the Act. Any such sharing or cooperation should be governed by primary legislation.**

18.12. *Oversight over Central List of Operational Purposes*: Section 183 of the Act requires the Heads of the Security and Intelligence Agencies to maintain a central list of all the

operational purposes, which they consider are purposes for which material may be selected for examination. However the Codes does not mandate any independent authorization of this list or oversight over it [§6.63].

18.12.1. ***Recommendation*: Subject the "List of Operational Purposes" to a mandated independent review process.**

18.13. *Cancellation and Destruction Procedures:* We are concerned about the adequacy of provisions around cancellation and destruction in the EI Code. The Code notes that "*in some circumstances it may be impossible, or not reasonably practicable, to cease all elements of interference upon cancellation of a warrant*." Moreover, the Judicial Commissioner or relevant official "***may** dictate whether such information is destroyed and **may** impose conditions on its use.*" [§§5.91-5.92, 5.94, 6.36-6.37, 6.59 EI Code]

18.13.1. **Recommendation: The cessation of interference in the circumstances above must be mandatory. The suggestion that it "may be impossible" in certain circumstances is unacceptable. The cessation of interference should also be mandatory at the conclusion of an EI warrant, a safeguard that is not currently provided for in the EI Code.**

19. Bulk Acquisition Code

19.1. At the outset, as noted above, Privacy International maintains that no amount of safeguards can make the bulk acquisition of data compliant with the requirements of UK law and the ECHR. However, even some of the attempts at safeguards provided in the Act have been undermined by a lack of clarity in the Bulk Acquisition Code. We provide examples of that lack of clarity in this section.

19.2. The bulk acquisition power permits the acquisition of an unlimited volume of communications data:

> *'3.4 In contrast to a targeted communications data authorisation issued under Part 3 of the Act, a bulk acquisition warrant need not be constrained to a specific operation.'*
>
> *'3.5 Chapter 2 of Part 6 does not impose a limit on the volume of communications data which may be acquired . . . the acquisition of all communications data generated by a particular CSP could, in principle, be lawfully authorised but only where necessary and proportionate to do so.'*

19.3. The Bulk Acquisition Code, as a result of changes from the previous version has added confusion to the examination aspect. We seek clarification of the following:

19.3.1. That a bulk acquisition warrant can only permit the examination of the communications data that has been obtained under the warrant. It cannot permit the examination of communications data obtained by previous or future bulk acquisition warrants. It cannot specify selection for examination

of communications data acquired under a different bulk acquisition warrant or obtained through a process / procedure outside the bulk acquisition regime.

19.3.2. The Code states '*A bulk acquisition warrant under that Chapter is a warrant which authorises or requires the person to whom it is addressed to obtain the communications data described in the warrant from a telecommunications operator,* ***as well as to select for examination the acquired communications data,*** *as specified in the warrant.'* [§1.2]

19.3.3. The Code states at §5.3 that *'In the case of a renewal of a bulk acquisition warrant that has been modified so that it no longer authorises or requires the acquisition of communications data in bulk, it is not necessary for the Secretary of State to consider that acquisition of communications data continues to be necessary before making a decision to renew the warrant.'*

19.3.4. It appears based on the above that a warrant can be renewed solely on the basis of examination and not in relation to acquisition.

19.3.5. Equally, given that the Code has removed reference to acquisition and examination being a two step process, it is unclear whether a bulk acquisition warrant could be used solely for examination. This must be clarified.

19.4. It is also unclear whether selection for examination of communications data has any effective limitation.

19.5. The requirement that bulk acquisition always be necessary in the interests of national security appears clearly applies to acquisition, but is vague with regard to selection for examination. This must be clarified.

19.5.1. Prior to submission, each bulk acquisition application involves consideration of whether the application is necessary for one or more of the permitted statutory purposes. A bulk warrant must always be necessary in the interest of national security. [§4.4]. The warrant refers both to acquisition of communications data and examination. There is a lack of clarity whether the acquisition of communications data must always be necessary in the interests of national security and the examination of communications data must always be necessary in the interest of national security.

