**IN THE INVESTIGATORY POWERS TRIBUNAL** **Case No IPT/13/92/CH**

**BETWEEN:**

**PRIVACY INTERNATIONAL**

**Claimants**

**-and-**

**(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS**

**(2) GOVERNMENT COMMUNICATION HEADQUARTERS**

**Defendants**

---

**WITNESS STATEMENT OF ERIC KING**

---

I, Eric King, Deputy Director, Privacy International, 62 Britton Street, London EC1M 5UY, SAY AS FOLLOWS:

1. I am the Deputy Director of Privacy International.

2. I hold a Bachelor of Laws from the London School of Economics and have worked on issues related to communications surveillance at Privacy International since 2011. My areas of interest and expertise are signals intelligence, surveillance technologies and communications surveillance practices. I regularly speak at academic conferences, with government policy makers, and to international media. I have spent the past year researching the "Five Eyes" intelligence-sharing arrangement and the materials disclosed by Edward Snowden.

3. I make this statement in support of Privacy International's claim. The contents of this statement are true to the best of my knowledge, information and belief and are the product of discussion and consultation with other

experts. Where I rely on other sources, I have endeavoured to identify the source .

4. In this statement I will address, in turn, the following matters:

    a. The transmission and interception of digital communications;

    b. The difference between internal and external communications under RIPA, as applied to the internet and modern communications techniques;

    c. Intelligence sharing practices among the US, UK, Australia, New Zealand and Canada ("the Five Eyes");

    d. The UK's consequent access to signals intelligence collected by the United States through its PRISM and UPSTREAM collection programmes;

    e. British mass signals intelligence collection, with particular focus on the Tempora mass interception programme; and

    f. The existence and scope of proper and meaningful safeguards in the British intelligence services and their oversight mechanisms.

5. Throughout this statement I use a number of the following terms to refer to practices and procedures related to the activities of the UK government:

    a. **Signals Intelligence** – the type of intelligence collection concerned with the interception of communications and other electronic signals; also known as SIGINT.
    b. **Metadata** (also known as communications data) – information about a communication, including the sender and recipient of emails and messages, their locations, and the subject of the communication; times of messages and phone calls made and received, and the location of the parties; websites visited.
    c. **Content** – information contained with emails, or phone calls among others.

d. **Applications, services and platforms –** these terms are used interchangeably to refer to internet programmes that facilitate the transmission of text, video, voice, picture communications and files. Such programmes include Gmail, Facebook, Twitter, Amazon, DropBox, etc.

## I. THE TRANSMISSION AND INTERCEPTION OF DIGITAL COMMUNICATIONS

6. For reasons that I outline below, the distinction drawn by the Government between "internal" and "external" communications no longer has any practical meaning. The safeguards provided by RIPA pertaining to the interception of "internal" communications do not in fact result in any meaningful protections for such communications privacy when applied to the modern communications system. First, a significant proportion of all "internal" communications in the UK today will be leave the British Isles and be picked up within TEMPORA, even when those communications relate to two people communicating in the UK. Second, given the nature of modern communication, the terms "internal" and "external" communication, and the Government's interpretation of them, leads to arbitrary and unforeseeable distinctions that render those categories entirely meaningless and no longer fit for purpose.

### How the internet works

7. It is necessary to begin with how the internet works. It works by taking each individual communication and breaking it down into smaller fragments, called "packets". These packets are then transmitted separately, often through different routes, to the recipient, where the message is reassembled. All forms of communication – emails, Google search, phone calls, text messages, Facebook post, requests to visit a web site, Skype calls – that utilise the internet for some or all of the transmission of the communication, will be broken down into these packets. The internet transmits every kind of communication using this method, whether it relate to text (an email, search results, or file sharing), voice, picture or video communications.

8. The internet works in the same way throughout the world. The fundamental protocols and systems are standardised worldwide. The common language that is used throughout the internet to enable computers on opposite ends of the globe to communicate using packets is known as the Internet Protocol suite. The suite is comprised of two protocols: Transmission Control Protocol (TCP) and the Internet Protocol (IP) and collectively are known as TCP/IP.

9. Each of the packets in an individual communication contains a fragment of the content of the communication, as well as some standardized information about the communication. This information includes the Internet Protocol (IP) address of the sender of the communication (equivalent to an address or telephone number), and that of the recipient of the communication. An IP address is a sequence of four numbers. For example, the Tribunal's website is hosted, by a hosting company, at IP address 213.171.193.42. Every time an individual wants to visit the Tribunal's website, they have to communicate with the Tribunal's IP address. However, to make the internet easier to use, Domain Name Servers ("DNS") allow individuals to use alphanumeric addresses (such as "www.ipt-uk.com") rather than actual IP addresses. These DNS addresses act as an address book for the internet.

10. Each packet of a communication is comprised of content and metadata, and is encapsulated by a set of "protocol data" drawing from different information from different layers within the packet. Figure 1 below displays the types of information contained at the various layers of each packet.

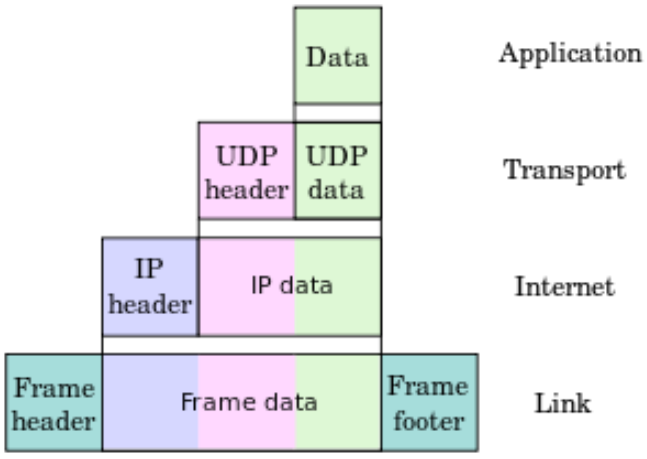



**Fig. 1 – packet layers**

11. Beginning from the bottom of the diagram, the "Link" layer contains only the information necessary to transport the packet along the physical transmission link (the cable or wire on which the communication is being transported) to the next "node". A node is like a pit stop for a packet, a place where it stops momentarily to assess its next routing orders and travel on to its next destination. The "Link" layer only ever needs to know the destination of the next routing node. The "Internet" layer of the packet knows the final destination of the packet, and has the responsibility of telling the "Link" layer, at each routing node, which route to take next. That decision is made on the basis of which is the most efficient route for the packet to take to get to towards the final destination.

12. It is important to emphasise that the "Internet" layer of the packet will not necessarily contain the IP address of the *ultimate* intended recipient of the communication – the individual to whom an email is being sent, for example. Rather, the IP address contained within the "Internet" layer of the packet will be that of the service or platform via which the communication is being sent. For example, an email sent from one Yahoo mail user in the UK to another Yahoo mail user in the UK will be broken up into packets that contain the Yahoo mail IP address in the "Internet" layer, but not the address of the individual recipient for whom the email was intended. This is because the communication assumes that once the email arrives at Yahoo, Yahoo will know what to do with it. In other services or platforms, such as Facebook, the information about the individual sender and recipient of the message is buried deep within the packet, beyond the "Application" layer and into the very content of the actual communication itself, and thus would not be visible in a scan of the packet information.

13. The "Transport" layer of the packet is often responsible for maintaining a connection with the final recipient of the communication. Packets can get dropped, garbled or misrouted along their path and so the "Transport" layer deals with these issues to ensure the complete communication reaches its final destination intact. The "Transport" layer effectively establishes the data channel that allows the application that the sender is using to transmit their communication to send the relevant data to the recipient of the communications, according to specific protocols that are contained in the

"Application" layer. The "Application" layer stores the various protocols – languages – used by internet providers to transfer the information. Types of protocols used in the transmission of communications include HTTP (HyperText Transfer Protocol, which accounts for all internet-based communications such as web sites and searches); FTP (File Transfer Protocol, used for the transfer of files) and SMTP (Simple Mail Transfer Protocol, which is used to transfer and manage email). Modern communications tools like Facebook use all of the above layers to transmit and receive data, but also have their own custom protocols that sit within the "Application" layer.

14. Each of these packet layers plays a critical role in ensuring that communications are successfully transmitted across multiple networks around the world to reach their destination. And communications do, indeed, travel around the world. An email from a person in Clapham to a friend in Camden may well be more likely to travel first to California before crossing the Thames.

15. Furthermore, the packets that make up a single communication (such as an email or a Facebook post) can traverse different paths to reach the communication's destination. This means that one part of same email might be routed via Japan, while another part will travel via Amsterdam. In practice, packets will take the quickest and route available to them with the greatest transmission capacity ("bandwidth"). This is often not the shortest route.

16. Nevertheless, while there are an almost infinite number of routes that a packet could take, there will be common steps that packets take in order to reach their destination. From a computer or mobile phone, packets will first be sent to the internet service provider, and thereafter routed via multiple routing notes to the relevant server that possesses the IP address that the data was intended to be transmitted to. In doing so, the packets utilize physical cables that connect computers to routers, routers to other routers, and those routers to the recipient's servers. Since the 1990s, these physical cables have been almost entirely fibre optic cables, which transmit communications faster and more efficiently than their predecessors, electronic cables.

17. The internet is built around a global infrastructure, which includes many fibre optic cables that are laid under the sea and which traverse numerous countries. A full map of the undersea cables is below at **Figure 2**. http://www.submarinecablemap.com/

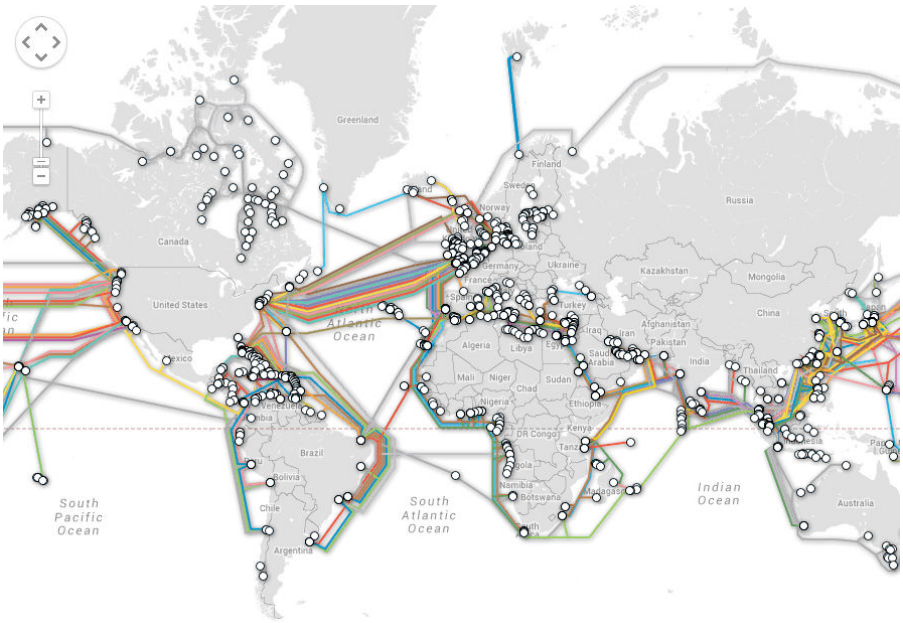



**Fig 2 – undersea fibre optic cables**

**Metadata is as valuable as communications content**

18. As described above, packets contain different types of information. Generally, this information can be designated as one of two kinds – communications data, or metadata, and content. Metadata is information about the communication – who it is to and from, the date and location from which it was sent, and the subject line of the email.