19.5.2. It appears from the Code that the requirement to always be necessary in the interest of national security only attaches to the acquisition of communications data and not to the examination of communications data. The information which should be contained in the form only requires *'An explanation of why the acquisition of communications data in bulk is considered to be necessary for one or more of the statutory purposes,*

which must always include an explanation of why the acquisition of the data is necessary in the interests of national security'. [§4.5]

19.5.3. The review of the application prior to submission considers whether acquisition of communications data is necessary and proportionate. However it does require that the examination of communications data must be necessary and proportionate; instead, the review must consider *'whether the examination of that material is, or may be, necessary for each of the operational purposes specified.'* [§4.4]

19.5.4. There is no requirement for any further, specific examination warrant at the point examination takes place. [§4.9].

19.6. The Code sets out in Chapter 6 the examination safeguards. These revolve around the 'operational purposes'.

19.6.1. Selection for examination *'may only be carried out for one or more of the operational purposes that are specified on the warrant'*. It states that *'Operational purposes limit the purposes for which data collected under the warrant can be selected for examination'.* [§6.2].

19.6.2. However, it then goes on to state that *'Communications data selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for* ***any of the authorised purposes.*** [§6.2]

19.6.3. It is unclear whether there is any relation between the 'operational purpose; and the authorised purpose. The authorised purpose is not the 'operational purpose' authorised via the warrant that is referred to at the start of the paragraph. Instead, authorised purpose appears later in the Code under chapter 9 'General Safeguards':

> *'9.2 Section 171 of the Act requires that disclosure, copying and retention of data obtained under the warrant is limited to the minimum necessary for the authorised purposes. Section 171(3) of the act provides that something is necessary for the authorised purposes if it:*
>
> - *Is, or is likely to become, necessary in the interests of national security or on any other purposes falling within section 158(2)...*
> - *Is necessary for facilitating the carrying out of the functions under the Act …*
> - *Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution;*

19.6.4. It appears that once selected for examination by reference to an operational purpose (see below on inadequacies of operational purpose) the communications data can be disclosed for use of another purpose. This undermines the safeguards.

19.6.5. There is also no clear role of independent oversight in relation to what happens to communications data obtained under a bulk acquisition warrant and the above indicates that there may be large scope for use of this data with little in the way of checks and oversight.

19.7. Request filter

19.7.1. The Bulk Acquisition Code refers to the request filter as less intrusive [§4.12]. There is no information on how the request filter will operate. It is therefore unacceptable to assert that the request filter is less intrusive.

20. National Security Notices

20.1. *Categories of NSNs*: The Code does not set out "*an exhaustive list of the type of conduct that might be required by a national security notice*" [§3.2]. The Code further notes that "*it is not possible to give a list of the full range of the steps that telecommunications operators may be required to take in the interests of national security*" as that would affect the ability of intelligence agencies and the police to carry out their work and in light of the need for flexibility to respond to new technologies [§3.3]. The result, however, is that the Code offers no foreseeability and in essence subjects the telecommunications operators to a regulatory regime whereby anything can be enforced on them.

20.1.1. ***Recommendation*: The Home Office should, at the very least, attempt to identify broad categories of NSNs that may be issued to telecommunications operators so to set some generalized parameters to the practice.**

20.2. *NSNs Interference with Privacy*: The February 2017 version of the Code eliminated the requirement that appeared in the 2016 autumn version, according to which "*a National Security Notice cannot be used for the primary purpose of interfering with privacy, acquiring communications or data*" [§3.6]. Instead the new Code establishes that a notice cannot be given "*when the main purpose of the notice is something for which a warrant or authorisation under a relevant enactment is required*" [§§3.4-3.5]. This in turns allows for an NSN to be issued with the primary purpose of interfering with privacy in cases where a warrant or authorisation are not required by law or when such warrant or authorisation is not available. Moreover, the Code further clarifies that an NSN may be issued where the privacy interference "*is incidental and cannot be authorised by other means*".

20.2.1. ***Recommendation*: Reintroduce previous language and prohibit any NSN whose primary purpose is to interfere with privacy. Similarly**

prohibit any use of the NSN to circumvent lack of statutory authorisations to obtain data and interfere with privacy protections.

20.3. *Lack of Clear Oversight*: The Code establishes that the Secretary of State may only give a notice after considering whether there are "satisfactory safeguards in place" [§3.15]. The Code does not establish in any way what safeguards would meet this test. Moreover, the Code clarifies that only the Secretary of State may decide when a disclosure relating to NSNs may be made, including to "*relevant oversight bodies*" and to "*regulators*" [§4.7]

20.3.1. ***Recommendation*: Clarify what safeguards must be put in place before a NSN may be lawfully issued. The Code should clarify that relevant oversight bodies, including administrative, judicial, and parliamentary bodies, should be granted complete access to all materials relating to NSNs.**

20.4. *Temporal Limitations*: The Code does not set any temporal limitations on National Security Notices. While the Notice must "*specify the period within which the steps specified in the notice are to be taken*" such is left to discretion of the Secretary of State based on whatever deemed reasonable to him or her [§3.16]. Therefore the notice "*remains in force until it is cancelled*". Equally troubling is the fact that while the 2016 autumn version required a review be conducted "*at six monthly intervals*" [§3.12] the 2017 version establishes that the review will take place "*at least once every two years*" [§3.17].

20.4.1. ***Recommendation*: Introduce temporal limitations on NSNs and require renewal once every specified period, this could be tied to a reintroduction of the six month mandatory review process.**

20.5. *Unanticipated Privacy Interferences*: The Code establishes that each review process must "*consider whether any interference with privacy has occurred since the last review that was not anticipated, and the Secretary of State must be satisfied that any continued interference is justified*" [§3.17].

20.5.1. ***Recommendation*: The Code should establish that whenever an unanticipated interference with privacy occurs, a review process is immediately triggered. There is no justification to wait until a scheduled review finally takes place, before such privacy interferences are studied.**

20.6. *Mandatory Revocation of NSNs*: the 2016 autumn version of the Code required that a NSN "*must be revoked in whole or in part if it's no longer necessary to require a telecom to provide a national security capability*" [§4.24]. This provision was taken out entirely from the 2017 version of the Code.

20.6.1. ***Recommendation*: Reintroduce the requirement.**

20.7. *Proportionality Assessment*: Whereas the other Codes reference an obligation to consider whether a measure is the least intrusive [*see e.g.* Interception Code §4.15: "*the following elements of proportionality should therefore be considered: ...how and why the methods to be adopted will cause the least possible interference to the subject and others*"], the NSN code does not make any such reference to exhaustion of less intrusive measures [see §3.7].

20.7.1. ***Recommendation*: Elaborate on what the standard of proportionality will entail in the NSN context.**

21. Interception Code of Practice

21.1. We have raised a number of concerns in other areas of this submission that relate to interception. We are limited in time due to the short consultation period and only make on further limited observation in respect of interception.

21.2. We note that targeted warrants [§5.6-5.10] allow for very broad categories even when not considered "thematic". We have concerns about the examples given and recommend elaboration of these examples in the Code, particlularly to enable Parliamentary and public scrutiny of these powers.

22. Bulk Personal Datasets

22.1. Privacy International has consistently called for the deletion of Part 7 of the Investigatory Powers Act in relation to Bulk Personal Datasets ("BPDs"). It maintains this position. However, should Bulk Personal Datasets come into force, we make the following observations and recommendations in relation to the Code of Practice.[15]

22.2. We highlight a number of concerns in relation to the following areas, which, beyond the criticisms we have raised in relation to the Act, further limit transparency, expand powers in relation to Bulk Personal Datasets and undermine safeguards. These areas are:

a. The initial examination phase;
b. Class warrants;
c. Specific warrants;
d. Categorisation of data;
e. Types of datasets.

22.3. Initial examination phase

22.4. **Recommendation: the initial examination / preliminary phase / destruction phase and any other activities that currently appear to fall outside the Code**

[15] See Submission to the Joint Committee on the Draft Investigatory Powers Bill, 21 December 2015, para 274 'Recommendations" Delete Part 7'
https://www.privacyinternational.org/sites/default/files/Submission_IPB_Joint_Committee.pdf

must fall within a regime which includes independent oversight and safeguards.

22.5. There is little detail in the Act about the 'initial examination' / 'preliminary examination'. The Code states that it *'must be followed before bulk personal datasets can be retained and examined'* [§1.1] It further states that *'Section 199 of the Act specifies that a Security and Intelligence Agency "retains" a BPD for the purposes of the Act if, **after** any initial examination of the contents, it retains a BPD…'*. [§2.3] [emphasis added] The Code thus does not apply to the 'initial examination', nor it appears do many of the safeguards in the Act applicable to Bulk Personal Datasets.