19. Traditionally, metadata have been afforded lower protections in legal frameworks and generally accorded lower worth. However, advancements in modern technologies and the advent of the internet have revolutionised the creation, storage, collection, interception and erasure of data. Mobile and digital devices are now ubiquitous, generating quantities of data that grow exponentially as more people live more of their lives online; the costs of storing data have decreased drastically, and continue to do so every year;

increasing amounts of data are transferred across borders with increasing frequency – more and more people use email, storage and financial services that are physically located in countries far away from them; and public and private services have become digitised and automated. The amount of data that exists in the digital realm today is around ten times that which existed less than a decade ago.[1] Technical means and methods of analysing data have advanced so rapidly that today what was previously considered incoherent, disparate or meaningless types and amounts of data can now produce incredibly revelatory analyses.

20. The way we communicate and use modes of communication has also changed considerably. While recognising that access to the internet remains a serious issue for a large portion of the world, for a great number of us the major portions of our lives are lived, to a large extent, online. We use the internet to talk, learn, shop, find employment, read books, watch movies, conduct financial transactions, organise travel, keep records, conduct research, impart ideas, diagnose health conditions, and learn and express our political views. Our mobile and digital devices are extensions of our personal and professional lives, seamlessly integrated into every aspect of our personal behaviours and relationships. They enable us to collect and catalogue a disparate range of media, information and tools. They have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, correspondence files, fixed-line telephones, and personal computers. Increasingly, they are also replacing our formal identification documents, our bank and credit cards.

21. Use of the internet via mobile and digital devices enables the creation of additional personal data about communications, known as communications data or metadata. This type of data can include personal information about individuals, their locations, travels and online activities, and logs and related information *about* the e-mails and messages they send or receive, even apart from the content of those messages themselves. Metadata are storable, accessible and searchable, and access to and analysis of the data can be hugely revelatory and, as described further below, highly invasive. The

[1] Helbing and Balietti. "From Social Data Mining to Forecasting Socio-Economic Crises." *Arxiv* (2011) 1-66 (26 Jul 2011).

historical distinction between data about an individual's communications and the content of his or her communications has become insignificant.

22. Put together, metadata can reveal an individual's identity, relationships, location and activity, as well as a vast array of diverse information about their web browsing activities, medical conditions, political and religious viewpoints and/or affiliation, interactions and interests. Access to and analysis of such data allows deep, intrusive and comprehensive view into a person's private life. Even seemingly innocuous transactional records, when analysed and matched with other personal data, can be extremely revelatory.[2] Books read and movies watched, items purchased from online stores or pharmacies, news sites subscribed to and games played online – each of these pieces of metadata tell a story of an individual's life.

23. Both the US and British Government have sought to downplay the importance of metadata in their signals intelligence activities. The argument is that as metadata is not the actual content of the communication, the threat to privacy is less severe. This position however, mischaracterises the nature of metadata. Metadata can provide a highly detailed social graph of a person's more intimate associations and interests and is structured in a way so that computers can search through it for patterns faster and more effectively than similar searches through just content. Indeed, metadata can now reveal equally sensitive information as communications content. [3]

24. In recent months, Ex NSA General Counsel Stewart Baker has said "*metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content*." [4] General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "*absolutely correct*," and offered a different perspective on how valuable NSA considers metadata, asserting, "*We kill people based on metadata.*" [5]

**Types of modern communication systems and the way they transmit data**

---

[2] Mayer and Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2013); US District Court/ Southern District of NY, *Declaration of Edward W. Felten*, ACLU v. Clapper, No. 13-cv-03994 (WHP) (SDNY Aug. 23, 2013), ECF No. 27.

[3] See for reference EFF Amicus Curiae Brief

[4] Rusbridger, "The Snowden Leaks and the Public," *The New York Review of Books* (21 November 2013).

[5] Cole, "We Kill People Based on Metadata", *The New York Review of Books* (10 May 2014).

25. Today, all forms of internet-based communications – even those between friends and families located within close proximity of each other – are likely to travel around the world before reaching their destination. In order to illustrate this, below I have described the operation of three popular communications services – Google (and the suite of communication products it provides), Facebook, and Twitter. Use of each of these three services involves the relevant communications physically leaving the United Kingdom in order to transit to a server in the United States. That is so even if the end recipient and the sender are both in the UK.

26. In considering how these services are used, it is important to remember that, not only do an increasing number of phone-based communications use the Internet Protocol for transmission (such as those in large offices), but increasingly individuals are choosing to use internet-based services rather than phone calls or text messages to communicate. This is facilitated by the fact that phones and the internet have become highly integrated in a practical sense: the internet is no longer something accessible just from personal computers; with the advert of smart phones, according to Ofcom, now 71 per cent of mobile users access the internet on their smartphone.[6] A similar increase is occurring in the rise of social networking websites that allow people to build a social profile online and interact with friends, acquaintances and others with similar interests, sharing photos, thoughts, and events happening to and around them. The Oxford Internet Survey shows that 61 per cent of internet users in the UK use social networking sites;[7] according to OfCom, 40 per cent of mobile internet users in the UK visit a social networking site almost every day.[8]

27. According to the Oxford Internet Survey (**at Figure 3)**, it is no surprise to learn that 61 per cent of students prefer to use social networks to communicate, and 23 per cent of students saying they use email and social media in equal measure. Of those who are employed, 34 per cent prefer to use social networking, and 36 per cent declare they use social networking and email in equal measure.

---

[6] Ofcom, *International Communications Market Report* (12 December 2013)
[7] Dutton and Blank, *Cultures of the Internet: The Internet in Britain,* Oxford Internet Survey 2013 Report.
[8] Ofcom, *International Communications Market Report* (12 December 2013).

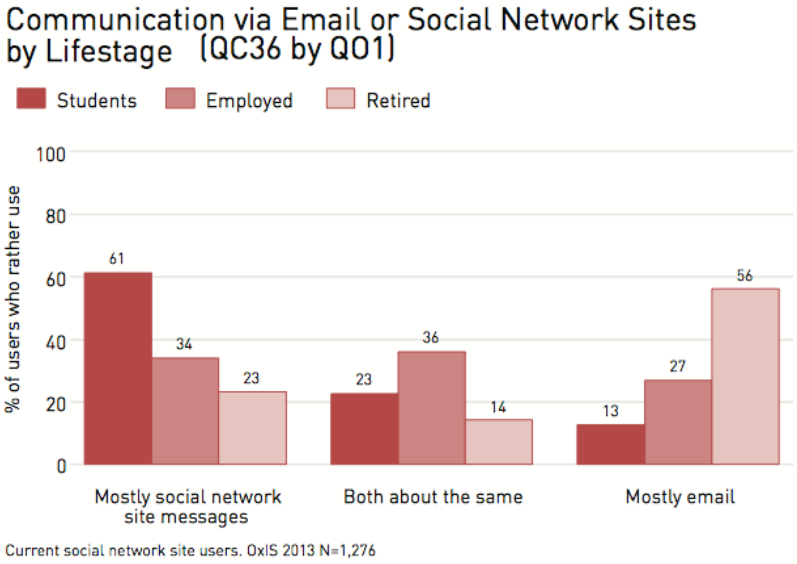



**Fig.3 – ofcom communication method comparison graph**

**Google**

28. Since Google's email client Gmail launched in 2004, it has become the most widely used web-based email provider in the world, with over 425 million active users worldwide.[9] Although, Google has servers all over the world which store its data, when an individual connects to Gmail they are first connected to IP address 173.194.34.150. which is the address of Google headquarters in Mountain View, California. This can be demonstrated by conducting a test called a "trace route", which involves tracking the data exchanged with Google when connecting with Gmail (see Figure 4 below). As a result, any initial communication with Gmail immediately is routed first to the US.

**Fig. 4.**

29. Using Gmail, an individual has the ability to send communications to an individual, or to a small or large group of people, depending on the number of recipients selected by the sender (see Figure 5 below, an example of an email sent to a large number of individuals via Gmail).

[9] D'Orazio, "Gmail now has 425 million active users, *The Verge* (28 June 2012).

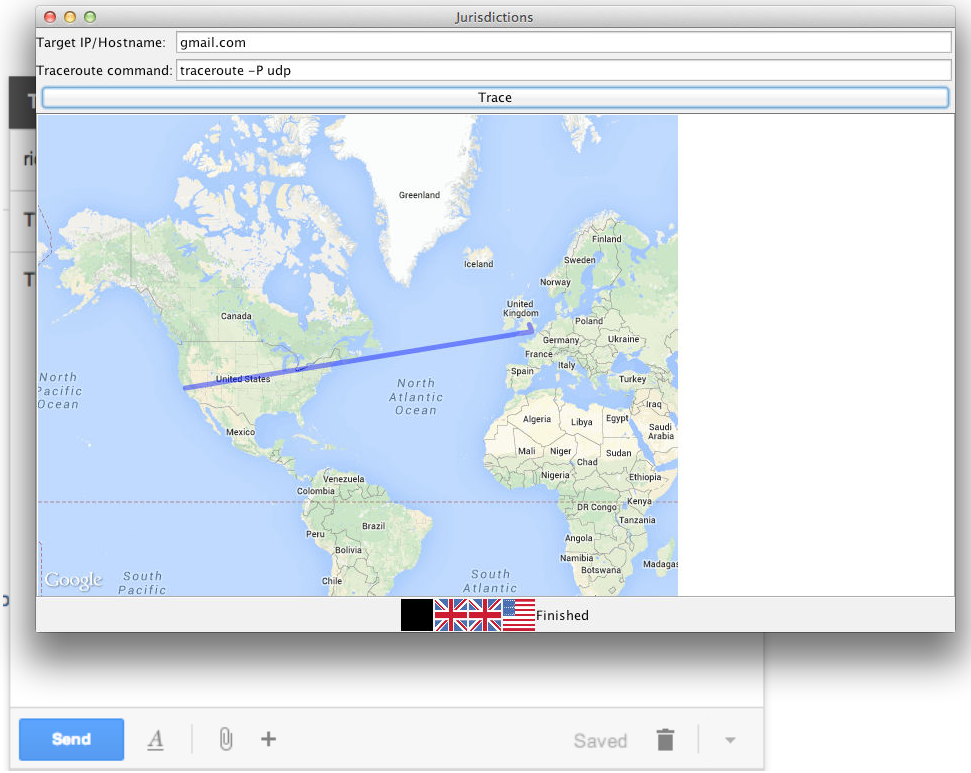



**Fig. 5**

30. Today, many people use mailing lists – the transmission of emails to large groups of people, similar to traditional newsletters – to stay in touch, either with friends, colleagues, peers, or as members of groups or associations. Sending such a message via an email account like Gmail is easily done and can enable one person to send one email that could reach hundreds or thousands of people.