22.6. It is made explicit that a warrant is not required for initial examination:

> *'2.8 Section 220(5) makes it clear that a Security and Intelligence Agency is not in breach of the requirement for a warrant to retain BPD for the period between deciding (as part of the initial examination) that it wants to retain a BPD and the determination of the Security and Intelligence Agency's application for a specific BPD warrant for that BPD.'*

22.7. The initial examination stages involve a number of activities. Again, neither the Code nor any safeguards or independent oversight appear to apply to the obtaining / acquiring / collecting a BPD, accessing the BPD and assessing of the *'intelligence or investigative value' [§2.4]* of the BPD. This is all part of the initial examination.

> *'As section 220 makes clear, the initial examination enables the Security and Intelligence Agency, when it **comes into possession** of a dataset, to **carry out a preliminary examination** of the contents with a view to establishing whether it is a BPD, and whether that BPD if of a nature that the Security and Intelligence Agency would wish to retain and/or examine it.' [§2.4]* [emphasis added]

22.8. The Code states *'This initial examination may only be carried out by a Security and Intelligence Agency for these limited purposes, and not for the purposes of any intelligence investigations or operations.'[§2.5]*. It is unclear what 'limited purposes' would fall within the permitted activities that take place during the initial examination: There is no reassurance that this is in fact 'limited' in terms of what can be undertaken.

22.9. **Recommendation: There should be an exhaustive list or definition as to what can be carried out under 'initial examination' and clarification as to what the limited purposes are, which do not fall under intelligence investigations or operations. There can then be effective public scrutiny regarding this phase, which at the least should be subject to independent authorisation, safeguards and oversight.**

22.10. <u>Class BPD Warrants</u>

22.11. The language in the Code indicates a wide interpretation for what could fall under a class warrant:

> *'4.7 Class BPD warrants are for those datasets which are **similar** in their **content** and **proposed use** and **raise similar considerations** ... This allows the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class,… for example … travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.'*

22.12. As we have previously stated, the class BPD warrant is unacceptably broad and prior to a BPD even having been obtained, it justifies the retention and examination of a BPD. The result is that at both the stage of retention and examination of a BPD deemed to fall under the class BPD regime, there is no independent authorization or oversight.

22.13. Neither the Act nor the Code clarify who makes the decision whether a BPD falls under an existing class warrant.

22.14. By way of example of the breadth of a class BPD warrant, the Code states that a class BPD could cover travel routes. This could include a wealth of datasets without any independent oversight for the retention and accessing of each one, including ANPR datasets, passenger name records, oyster card data, train travel, credit card data associated with bookings, IP addresses, IMSI and IMEI numbers collected by transport networks, and so on.

22.15. Even an unsolicited BPD can be waved in under the class BPD regime with no oversight:

> *'2.8 …. This is most likely to occur where a BPD is unsolicited, because a Security and Intelligence Agency will not have had the opportunity to assess whether the BPD is covered by a class warrant.'*

22.16. The Judicial Commissioner approving a class warrant only reviews the 'Secretary of State's conclusions' in the warrant. Actual oversight of particular BPD's is thus woefully inadequate.

22.17. **Specific BPD warrants**

22.18. While a specific BPD warrant is still objectionable, it at least provides further potential for an assessment of the necessity and proportionality of obtaining a particular dataset.

22.19. However, the Code states that using a specific BPD warrant is the exception:

> *'4.22 In general, it is expected that there are likely to be few scenarios where a Security and Intelligence Agency is likely to consider it necessary to apply*

for a specific warrant, rather than a class warrant, other than in circumstances where the SIA is required to apply for a specific warrant under section 202.'

22.20. The previous Code was clear that specific BPD warrants should be used where the BPD is relatively more intrusive. However, as noted the previous section 4.17, or what is intrusive has been deleted.

22.21. Further, changes in the Code make it unclear whether *'4.18 …selection for examination of data from BPDs could reveal the sources of journalistic material'* still require a specific warrant or now can fall under class BPD warrants.

22.22. It is a concern given the nature of the data that a specific BPD warrant can be issued without conditions:

> *'4.50 Where the Secretary of State is satisfied that the selection for examination safeguards are sufficient, the Secretary of State may issue the warrant without conditions.'*
>
> The Code states that *'4.49 … The section 221 safeguards are likely to be adequate and sufficient to provide the necessary Article 8 protections in cases where the BPD comprises a dataset containing protected data of low level of intrusiveness (for example, protected data contained in a travel BPD provided by a prospective traveller to a service provider or in an internet dataset with minimal privacy settings which is accessible by a very large user group).*

22.23. It is extremely unclear what the Code is referring to at 4.49. Is it stating that if a large travel company has a dataset of its customers which is not secure, then by default the data is 'low level of intrusiveness?'

22.24. The Code at 4.28 appears to exclude oversight:

> *'4.28 Section 205(6) also enables a Security and Intelligence Agency, when applying for a specific BPD warrant in respect of a particular BPD ('dataset A'), to request* ***at the same time*** *that the authorisation should extend to the retention and use of* ***replacement datasets****, i.e. other bulk personal datasets that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.'*

22.25. §4.10 This wholly undermines independent oversight and should be deleted. Every BPD that falls under the Specific BPD warrant regime, whether deemed to be a replacement dataset or not, requires independent oversight.

22.26. **CATEGORISING DATA**

22.27. **Recommendation:** The Code should delete '4.37' and replace it with language that accepts that datasets comprising data from social media engages Article (8) and represents a significant intrusion to private life.

22.28. **Recommendation : The Government must explicitly state whether it seeks to use the Investigatory Powers Act to gather open source intelligence and social media intelligence in addition to or instead of RIPA**.

22.29. We are extremely concerned by the Code's language in relation to what is an is not private data. For example:

> *4.37 When categorising data contained in a BPD, the Agencies should first consider whether the dataset as a whole comprises data that are not "private information". For example a dataset consisting of data which is publicly accessible online could be categorised as non-private information, in circumstances where there is* ***no expectation of privacy over that information****.* ***There is unlikely to be an expectation of privacy where data has been posted online and the purpose is to communicate that information to a wide audience****. By contrast, information posted on personal social network sites normally accessed by a smaller circle of personal contacts may include information to which an expectation of privacy would apply.*
>
> *4.42 Private information includes information relating to a person's private or family life. In the BPD context, information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, commercial subscription databases, academic articles, conference proceedings, business reports,* ***and more****. Such information may also include commercially available data where a fee may be charged and any data which is available on request or* ***made available at a meeting to a member of the public****. Non-private data may also include the attributes of inanimate objects such as the class to which a cargo ship belongs.*

22.30. We strongly dispute that there is no expectation of privacy over data that is publicly accessible online and posted online, the purpose of which is to communicate that information to a wide audience.

22.31. This is not addressed at all in the Act. It is not acceptable to define what is and is not private data and where there is no expectation of privacy in a Code of Practice. The government have not at any time indicated that social media monitoring / social media intelligence and open source intelligence fall under the Investigatory Powers Act, that they will be collected under the 'Bulk Personal Datasets' regime and that it is depend this does not engage privacy rights as 'there is no expectation of privacy.'

22.32. Though ostensibly 'overt', social media and other platforms where data is posted online, engage individual privacy. By way of example 'tweets' posted from a mobile phone can reveal location data ["*A Question of Trust"*, at §4.30], and their content can also reveal individual opinions (including political opinions) as well an information about a person's preferences, sexuality, and health status. Further, this

activity engaged rights to freedom of expression and assembly. The interference with individual's Article 8(1) rights is significant.

22.33. The Code allows for wide interpretation of what is not private information. This is unacceptable and an exhaustive list should be set out in the code. We note the potential implication that what is '***made available at a meeting to a member of the public'*** is fair game. However, it is unlikely that in providing data to someone at a meeting, there is an expectation it would end up in an SIA's Bulk Personal Dataset.

22.34. The Code classifies data as systems data, identifying data, private information and non-private data. However, the classification of what is non-private data is not an accurate reflection of what data would attract rights under the Data Protection Act 1998 and/or Article 8 ECHR. Further, it should be stated explicitly that identifying data and systems data are private information relating to a person's private or family life.

22.35. We are unclear whether the Code accepts that both communications content and communications data, can both attract legal professional privilege.

22.36. Given that the new Code is the first time it appears the Government has categorised data in BPD, and given the lack of clarity, it is difficult to understand the implications of this and how it will impact on individual rights. Further information must be provided and there is a clear need for independent oversight in this opaque area of Bulk Personal Datasets.

22.37. **<u>TYPES OF DATASETS</u>**

22.38. **Recommendation: The Commissioner should review and update the broad categories of data under which BPDs are classified by the SIA. We note the importance of this if the SIA are collecting BPDs, for example, of social media intelligence and other new datasets that arise as a result of developments in technology, e.g. Smart Cities.**

22.39. Bulk Personal Datasets are broadly defined at Clause 199 of the Investigatory Powers Act and there is some elaboration in the Code. However, both the Code and the Act lack clarity as to what is or is not a Bulk Personal Dataset. The nature of BPDs has, since avowal, been an area where the Government has resisted transparency.