31. Recently, however, Google has encouraged users who are regularly sending emails to a large group of people via Gmail to consider using another Google product, a social media service called Google Plus, which tries to offer better controls and layout for managing large group messages. This service, like Gmail, gives the user granular controls to manage to whom the message is being sent (see Figure 6 below).

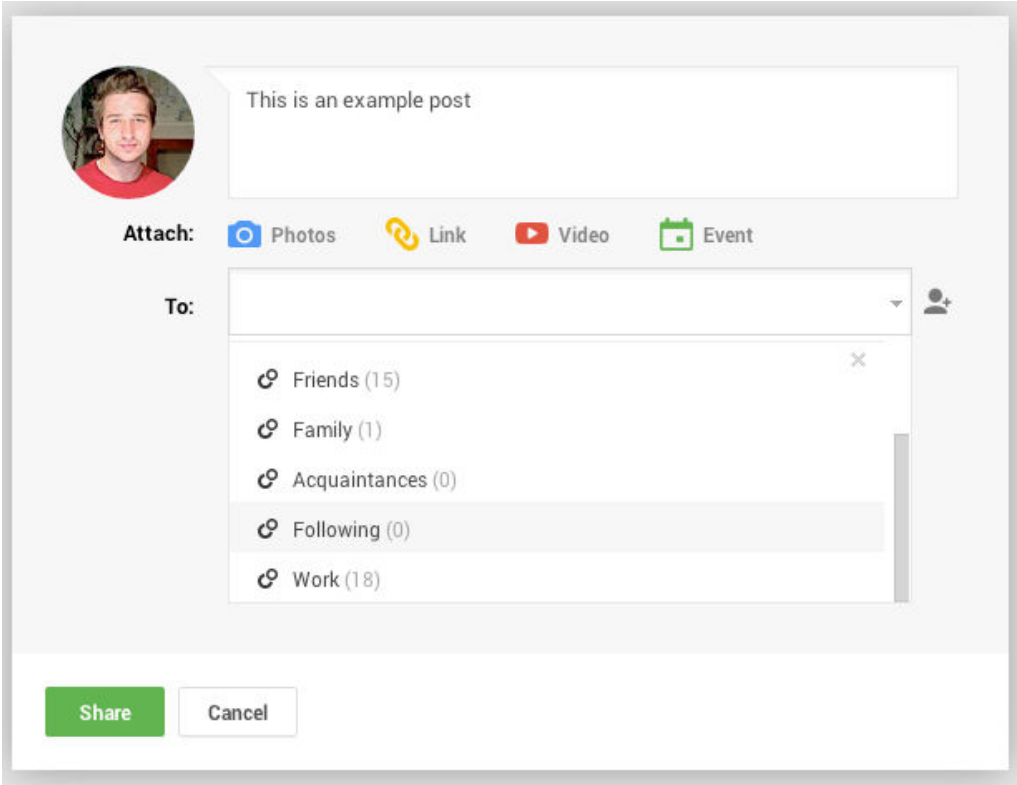



**Fig. 6.**

32. Rather than send an email to an individual contact, Google users could also opt to send the same text via Google's instant message platform. Until last year this was in the form of a Gmail feature called Google Talk, however this service has been merged with other chat platforms into an integrated instant messaging and video chat platform called Google Hangout. Google Hangout allows an individual to speak to a contact via video chat, while also sending text-based instant messages (see Figure 7 below). Both video and text-based conversations using Google Hangout are synced across many different devices and platforms at once and are tied to Gmail (Figure 8 below), Google Plus (Figure 9 below), and to Google's smart phone instant messaging applications (Figure 10 below).

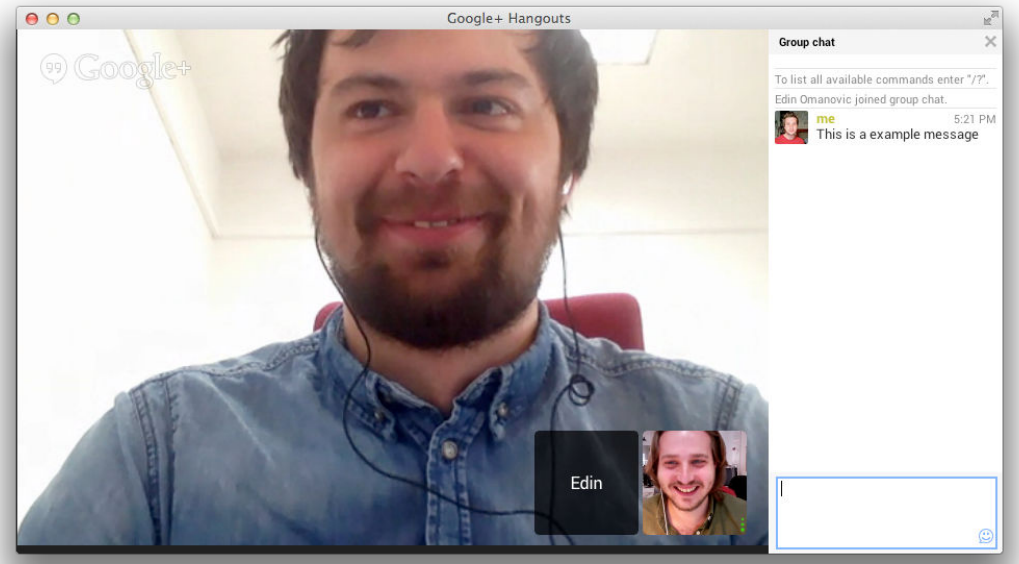

Google+ Hangouts
Group chat
To list all available commands enter "/?".
Edin Omanovic joined group chat.
me
5:21 PM
This is a example message
Edin

Fig. 7.

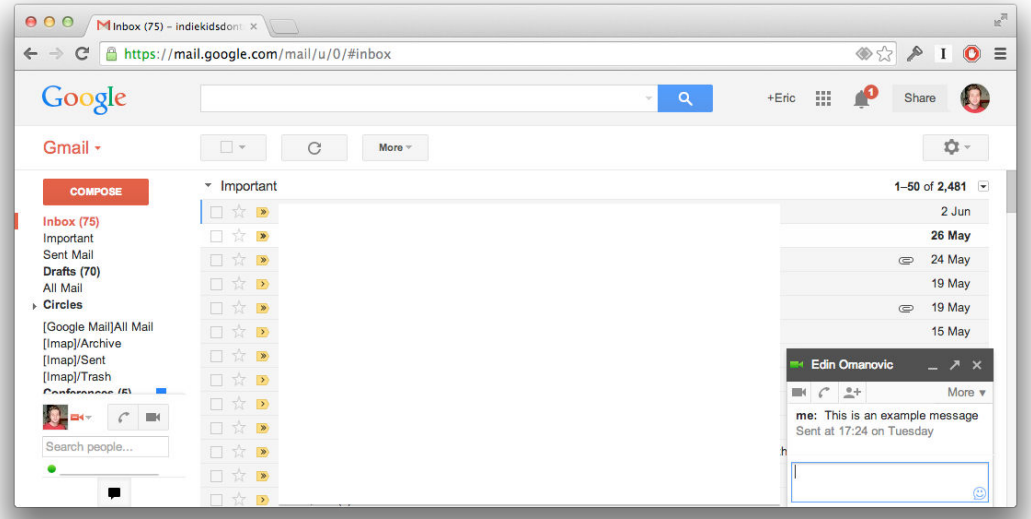

https://mail.google.com/mail/u/0/#inbox
Google
+Eric
Share
Gmail
More
COMPOSE
Inbox (75)
Important
Sent Mail
Drafts (70)
All Mail
Circles
[Google Mail]All Mail
[Imap]/Archive
[Imap]/Sent
[Imap]/Trash
Search people...
Important
1–50 of 2,481
2 Jun
26 May
24 May
19 May
19 May
15 May
Edin Omanovic
More
me: This is an example message
Sent at 17:24 on Tuesday

Fig. 8.

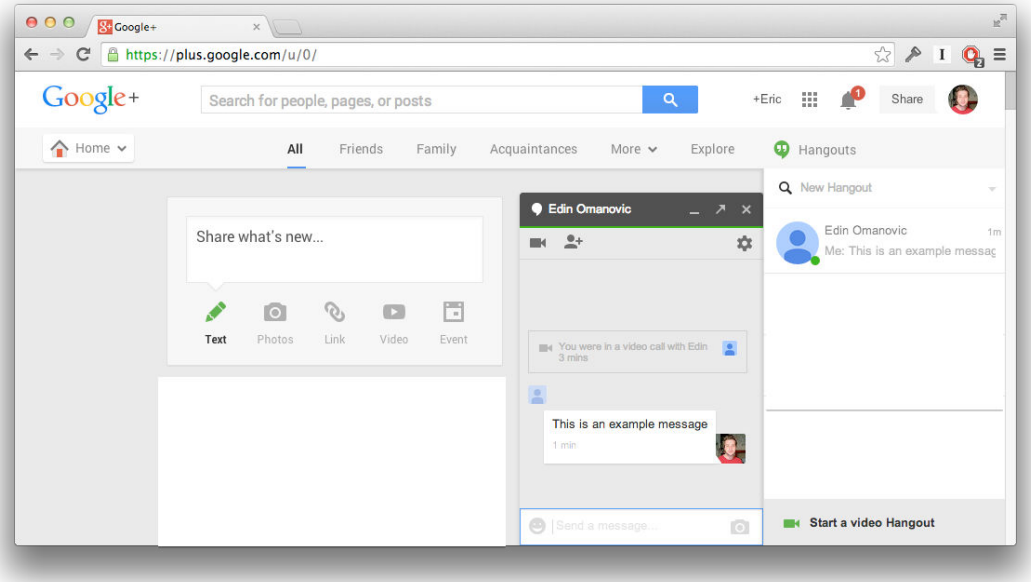

Google+
https://plus.google.com/u/0/
Google+
Search for people, pages, or posts
+Eric
Share
Home
All
Friends
Family
Acquaintances
More
Explore
Hangouts
Share what's new...
Text
Photos
Link
Video
Event
Edin Omanovic
You were in a video call with Edin
3 mins
This is an example message
1 min
Send a message...
New Hangout
Edin Omanovic
1m
Me: This is an example messag
Start a video Hangout

**Fig. 9**

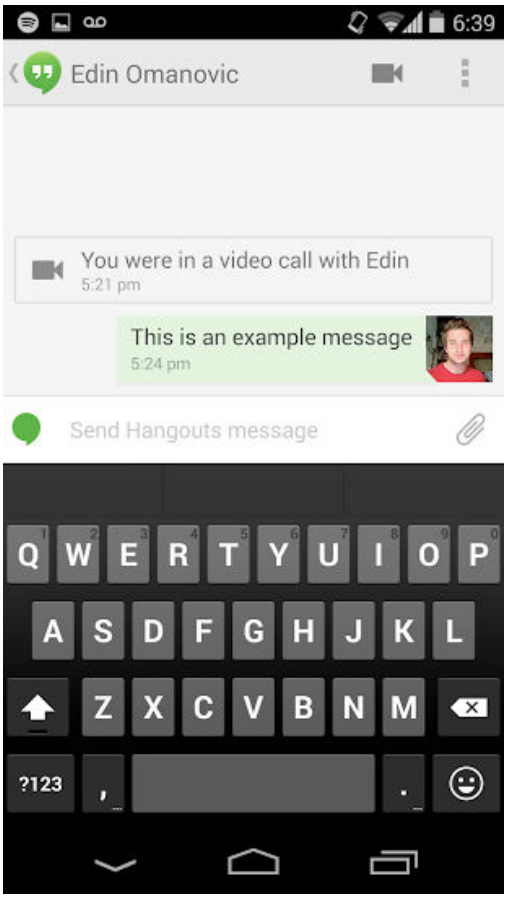

6:39
Edin Omanovic
You were in a video call with Edin
5:21 pm
This is an example message
5:24 pm
Send Hangouts message
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
?123

**Fig. 10.**

**Facebook**

33. With over one billion active users in 2012, Facebook is the largest social networking service in the world. Facebook's mission, according to its website, is to help individuals connect and share with the people in their lives. Like Google, although Facebook has servers all over the world, when an individual connects to Facebook, they are first connected to 173.194.34.150, which is the IP address of Facebook's headquarters in Menlo Park, California (see Figure 11 below.)