22.40. We strongly recommend that the types of BPDs that are retained and examined under the regime are specified for oversight purposes. We note below the resistance of the Government in giving even the most basic understanding of the broad classes of BPDs. Rather than providing information to Parliament, regrettably, transparency resulted from litigation.

22.41. BPDs were first avowed on 12 March 2015, in the Intelligence and Security Committee report *"Privacy and Security: A modern and accountable legal framework"* ("the ISC Report"):

> *"284. The publication of this Report is an important first step in bringing the Agencies 'out of the shadows'. It has set out in detail the full range of the Agencies' intrusive capabilities, as well as the internal policy arrangements that regulate their use. It has also for the first time, avowed Bulk Personal Datasets as an Agency capability."*

22.42. The ISC Report[16] gave the following explanation of Bulk Personal Datasets:

> Bulk Personal Datasets are *"large databases containing personal information about a wide range of people"* (p.55).
>
> Bulk Personal Datasets are used to identify subjects of interest, establish links between individuals and groups and improve understanding of a target's behaviour and connections, and to verify information obtained from other sources (p.55).
>
> The collection and search of Bulk Personal Datasets *"may be highly intrusive and impacts upon large numbers of people"* (p.59Y).
>
> Bulk Personal Datasets are *"an increasingly important investigative tool"* (§153).
>
> Bulk Personal Datasets may be acquired through overt or covert means (§154).
>
> Means of acquisition include where a person discloses data pursuant to section 19 of the Counter Terrorism Act 2008. As the Director General of Security Service put it in evidence to the ISC *"in 2008, the Government deliberately . . . added section 19 of the Counter Terrorism Act, which is an explicit licensing to those who might share data, that doing so overrides any other duties of confidentiality which they might have about data, where a case is made that is a necessary to share that for national security."* (fn 138)
>
> Bulk Personal Datasets vary in size *"from hundreds to millions of records"* and may be *"linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or a ***) from one search query"* (§156).
>
> Bulk Personal Datasets affect British citizens (*"may include significant quantities of information about British citizens"* and *"none of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets")* (§158 and FN 142).

22.43. On the same day as the ISC Report was published, the Prime Minister signed the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal

[16] http://isc.independent.gov.uk/news-archive/12march2015

Datasets) Directions 2015. Bulk Personal Datasets were defined in the Direction as follows:

> *"5. For the purposes of this direct, a bulk personal dataset means any collection of data which:*
> *Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;*
> *Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;*
> *Is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies."*

22.44. When Privacy International filed Grounds in its litigation, there was no detail about the information that could be contained in Bulk Personal Datasets, although potential categories were set out. See Annex A.

22.45. Subsequently, when the Act, then in draft form, was being considered by the Joint Committee from November 2015, limited information was provided by the Government as to the nature of Bulk Personal Datasets.

22.46. It was noted that the Bill and Explanatory Notes were '*very vague'* in relation to bulk personal datasets and that *'The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?'*[17]

22.47. When questioned about the nature of bulk personal datasets the then Home Secretary Theresa May MP stated:

> *'…we do not feel it is right to go down the route of giving information about the sort of datasets that would be acquired and the sort of datasets that would not be acquired.'*

22.48. In written evidence the Home Office give limited examples: electoral roll, passport or firearm license records or a telephone directory; travel data.

22.49. It was only as a result of Privacy International's litigation that more detailed information (whilst limited) was revealed about the extent and nature of bulk personal datasets.