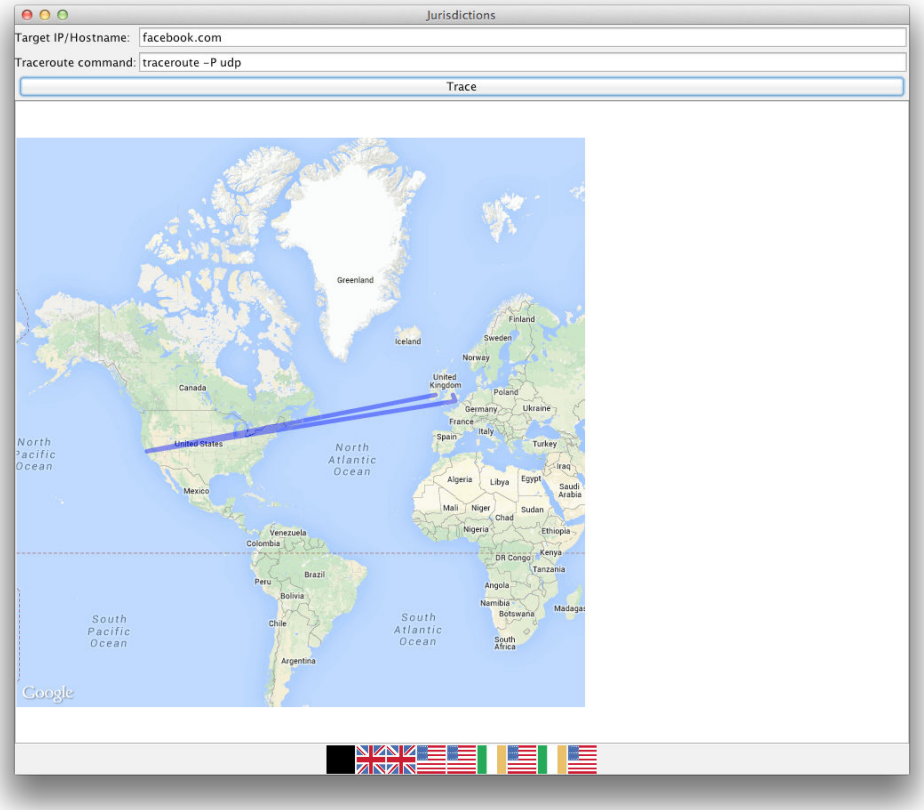



**Fig. 11**

34. Just like Gmail, and Google Plus, through Facebook an individual is able to communicate text messages, photos or other content to an individual, or to a small or large number of people. This is through a method called "posting", whereby a user places a message on their Facebook "wall" for selected contacts to read and respond to. Although when Facebook was initially launched it was the service's default settings were set to ensure that every

post made by a user was in fact viewable and accessible by the general public, today Facebook has a sophisticated system of privacy settings that enables a user to determine, with respect to each post they make, whether that communication will be received, viewed and accessed by one, ten, or 100 "friends" of the user (people who they know and have consented to sharing information with), or to the public at large (see Figures 12 and 13 below). While there are still options for posting content publically, the default setting now for individuals signing up to Facebook is that posts will only be shared with "friends.[10] Users have even more granular levels of control; for example, they can make a post viewable by all but one of their "friends."

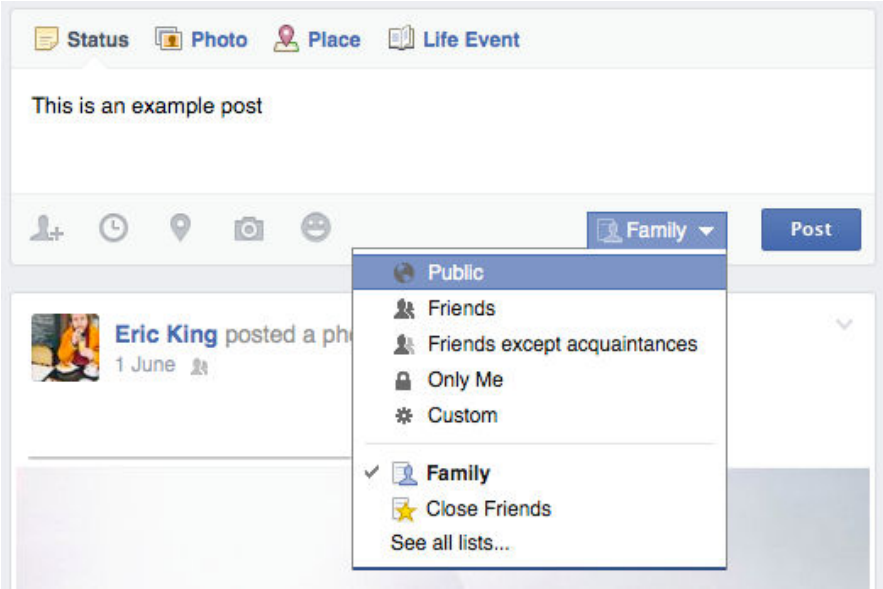



**Fig. 12.**

[10] Facebook, *Making It Easier to Share With Who You Want* (22 May 2014)

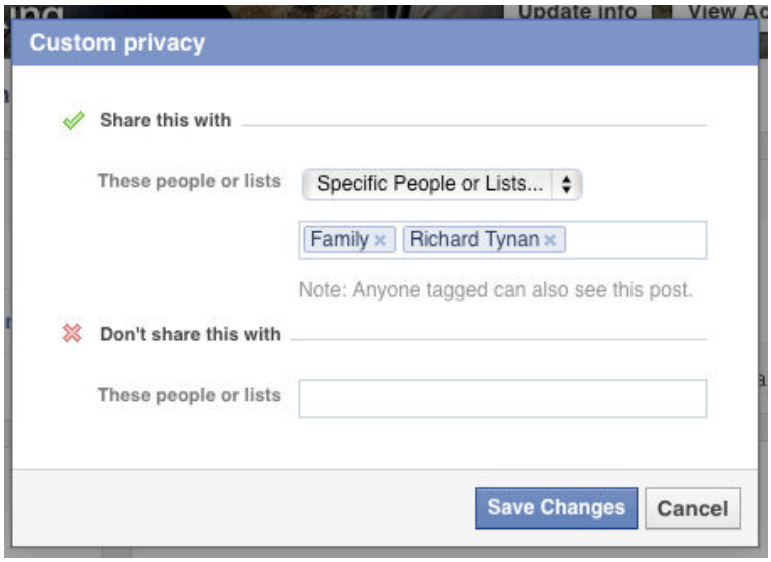



**Fig. 13.**

35. Facebook also provides a different mode of sending communications – the Facebook Messenger facility – that operates much the same as Google Hangout. Again, users can send messages to either one or many friends at a time.

36. For a time, Facebook also offered an email service, which automatically created an @facebook.com address for Facebook users. Earlier this year the email option was removed,[11] only a few days after Facebook bought one of the largest mobile instant messaging services, WhatsApp.[12] It is anticipated that Facebook will integrate WhatsApp with Facebook's existing instant messaging service, Facebook Messenger.

**Twitter**

37. Twitter is an online social networking service that allows people to send and read 140 character text messages known as tweets. It is known as "the SMS of the internet" and, as of 2012, had 500 million registered users. As with Google and Facebook, Twitter has servers all over the world, but when and individual connects to Twitter, they are first connected to 199.16.156.102 which is the IP address of Twitter's headquarters in San Francisco, California.

[11] "Facebook quietly ends email address system," *BBC News* (24 February 2014)
[12] "Facebook quietly ends email address system," *BBC News* (24 February 2014)

38. Twitter's default settings prescribe that the text messages sent by a user will be transmitted to the public at large. However, it is possible for a user to modulate settings to control who receives or can view a user's communications. For example, users can set their account to private, ensuring only people that are manually individually approved can receive a user's messages. A private Twitter account would operate very similarly to a Facebook account with standard privacy settings engaged. Should users elect not to set an account to private, the majority of the messages they transmit will be viewable by the public.

39. Like Facebook, Twitter also provides a "Direct Message" facility that enables users to communicate privately with another individual, or with a small or large group of friends (see Figure 14 below).

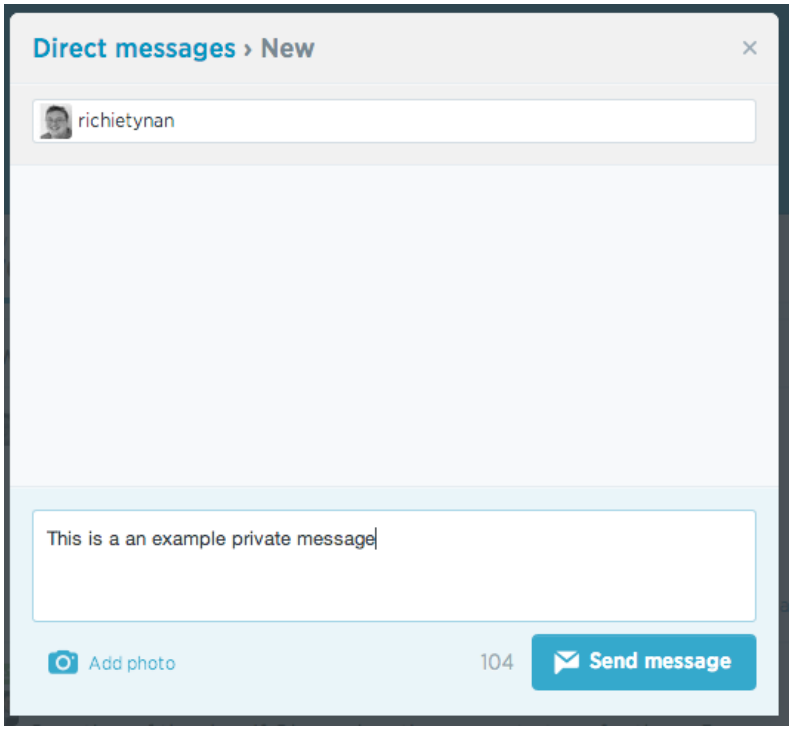



**Fig. 14.**

**Interception of modern communication systems**

40. Traditional communications systems like the telephone required a dedicated physical link (circuit) to be set up between two callers in order to enable them

to communicate. Such systems used a series of switches to set up that unique circuit for the call. Traditional forms of phone communications interception involved placing a tap on that physical link to intercept – collect and record, but not prohibit from reaching their destination – the communications between the two callers. Similarly, interception of traditional postal mail involved the opening and copying of letters as they passed through a postal collection office on the way to their destination.

41. As explained above, the large majority of the world's internet, as well as mobile and fixed telephony, communications are now conducted via Internet Protocol, and a single communication, once split up into different packets, may traverse numerous entirely separate links. These packets are comprised of different layers, and can contain different information at different layers within the packet; so, in the case of a Facebook message, the information about the sender and receiver of a particular communication is between is buried deep within the packet.

42. The interception of IP-based communications involves the handling, duplication or storage (for either a brief or long period of time) of packets as they flow through a certain link. At the point of interception, the packet is opened and an inspection of some layers or every layer within the packet takes place, in order to analyse whether the packet contains something of interest. Each packet can then be duplicated, categorised, logged, copied and stored. The process is conducted instantaneously such that the packets are not necessarily delayed in their transmission, nor are they prevented from reaching their destination. As will be explained in more detail below, GCHQ's TEMPORA program does exactly this, on a mass scale.

43. This process clearly amounts to an interference with the communication. If we take the analogy of traditional interception of postal mail, mass interception of IP-based communications is akin to an inspection and recording of both the address of every single piece of mail that passes through a certain post office, as well as the opening, inspection and potentially duplication of the contents of that piece of mail, prior to the forwarding on of the mail to its intended destination. Just like with postal interception, the interception of digital communications is effected at the

moment at which a communication is engaged with sufficiently to enable its collection and retention for analysis, either contemporaneously or subsequently.

44. The Interception Commissioner[13] described this act both as "filtering", as well as interception. He explains that:

> *"Any significant volume of digital data is literally useless unless its volume is first reduced by filtering. What is filtered out at this stage is immediately discarded and ceases to be available."* [14]

45. He also refers to this process as *"generalised initial interception"*. [15] Both statements are correct. In order to filter, you need to intercept; communications cannot be filtered unless they are first intercepted.

## II. THE DIFFERENCE BETWEEN INTERNAL AND EXTERNAL COMMUNICATIONS UNDER RIPA

46. Mr Farr has explained how GCHQ has interpreted the section 8(4) regime in respect of email communications:

> "*Under paragraph 5.1 of the Code, the relevant question to ask is not via whom (or what) a message has been transmitted, but for whom (or what), objectively speaking, the message is intended. Thus, an email from a person in London to a person in Birmingham will be an internal, not external, communication for the purposes of RIPA and the Code, whether or not it is routed via IP addresses outside the British Islands, because the intended recipient is within the British Islands. The intended recipient is not any of the servers that handle the communication whilst en route (whether that server be located inside, or outside, the British Islands). Indeed, the sender of the email cannot possibly know at the time of sending (and is highly unlikely*

---

[13] *2013 Annual Report of the Interception of Communications Commissioner,* p. 52.
[14] *2013 Annual Report of the Interception of Communications Commissioner,* p. 52.
[15] *2013 Annual Report of the Interception of Communications Commissioner,* p. 52.

*to have any interest in) how that email is routed, or what servers will handle it on its way to the intended recipient.*"[16]

47. This explanation has a number of important practical consequences. First, the packet data relating only to the sender and initial recipient of a communication cannot provide GCHQ with any means to determine whether a communication is actually internal or external. Second, in order to determine who the ultimate recipient of a communication is, GCHQ would have to inspect the entirety of the packet, including the content of the communication. There is no boundary between the sender and receiver information, and the content of a message, in a packet. This is, of course, in stark contrast to older forms of communication where the communication itself revealed where the receiving party was located. Depending on the protocol used by the packet, the ultimate recipient's information may not be available until end of the content, requiring the analysis of all content in the packet in order to obtain the metadata.

48. By way of example, a communication between two Gmail users will be broken into packets that only contain the IP addresses of the sender and Gmail – not the IP address of the email receiver. In order to determine whether the communication is internal or external, GCHQ would need to collect the entire sequence of packets and reconstruct them, and then look inside in order to determine who is in fact communicating.

49. As well as the difficulty in determining what is internal and what is external for the purposes of RIPA, it also appears from Mr Farr's evidence that the Government distinguishes in legal terms between emails and other forms of internet-based communications. Mr Farr explains that GCHQ considers that sending a message to "friends" on Facebook is always deemed to be an external communication (and as such subject to mass interception under section 8(4)) because Facebook is a "platform". This is the case even if all my "friends" who see the message are in the UK, and even if the message is being sent to only one "friend" in the UK.

[16] Statement of Mr Farr, at [129].

50. It is not entirely clear what online services fall within Mr Farr's definition of a "platform", as will become apparent in the examples below. His definition appears to stem from a belief that people in the UK don't communicate with *each other* on when they use Facebook or other similar modern communication services, they simply communicate with the platform itself.

51. This came as a considerable surprise to me, and is in my opinion an entirely novel explanation, not to mention an interpretation of RIPA that has been secretly adopted and is not evident on the face of the legislation. The concept of a 'platform' appears nowhere in the legislation, or in the Code of Practice. Even a person familiar with the complexities of RIPA would have no idea, until he or she read Mr Farr's statement, that this was the approach taken by HM Government.

52. It was previous my understanding that all communications that are both sent and received within the British Islands would be considered an internal communication. My understanding was based on the on the basis of the RIPA Code of Practice states:

> "*[External communications' include those [communications] which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route.*"

53. Lord Bassam of Brighton[17] also made clear that an email message from people within the United Kingdom would be an internal communication, whatever route it took to reach its destination, and via whatever Internet Service Providers servers it passed through on the way.[18] As such, to my mind this would apply regardless of the method of communication used. If communicating with the same people in the UK, why should it matter if an email, a Facebook message, a Google Hangout, or a private Twitter account or a Twitter direct message is used? A technically equivalent method for performing the same communication should also be subjected to the same legal regime. Yet Mr Farr has said that if individuals use "platforms" such as

[17] Lords Committee, Hansard, 12 July 2000 at column 323.
[18] Statement of Mr Farr, at [130].

Facebook to send messages within the UK to someone else in the UK, it would be considered an external communication, whereas if they used Gmail to send the same message to the same people, that would be internal.

54. To illustrate the arbitrariness of this distinction, I have analysed the implications of Mr Farr's distinction for a series of communications between friends, based in the UK, using different products supplied by Google. For the purpose of the example, I shall ignore the practical obstacle that GCHQ could not identify the communication as being internal without intercepting the whole communication, as well as breaking Google's transport encryption.[19]

55. Should the friends all use the most popular email service, Gmail, it is clear that although routed externally and as such intercepted by GCHQ, the communication would be considered internal by GCHQ and as such have some protective status under RIPA. However, should the friends be in regular contact, and use a private group on the social networking layer of Google, Google Plus, to share the exact same message, it would appear from the Facebook platform approach set out in Mr Farr's statement that this would constitute an external communication and thus have none of the protections afforded to internal communications.

56. From a technical perspective, both of these means of communication are essentially identical. In each case, a webpage is requested and a username and password is sent to provide authentication of the user to the service. When the communication is actually sent, the message will be encapsulated in a structure akin to a file and uploaded to the server. The server will examine the communication and copy it to another location on the server or another server in the Google network where the recipient can access it. Once the recipient checks for the communication, they will be presented with the content of the message akin to downloading a file with the message in it. This data will then be interpreted by an application on the user's machine and displayed appropriately to the recipient. In all cases, the communication was sent to the server, copied to another location on the server or within the

[19] Google encrypts all its users' traffic, and the IP packets themselves simply record communications to and from Google's servers and individual users. Without decrypting and looking at the content of the email, GCHQ will not know who Gmail emails are to or from.

network and the recipient given access to read it. There is no meaningful technical distinction between an email or a message.

57. In this context, an individual sending a communication will have little idea which of their communications leave the United Kingdom, and which stay within, let alone whether they are being treated as "internal" or "external" for the purposes of RIPA.

58. The only reason that I can imagine for the introduction of such this new secret classification is that it enables the Government to classify a greater number of "internal" communications (in the sense of communications between individuals in the UK) as "external" for surveillance purposes.

59. Consider if the friends relayed the same message via a voice or video chat using Google Hangouts. Data, this time in the form of audio and video, would be uploaded to the Google server and then sent to the recipient. As pointed out by the government, Google's servers are outside the UK. The Government has already admitted that the upload and download of emails, that may include voice and video, is deemed internal when the users are located within the UK and should be considered "internal". It appears, however, that Google Hangout may be considered "external" given the Government's "platform" analysis set out for the first time in Mr Farr's statement in these proceedings,

60. This question gets more complicated when examining in closer detail how internet-based instant messaging is slowly replacing the text message. If a UK mobile phone customer wishes to send a short message to another UK mobile phone, traditionally they would use a Short Messaging Service (SMS), otherwise known as a text message. The transmission of this SMS would probably have been confined to the UK, and thus be considered an internal communication. There is no obvious reason why an ordinary SMS between two people in London would have left the UK for processing. However, in the last few years, instant messaging (IM) chat apps such as Google Hangout or Facebook Messenger have replaced traditional SMS services; today, more IMs are sent than text messages. According to one report by Informa almost 19 billion messages were sent per day on chat apps in 2012, compared with

17.6 billion SMS texts.[20] IM chat apps may indeed involve what were originally internal communications travelling externally via the company servers of the application provider.

61. These instant messaging platforms are deeply integrated into the other services that large internet services provide. As explained above, Google Hangout, is the default way to chat in the Gmail infrastructure, but also the default way to chat in the Google Plus infrastructure. Although routed externally and thus intercepted under TEMPORA, according to Mr Farr's, statement, Gmail falls as an "internal" communication, but Google Plus presumably falls within his category of a "platform" and is thus an external communication. It is entirely unclear in which of the two categories a text message, sent via the Google Hangout application on an Android mobile phone, would fall following the Government's analysis.

62. Importantly, for many with the latest smart phones, this type of change will have happened without them noticing. Now, when an individual opens the messaging application on an Android phone and sends a message to another Android phone, it is automatically detected, the message is automatically sent using Google Hangout. The only indication the user gets that their communication has been routed to Google servers outside the UK instead of staying inside the UK is a one-time pop-up notification. A similar functionality exists by default for anyone that uses the latest version of Apple's smart phone operating system, which uses iMessage.