22.50. The 'Open' version of the Respondents' Closed Response provided on 11 April 2016 defined Bulk Personal Datasets as:

[17] Lord Strasburger Q.92 https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf

> *'1) A Bulk Personal Datasets is a dataset that contains personal data about individuals that majority of whom are unlikely to be of intelligence interest and that is incorporated into an analytical system and used for intelligence purposes.*
> *…*
> *3) BPD obtained and exploited by the Intelligence Services include a number of broad categories of data. By way of example these include: biographical and travel (e.g. passport databases); communications (e.g. telephone directory); and financial (e.g. finance related activity of individual).*
>
> *…*
> *Population (these datasets provide population data or other information which could be used to help identify individual e.g. passport details).*
> *Travel (these datasets contain information which enable the identification of individuals' travel activity)*
> *Finance (these datasets allow the identification of finance related activity of individuals).*
> *Communications (these datasets allow the identification of individuals where the basis of information held is primarily related to communications data e.g. a telephone directory).*

22.51. The GCHQ compliance guide extracts 1 June 2005 to 2010 obtained mid-2016 as a result of disclosure refer to:

> *Other information held or obtained in relation to 'persons to whom he provides the service, by a person providing a Telecommunications service': Credit card details of bill payee, or the email address owner would fall within this category.*
> *Billing data and feasibility checks for all UK telephone numbers.*
> *Geo-location where the user is known to be located in the UK.'*

22.52. At the time of the hearing the Agencies held bulk travel data; bulk untargeted communications metadata; anonymised records of financial transactions; bulk databases obtained by computer hacking; internet network management data and logs.[18]

18 https://privacyinternational.org/sites/default/files/1.%20Claimant%27s%20Skeleton%20Argument.pdf

Annex A

"9. The nature, scope and content of all the Bulk Personal Datasets kept by the Agencies have been redacted from the ISC Report. However, the Bulk Personal Datasets are likely to include a variety of information, some volunteered, some stolen, some bought and some obtained by bribery and coercion:

Retained telephone and internet communications data: Telecommunications companies retained telephone and internet communications data, as required previously under the Data Retention Directive and now under the Data Retention and Investigatory Powers Act 2014. Such records include subscriber information, location and length of phone calls. Internet communications data include billing records, and IP addresses.

Data brokers and credit reference agencies: Companies exist to harvest, trade or sell personal information, often for targeted advertising or to provide credit references. Credit reference agencies in the UK such as Experian, Equifax or Callcredit hold personal details on most of the adult population. These databases contain information such as loan borrowing and repayments, water and energy bills, payday loans, court records and fraud allegations. Some even include the direction of your garden (useful information for firms that sell solar panels or satellite dishes), whether you have a burglar alarm fitted, the make and mileage of your car, how much you spend on wine, sports and vitamins, if you gamble, where you go on holiday and what you read[1]. Information held by other databrokers includes lists containing sensitive personal information, such as the identities of people with alcohol, sexual or gambling addictions[2].

Communication Service Providers: As part of their business communication service providers create large databases of their customers' private information. This can include a wide variety of content, such as chat logs, search histories and content of emails.

Medical records: Databases such as those held by the NHS Prescription Pricing Division holds all prescriptions written in England in the last five years. The NHS Personal Demographics Service, the national electronic database of NHS patients, could be acquired. The British Pregnancy Advisory Service, which is Britain's largest single abortion provider, holds hundreds of thousands of records for the 65,000 women they help each year. Private health records from BUPA or Nuffield Health will exist on a similar scale.

Travel records: Many databases contain detailed personal travel records. Oyster card transactions provide a detailed map of movements throughout London and similar databases could be obtained for other cities. Hotel reservation services, airline computerized reservation systems, as well as automated number plate recognition databases, car rental databases form companies like Sixt, Europcar, or Enterprise, all contain personal information on a large number of people that may be of interest to the Agencies.

Financial records: Financial records from banks, transactional records from credit and debit cards provided by Visa or Mastercards; and interbank transaction databases such as SWIFT provide a detailed look at millions of peoples' lives.

Biometric records: Private companies such as AncestryDNA[3] hold more than 850,000 DNA records. Voiceprint records that identify who is speaking on the phone, or in a voice recording are held by companies such as ValidSoft. Facial recognition databases such as those created by face.com (now owned by Facebook) holds 18 billion face IDs.

Membership databases: Most membership bodies hold records in databases about their supporters, subscribers, or members. These could include databases held by political parties, professional associations, or religious databases belonging to churches, synagogues or mosques.

Loyalty Card Schemes: Many businesses offer loyalty cards, tracking consumers' buying habits in a way that can real extremely personal details, such as whether a buyer is pregnant. Tesco Clubcard has over 15 million members. Nectar Card has 19 million cardholders.

---

[1] http://www.thisismoney.co.uk/money/cardsloans/article-2324451/Credit-spies-making-millions-watching-move.html
[2] http://paramountdirectmarketing.com/
[3] http://dna.ancestry.co.uk