63. The position, therefore, is that, as set out in the following section, a large number of "internal" communications will be routed externally and incidentally collected under TEMPORA. Further it now appears that GCHQ has relied on a secret, hitherto unpublished interpretation of the law, namely that people in the UK don't communicate with *each other* on modern communication platforms, they only communicate with the platform itself. Individuals using such platforms are communicating "externally" rather than "internally" and as such have none of the safeguards and protections afforded to internal communications.

[20] "Chat app messaging overtakes SMS texts, Informa says," *BBC News* (29 April 2013).

**What quantity of domestic communications is incidentally collected?**

64. Furthermore, even on the Government's analysis of an email between two people in the UK qualifying as "internal" it is likely that a majority of such communications, transmitted using Internet Protocol, will be "incidentally" caught within GCHQ's mass interception programme, TEMPORA. It is difficult to understand the contention, made by the Interception Commissioner, [21] that only an "extremely small percentage" of communications between people in the UK will be intercepted under the TEMPORA programme.

65. *The Guardian* reported that, according to one source who has been directly involved in GCHQ operations, concerns were raised when the programme was put into place about the quantity of communications solely between UK residents that would be caught up in TEMPORA:[22]

> "*Internet traffic is also liable to be routed internationally even if the message is exchanged between two people within the UK. "At one point, I was told that we were getting 85% of all UK domestic traffic – voice, internet, all of it – via these international cables.*"

66. The automatic transmission of communications that would have traditionally stayed within the British Islands outside the United Kingdom is growing, without the knowledge of the individuals to whom they pertain. SMS text messages being transmitted via internet-based instant messaging programmes is just one example of this trend. With 29 per cent of UK smart phone users owning an iPhone and 44 per cent of UK smartphone users owning an Android,[23] devices which contain the default settings described above, the amount of communications that leave the United Kingdom has certainly increased. Moreover, with email hosts, social networking websites, and VoIP (Voice over Internet Protocol) services like Skype all being run and transmitted by Silicon Valley companies, significant quantities of "internal" communications between UK residents are leaving the UK, and being swept up GCHQ's mass interception programmes.

---

[21] *2013 Annual Report of the Interception of Communications Commissioner,* p. 55.
[22] Davies, "MI5 feared GCHQ went 'too far' over phone and internet monitoring," *The Guardian* (22 June 2013).
[23] Ofcom, *International Communications Market Report* (12 December 2013), p. 210

67. In addition, a growing number of UK residents' private activities, which never previously involved communications systems, are now habitually conducted via IP-based communications and consequently transmitted externally, thus enabling their collection by TEMPORA. Whereas previously our private documents were stored in filing cabinets under lock and key, and months could pass without one having the need or luxury of making an international phone call, now, private documents are stored in unknown data centers around the world, international communications are conducted daily, and our lives are lived – ideas exchanged, financial transactions conducted, intimate moments shared – online. Indeed, intelligence services have recognised that changes in the way people interact with technologies and the internet have enabled wider-reaching and more invasive surveillance practices. A leaked NSA strategy document, for example, noted that:

> "*Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend projected to continue; ubiquitous computing is fundamentally changing how people interact as individuals become untethered from information sources and their communications tools; and the traces individuals leave when they interact with the global network will define the capacity to locate, characterize and understand entities*."[24]

68. "Ubiquitous computing" is being exploited by GCHQ. Consider access to news sources; whereas traditionally, an individual's choice of newspaper was known only to them and to their newsagent, now 35 per cent of the British public relies upon internet news platforms, many of which are hosted outside the United Kingdom, as their main source for news.[25] An individual reading a newspaper's online edition hosted outside the United Kingdom will certainly be swept up by TEMPORA, and their activity may additionally be likely to be considered an "external" communication, thus losing all safeguards and protections.

69. Another example of the UK Government acquiring data about activities that they would have previously not had any access to is the ability to intercept searches and queries made via search engines and online knowledge

[24] NSA SIGINT Strategy, 23 February 2012, p. 2.
[25] Ofcom, *International Communications Market Report* (12 December 2013).

platforms. Traditionally, in order to acquire information or consult authoritative sources, people visited their local library, or consulted their own encyclopedia. Today, more information than could possibly be held by any library or encyclopedia is easily available and widely accessed by people via the internet. The top three search engines used by the British public to search for information on the internet (Google, Microsoft Bing, and Yahoo!) are all hosted externally from the United Kingdom. Likewise, access by the British public to the world's largest and most popular general reference resource, Wikipedia, will likely to be considered an "external" communication, and thus have none of the safeguards and protections.[26]

## III. INTELLIGENCE SHARING PRACTICES

70. The highly integrated relationship between the US and the UK intelligence services must be viewed within the context of a long-standing intelligence sharing arrangement that binds together the intelligence activities of the two countries, along with Australia, Canada and New Zealand. The agreement provides for the full exchange of intelligence collected, the division of tasks amongst agencies of the five States to prevent duplicity, high levels of cooperation, including provision for jointly run facilities, and the extensive dissemination of intelligence analysis.

### The Five Eyes alliance

71. Beginning in 1946, the United Kingdom developed a series of bilateral agreements with the United States, Australia, Canada and New Zealand over more than a decade that became known as the UKUSA agreement, establishing the "Five Eyes" alliance for the purpose of sharing intelligence, but primarily signals intelligence derived from the interception of communications travelling and transmitted by fibre optic cables, radio waves, satellites, and other forms of wireless telegraphy.

72. Since its inception, the Five Eyes alliance has been shrouded in secrecy. It was not until 2010 that the text of the original agreement was declassified and

[26] Ofcom, *International Communications Market Report* (12 December 2013), p. 222.

published, concurrently by the US and UK governments. Accordingly, even within the governments of the respective countries, there has historically been little appreciation of the extent of the arrangement. The arrangement is so secretive that the Australian Prime Minister reportedly wasn't informed of its existence until 1973.[27] Former Prime Minister of New Zealand, David Lange, once remarked that "*it was not until I read this book* [Nicky Hager's "Secret Power", which detailed the history of New Zealand's SIGINT agency, the Government Communications Security Bureau ("GCSB")] *that I had any idea that we had been committed to an international integrated electronic network*." He continued: "*it is an outrage that I and other ministers were told so little, and this raises the question of to whom those concerned saw themselves ultimately answerable*."[28]

73. A biography of US wartime hero Colonel William F. Friedman, published in 1977, suggested that, from the outset, the relationship was a highly integrated one, particularly as it concerned the cooperation of American and British agencies:

> "*In 1946 Friedman himself again visited the British cryptographers, now moved to Cheltenham, and helped work out methods of postwar collaboration. An American Liaison Office was set up in London and schemes were devised for avoiding duplication of effort. Solved material was to be exchanged between the two agencies and, more important, an interchange scheme was started under which men from each agency would work two or three years at the other. The only problem was to ensure that the British should be kept away from American work on breaking British ciphers and that the Americans at Cheltenham should be treated reciprocally.*"[29]

74. Outside of footnotes in history books and passing references made in the course of reporting on the intelligence agencies, there is little public knowledge or understanding of exactly what the arrangement comprises. Indeed, Mr Farr's statement is the most complete public account I have ever read given by the British government on the nature of the relationship.

---

[27] Chittley and Newman, "Canada's role in secret intelligence alliance Five Eyes," *CTV News* (8 October 2013).
[28] Nicky Hager, *Secret Power* (1996), p. 8.
[29] Clark, *The Man Who Broke Purple, The Life of Colonel William F Friedman, Who Deciphered the Japanese Code in World War II* (1977), p. 208.

**Full exchange of intelligence**

75. The original UKUSA agreement, declassified more than 60 years after its execution in 2010, explains that the exchange of the intelligence between the parties

> "*will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon*."

76. Indeed, in addition to facilitating collaboration, the agreement suggests that all intelligence material is shared between Five Eyes States by default. The text stipulates that "*all raw traffic shall continue to be exchanged except in cases where one or the other party agrees to forgo its copy*."

77. In an essay[30] by an ex-NSA employee marked UNCLASSIFIED and approved for public release by the NSA's office of Pre-Publication Review it was confirmed that:

> "*If you are a citizen of the UK, Canada, New Zealand, or Australia, you may also be glad, because everything the NSA collects is by default shared with your government.*"

**Division of tasks**

78. The Five Eyes arrangement therefore not only creates a set of principles of collaboration, and facilitates information sharing, but, in an effort to minimise the duplication of SIGINT collection, imagines the division of tasks between SIGINT agencies from the respective parties. The agreement explains:

> "*Allocation of major tasks, conferring a one-sided responsibility, is undesirable and impracticable as a main principle; however, in order that the widest possible cover of foreign cypher communications be achieved the COMINT agencies of the two parties shall exchange proposals for the elimination of duplication. In addition, collaboration between those agencies*

[30] Sands-Ramshaw, "The NSA: An Inside View," *Loren's Blog* (10 December 2013) - http://lorensr.me/nsa-an-inside-view.html

*will take the form of suggestion and mutual arrangement as to the undertaking of new tasks and changes in status of old tasks."*[31]

79. The continuing policy of dividing tasks between agencies was confirmed in 1986 by former Defense Secretary Caspar Weinberger, who observed that the "*United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing arrangements with other nations in the world*."[32] The website of the Communications Security Establishment Canada ("CSEC") explains how it "*relies on its closest foreign intelligence allies, the US, UK, Australia and New Zealand to share the collection burden and the resulting intelligence yield.*"[33] Other former intelligence analysts have confirmed that "task-sharing" continues to take place amongst the Five Eyes agencies.[34]

**High level of cooperation and integration**

80. The level of co-operation under the UKUSA agreement is so complete that "*the national product is often indistinguishable*."[35] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "*that SIGINT customers in both capitals seldom know which country generated either the access or the product itself.*"[36] Another former British signals intelligence officer has said that "*[c]ooperation between the two countries, particularly, in SIGINT, is so close that it becomes very difficult to know who is doing what [...] it's just organizational mess.*"[37]

81. The relationship is so close that one senior member of Britain's intelligence community told the Guardian[38] "*[w]hen you get a GCHQ pass it gives you access to the NSA too. You can walk into the NSA and find GCHQ staff holding senior management positions, and vice versa.*"

---

[31] UKUSA Agreement, Appendix E, *Co-ordination of, and exchange of information on, cryptanalysis and associated techniques*, p. 34.
[32] Declaration of the Secretary of Defence Caspar W Weinberger, USA v Jonathan Pollard (1986).
[33] *Safeguarding Canada's security through information superiority*, CSEC website.
[34] "Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance," *Japan Times* (18 November 2013).
[35] Aldrich, *Transatlantic intelligence and security co-operation* (2006).
[36] Lander, "International intelligence cooperation: an inside perspective," 17 *Cambridge Review of International Affairs* 3 (2007) p.487.
[37] "Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance," *Japan Times* (18 November 2013).
[38] Hopkins, "From Turing to Snowden – how US-UK pact forged modern surveillance," *The Guardian* (2 December 2013)

**Jointly run facilities**

82. Many intelligence facilities run by the Five Eyes parties are jointly operated, even jointly staffed, by members of intelligence agencies of Five Eyes countries. Each facility collects SIGINT, which can then be shared with the other Five Eyes members.

83. An earlier incarnation of Australian Signals Directorate ("ASD"), the Defence Signals Branch, was housed in a Melbourne facility that was described in the 1956 UKUSA agreement as

> "*not purely a national centre. It is and will continue to be a joint U.K – Australian – New Zealand organization manned by and integrated staff. It is a civilian organization under the Australian Department of Defence and undertakes COMINT tasks as agreed between the COMINT governing authorities of Australia and New Zealand on the one hand and the London Signal Intelligence Board on the other. On technical matters control is exercised by GCHQ on behalf of the London Signal Intelligence Board.*" [39]

84. In addition to bases in Australia and New Zealand, Britain's legacy of Empire allowed GCHQ a widespread network of SIGINT outposts. Intelligence stations in Bermuda, Cyprus, Gibraltar, Singapore and Hong Kong have all played critical collection roles over the past 60 years.

85. One of the largest Five Eyes listening posts outside the US is based in northern England and has been under US control since the 1950s. It was not until 1996 that the base was renamed RAF Menwith Hill, and the Union Jack was reportedly raised for the first time alongside the Stars and Stripes. Yet David Bowe, MEP for Cleveland and Richmond, said this change was "*designed to mislead*" and that "*[m]y information is that the RAF representation on the base amounts to one token squadron leader. The name change was presumably decided to make the whole site look more benign and acceptable.*"[40] The base was the

---

[39] "The Defence Signals Bureau was established in 1947, as part of the Department of Defence, with responsibility for maintaining a national sigint capability in peacetime. In 1977, DSD assumed its current name". See *Inquiry into Australian Intelligence Agencies – Chapter 7, Resourcing and effectiveness of the agencies* (2004), p. 135.

[40] "US spy base `taps UK phones for MI5'", *The Independent* (22 September 1996).

subject of a six billion pound investment over the subsequent 20 years, with the majority of those funds likely to have originated in the US. [41]

86. Other bases, such as the GCHQ base at Bude, in the South West of England, are also jointly staffed. *The Guardian* reported that GCHQ and the US National Security Agency ("NSA"), in addition to jointly developing the TEMPORA program, jointly examine material collected under the programme at Bude, where some 300 GCHQ analysts and 250 NSA analysts are located.[42] It is assumed that a continuation of the arrangement highlighted by Colonel William F. Friedman in which *"an interchange scheme was started under which men from each agency would work two or three years at the other"*[43] continues to be in effect, and that GCHQ staff are also located in the US at NSA run bases.

**Intelligence collection, analysis and dissemination**

87. As early as the 1980s, the Five Eyes countries used a "global Internet-like communication network to enable remote intelligence customers to task computers at each collection site, and receive the results automatically."[44] This network was known as ECHELON and was revealed to the public in 1988 by investigative journalist Duncan Campbell.[45] An often-misunderstood term, ECHELON is in fact a

> *"code name given by the NSA (U.S. National Security Agency) to a system that collects and processes information derived from intercepting civil satellite communications. The information obtained at ECHELON stations is fed into the global communications network operated jointly by the SIGINT*

[41] "US spy base `taps UK phones for MI5'", *The Independent* (22 September 1996).
[42] An early version of TEMPORA is referred to as the Cheltenham Processing Centre, additionally codenamed TINT, and is described as a "joint GCHQ/NSA research initiative". The Guardian quotes an internal GCHQ report that claims "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures." It was additionally reported that NSA provided GCHQ with the technology necessary to sift through the material collected. The Guardian reported that 300 analysts from GCHQ and 250 from NSA were directly assigned to examine the collected material, although the number is now no doubt much larger. GCHQ have had staff examining collected material since the project's incarnation in 2008, with NSA analysts brought to trials in Summer 2011. Full access was provided to NSA by Autumn 2011. An additional 850,000 NSA employees and US private contractors with top secret clearance reportedly also have access to GCHQ databases.
[43] Clark, *The Man Who Broke Purple, The Life of Colonel William F Friedman*, Who Deciphered the Japanese Code in World War II (1977), p. 208.
[44] Duncan Campbell, *Inside Echelon* (2000) – http://www.heise.de/tp/artikel/6/6929/1.html
[45] "Somebody's listening," *New Statesmen* (12 August 1988).

*organisations of the United States, United Kingdom, Australia, Canada and New Zealand."*[46]

88. A more recently-revealed NSA developed system XKEYSCORE is a core part of a number of the Five Eye other codenamed programs and has sites that appear in Five Eyes countries,[47] with the New Zealand's Waihopai Station, Australia's Pine Gap, Shoal Bay, Riverina and Geraldton Stations, and the UK's Menwith Hill base all present. It has been confirmed that all these bases use XKEYSCORE and "contribute to the program."[48]

89. Other shared and integrated databases have been created by the NSA and GCHQ, as revealed by one NSA document that references "GCHQ-accessible 5-eyes [redacted] databases."[49] One Guardian article explained:

> *"Legal training sessions – which may also be required for access to information from Australian, Canadian, or New Zealand agencies – suggest that gaining credentials for data is relatively easy. The sessions are often done as self-learning and self-assessment, with "multiple choice, open-book" tests done at the agent's own desk on its "iLearn" system. Agents then copy and paste their passing result in order to gain access to the huge databases of communications."*[50]

## IV. UK ACCESS TO US SIGNALS INTELLIGENCE

90. It is apparent from recently revealed information that the UK has extensive access to both the raw signals intelligence (i.e. data collected through direct interception of communications, or through the provision of access by corporate entities) and refined signals intelligence (i.e. data that has been analysed, collated, optimised, extrapolated upon, cultivated or discerned from raw signals intelligence) produced by the US. This SIGINT is collected

---

[46] *Echelon and its role in COMINT*, Temporary Committee on the Echelon Interception System, Brussels Meeting, 22-23 January 2001, p. 2.
[47] NSA XKEYSCORE presentation, retrieved from *The Guardian,* p. 5.
[48] Dorling, "Snowden reveals Australia's Links to US Spy Web," *The Sydney Morning Herald (*7 August 2013).
[49] Ball, "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data," *The Guardian* (20 August 2013).
[50] MacAskill and Ball, "Portrait of the NSA: no detail too small in quest for total surveillance," *The Guardian (*2 November 2013),

by the US through a number of programmes described below, primarily through corporate partnerships that facilitate the interception of undersea fibre optic cables and the provision of access to stored communications data and content. Because of the NSA's pervasive access, it collects a large majority of the world's communications, including a significant amount of signals intelligence pertaining to UK residents and which will include numerous communications that, on any analysis, are "internal" communications between two people located in the UK.

91. On 6 June 2013 *The Guardian* and *The Washington Post* published reports on the existence of an extensive intelligence-gathering programme operated by the NSA. The scope of the reported programme was unprecedented, giving the US access to the communications, documents, emails, videos and much more of non-US persons located outside of the US. Both newspapers based their stories on a 41-slide presentation leaked by former NSA system administrator Edward Snowden.[51]

92. The documents disclosed by Edward Snowden have been provided to a number of newspapers and the United States has confirmed the existence of a number of the programmes revealed by the documents. In the UK, D notices have been served on *The Guardian* with respect to the material; David Miranda, the partner of one of the lead journalists on the Snowden stories, was detained and charged for possessing classified documents.

93. The slide published by both *The Guardian* and *The Washington Post* details two programmes, PRISM and UPSTREAM collection, purportedly authorized by section 702 of the FISA Amendments Act 2008.

**PRISM**

94. According to *The Guardian*, NSA documents describe PRISM as "*one of the most valuable, unique and productive accesses*."[52]

---

51 Greenwald and MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian* (6 June 2013); Gellman and Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post* (7 June 2013); "NSA slides explain the PRISM data- collection program," *The Washington Post* (6 June 2013).

52 Greenwald and MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian* (6 June 2013)

95. Through PRISM, the NSA has gained access to the data and content handled by some of the world's largest Internet companies, including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The released slides and subsequent reporting have left open the question of how exactly the NSA accesses this information, and the mechanism likely varies from company to company. According to *The Washington Post,* "*collection managers [can send] content tasking instructions directly to equipment installed at company-controlled locations*."[53] *The New York Times* has reported that while special equipment is not installed at company facilities, discussions at both Facebook and Google took place to "*build separate, secure portals, […] in some instances on company servers. Through these online rooms, the government would request data, companies would deposit it and the government would retrieve it*."[54]

96. Google has stated that the NSA does not have direct and automated access to data but rather the ability to compel the provision of information from internet services: "*[w]e refuse to participate in any program -- for national security or other reasons -- that requires us to provide governments with access to our systems or to install their equipment on our networks […] [w]hen required to comply with these requests, we deliver that information to the US government -- generally through secure FTP transfers and in person*."[55] Secure FTP is a standard protocol for transferring files over an encrypted channel.

97. NSA presentation slides list the types of "Surveillance and Stored Comms" available through PRISM:

> " - *E-mail*
>
> - *Chat – video, voice*
> - *Videos*
> - *Photos*
> - *Stored data*

[53] O'Harrow JR., Nakashima, and Gellman, "U.S., company officials/ Internet surveillance does not indiscriminately mine data" *The Washington Post* (8 June 2013).
[54] Miller, "Tech Companies Concede to Surveillance Program", *The New York Times* (8 June 2013).
[55] Zetter, "Google sends Prism data to NSA by secure FTP or 'by hand'" *Wired* (12 June 2013).

- *VoIP*
- *File transfers*
- *Video Conferencing*
- *Notifications of target activity – logins etc.*
- *Online Social Networking details*
- ***Special Requests.***" (emphasis in original)[56]

98. The NSA's list is consistent with the type of data the identified internet companies have access to, but it is by no means exhaustive. Unlike phone companies, the vast majority of internet companies store both the data about users' transactions, as well as the content of the transactions themselves. They do this mostly in order to provide users with the service itself, e.g. a record of all of a user's emails. However they often collect other types and amounts of information in order to better profile users and deliver targeted advertisements. The information collected would include, but not be limited to, the location from which a communication originated, the device that sent the communication, the Internet Protocol address of the sender, the time at which it was sent, the recipient of the communication and his/her device and IP address, the size or length of the communication. The companies will also collect data on, for example, what searches users conduct, what websites they visit and the time users stay on a particular website, what advertising they respond to, and what videos they watch.

99. Email services such as Gmail commonly retain copies of a user's emails in the Inbox or Archived folders of the service for later reference. Attachments, both sent and received, as well as drafts are all stored. Additionally the user's list of contacts will be retained by Google. This information is stored by Google on at least two servers at data centres operated by the company. If signed into a Google account (such as Gmail), all searches performed by a user anywhere in the world, including the UK, will be logged and recorded by Google.

[56] NSA PRISM presentation, retrieved from *The Guardian.*

Search results clicked on will also be recorded and may be retained, resulting in the collection of the majority of a person's internet browsing history. Services such as Google Docs/Google Drive allow users to store and edit in real time text documents, spread sheets and presentations. These services are increasingly becoming standard in many industries and could therefore be used to exchange sensitive and confidential information. In the circumstances, information stored by companies like Google reveal a huge amount of information about anyone who uses their service. The information when read together can build a picture of a person's private and family life including their interests (political or otherwise), activities, friends and familial relationships and sexual orientation. All of this data can be requested by the NSA under the PRISM program.

**UPSTREAM collection**

100. While PRISM provides the NSA with access to a vast amount of information, the slides reveal the agency has implemented another method for obtaining the communications of people located outside the US. An NSA presentation slide published by *The Guardian*, entitled "FAA 702 Operations: Two Types of Collection" exhorts the NSA to "*use both*" PRISM and a form of collection labeled "UPSTREAM."[57]

101. In the slide, UPSTREAM is described as the "*collection of communications on fibre cables and infrastructure as data flows past.*" This description is superimposed over a map of the world that contains brown lines that track the routes of the world's major undersea fibre-optic cables. It is estimated that fibre optic cables carry around 90% of the world's communications. By intercepting these cables, therefore, the NSA has access to an almost unlimited array of data and content.

102. It is not only communications between persons located in different countries that are transmitted via the undersea cables. Communications between two people within a country's national boundaries may be routed outside of the country for efficiency or other reasons as has been explained above. As another NSA presentation slide explains, "*much of the world's communications*

[57] NSA PRISM presentaiton, retrieved from *The Guardian.*

*flow through the US*." It continues, "*A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path. Your target's communications could easily be flowing into and through the U.S.*" (emphasis in original). The US thus appears to have the ability to intercept the world's communications as they travel through the US.

103. An NSA presentation slide released by Dutch Newspaper *NRC Handelsblad* on 23 November 2013, depicts a map of the NSA's "Worldwide SIGINT/Defense Cryptologic Platform.[58] Large blue dots are used to show 20 locations where the NSA has "High Speed Optical Cable" access, which it describes as being made up of "Covert, Clandestine or Cooperative Large Accesses." This suggests that the US is also intercepting fibre optic cables outside of US territory in order to conduct UPSTREAM collection.

104. It is likely that the references to UPSTREAM collection in the NSA slides refer to a number of different programmes that enable access to under-sea fibre optic cables through a variety of methods. These programmes are known by a wide variety of codenames and involve partnerships with telecommunications companies to enable the NSA direct access to fibre optic cables within the US and internationally. Each of the programmes has different authorizations, activities and targets.

105. Using a combination of overseas access points, the hacking of international infrastructure[59], key domestic communications infrastructure "chokepoints" under the STORMBREW [60] program and corporate partners artificially shaping the natural route of communications traffic to run past NSA monitors[61], collectively these programmes enable the US to collect a large majority of the world's communications, including a significant amount of signals intelligence pertaining to UK residents. The *Wall Street Journal* has reported that, collectively, UPSTREAM collection programmes enable the NSA the capability to collect roughly 75% of all internet traffic flowing

[58] Boon, Derix and Modderkolk, "NSA infected 50,000 computer networks with malicious software," *NRC.*
[59] "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Spiegel Online* (29 December 2013).
[60] Greenwald, *No Place to Hide,* 2014, p. 107
[61] Greenwald, *No Place to Hide,* 2014, p. 105.

through the US.[62] Given the concentration of internet companies such as Google and Facebook in Silicon Valley, California, much of the world's internet traffic flows through the United States. Many emails, or VoIP (Voice Over IP) calls like Skype made anywhere in the world will pass through cables in the US, or connect to servers in the US at some point in the course of transmission. Even internet communications between two people in London will on many occasions be sent to a server located outside the UK, then sent on to the recipient back in the UK. Therefore, the NSA's extensive access to US internet traffic in effect means the American intelligence services have access to a significant proportion of worldwide internet traffic, including "internal" communications of UK residents seeking to email, phone or otherwise communicate with one another.

**Additional programmes operating within UPSTREAM**

*DISHFIRE*

106. The NSA has a number of programmes designed to organize, analyse and optimize data collected under the PRISM and UPSTREAM collection programmes. Such additional programmes can be run on top of existing interception points and already intercepted material to retrieve certain categories of information that don't meet specific targets that relate to people, classes of people, or even keywords. For example, *The Guardian* has reported that the NSA collects an average of 194 million text messages daily under a programme called DISHFIRE.[63] According to documents, the programme collects and stores "*pretty much everything it can*" including text messages that don't meet any selection criteria. The programme can extract specific data or derive additional information from data intercepted via UPSTREAM collection. DISHFIRE has reportedly been used to identify 1.6 million border crossings a day, more than 110,000 names from electronic business cards, and 800,000 financial transactions by text-to-text payments or linking credit cards to phone users. The NSA was also able to extract geo-location information from the data, using information from travel itineraries sent by text, including

[62] Gorman and Valentino-Devries, "New Details Show Broader NSA Surveillance Reach," *The Wall Street Journal* (20 August 2013).
[63] Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian* (16 January 2014).

cancellations and delays to travel plans. *The Guardian* explains in reference to internal documents that under DISHFIRE "*It is also possible to search against the content in bulk (e.g. for a name or home telephone number) if the target's mobile phone number is not known*." Analysts were asked to restrain their searches to no more than 1,800 phone numbers at any one time.

*CO-TRAVELLER*

107. The NSA also collects nearly five billion records a day pertaining to the location of mobile phones around the world, under a set of programmes known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the organization is collecting so much locational information under the programme it is "outpacing our ability to ingest, process and store" the data.[64] Locational data is incredibly intimate and invasive; it allows NSA to track from afar people going into medical facilities, in hotel rooms, private homes, or at places of religious worship, or attending protests and demonstrations, and mine that data for patterns. Location data can be mined to draw a map of connections and networks, linking the world together into a large social map based on locational habits.

*Content Acquisition Optimisation*

108. A further example of an NSA programme is the harvesting of hundreds of millions of contacts lists from email and instant messaging accounts around the world. Rather than targeting individual users, the NSA is gathering the contact lists in large numbers that amount to a sizable fraction of the world's e-mail and instant messaging accounts. According to *The Washington Post*[65]

> "*During a single day last year, the NSA's Special Source Operations branch collected 444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers, according to an internal NSA PowerPoint presentation. Those figures, described as a typical daily intake in the document, correspond to a rate of more than 250 million a year.*"

---

[64] Gellman and Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," *The Washington Post* (4 December 2013).
[65] Gellman and Soltani, "NSA collects millions of e-mail address books globally," *The Washington Post* (14 October 2013).

109. *The Washington Post has* subsequently confirmed that GCHQ has assisted the NSA in the collection of contact lists from personal e-mail and instant-messaging accounts.

110. As with CO-TRAVELLER, the collection of contacts is such a significant collection activity for the NSA it occasionally threatens to overwhelm storage repositories.[66] Intercepted contact lists are often richer sources of data than email or text message records. Address books commonly include not only names and e-mail addresses, but contact photographs, telephone numbers, street addresses, business and family information, as well as links to online profiles that might be under pseudonyms or nicknames. Cumulatively, such data can be hugely revelatory, suggesting political, religious or professional connections, as well as misleading, hinting at associations and relationships that have long since lapsed.

*MYSTIC and SOMALGET*

111. Capabilities to record and store copies of 100 per cent of telephone calls made in a particular country are also in use by the NSA. The NSA's voice interception programme, codenamed MYSTIC and SOMALGET, is referred to as a "time machine" because it enables the NSA to replay the records of any telephone call without requiring that a individual be targeted in advance for surveillance.[67] It has already been implemented in a number of countries, with a combined population of more then 250 million people. According to *The Intercept,*[68] the NSA is seeking to expand this capability elsewhere.

112. One of the countries being targeted by this programme is the Bahamas. According to *The Intercept*, the justification for mass interception is that the country provides a good "test bed for system deployments, capabilities, and improvements." [69] According to one NSA document, SOMALGET is "deployed against entire networks" in the Bahamas and in another unnamed

[66] Gellman and Soltani, "NSA collects millions of e-mail address books globally," *The Washington Post* (14 October 2013).
[67] Gellman and Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *The Washington Post* (18 March 2014).
[68] Devereaux, Greenwald and Poitras, "Data Pirates of the Caribbean/ The NSA Is Recording Every Cell Phone Call in the Bahamas," *The Intercept* (19 April 2014).
[69] Devereaux, Greenwald and Poitras, "Data Pirates of the Caribbean/ The NSA Is Recording Every Cell Phone Call in the Bahamas," *The Intercept* (19 April 2014).

country (later revealed by Wikileaks to be Afghanistan), and processes "over 100 million call events per day".[70]

113. Other versions of SOMALGET have been deployed in Mexico, Kenya, and the Philippines, where the NSA is recording, storing and analysing metadata related to every single telephone call and text message transmitted in the country.

**The reach of US SIGINT**

114. In his statement, Mr Farr cites an NSA document that claims the SIGINT agency "touches" approximately 1.6 per cent of the data carried over the internet across the world. This is in fact an extraordinary amount of data. Using the NSA's figure of the internet carrying 1,826 petabytes of information per day, touching 1.6 per cent is still 29.21 petabytes of data a day. It is equivalent to the daily collection a third of all the data that Facebook has ever collected, which in 2012 was 100 petabytes.[71] It is equivalent to processing the entire Library of Congress 90,000 times every single day, and amounts to more than Google processed every single day in 2009, which is around 24 petabytes. [72]

115. The seemingly small percentage of data collected by the NSA is undoubtedly due to the fact that the vast majority of data carried over the internet would have no possible signals intelligence value. According to a recent report from Sandvine,[73] streaming video and audio are the largest traffic category on virtually every network they examined. Netflix and YouTube alone accounts for 50 per cent of the total monthly network traffic, of which NSA would take steps to avoid intercepting, as the intelligence value is likely to be limited. It is likely, therefore, that NSA surveillance architecture is designed to avoid low value intelligence collection, targeting only data of possible interest and value. Indeed, the NSA's "touching" of 1.6 per cent of internet data could represent the collection of a majority of all transmitted metadata pertaining to person-to-person communications of interest to the NSA.

---

[70] NSA SSO Dictionary Excerpt, Retrieved from Document Cloud.
[71] United States Securities and Exchange Commission, *Registration Statement on Form S-1, Facebook.*
[72] Dean and Ghemawat, "MapReduce - Simplified Data Processing on Large Clusters," 51 *Communications of the ACM* 1 (January 2008), p. 107-113.
[73] "Netflix And YouTube Account For 50% Of All North American Fixed Network Data," *Sandvine* (11 November 2013).

116. In any event, the choice of the word "touch" to describe NSA's SIGINT activities is apt to mislead. According to *The Wall Street Journal*, the NSA defines "touching" as things that are actually accessed by analysts *after* communications have been intercepted and filtered on the basis of selectors.[74] The explain that according to internal NSA documents:

> *"The systems operate like this: The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the data.*
>
> *These requests don't ask for all Internet traffic. Rather, they focus on certain areas of interest, according to a person familiar with the legal process. "It's still a large amount of data, but not everything in the world," this person says.*
>
> *The second cut is done by NSA. It briefly copies the traffic and decides which communications to keep based on what it calls "strong selectors"—say, an email address, or a large block of computer addresses that correspond to an organization it is interested in. In making these decisions, the NSA can look at content of communications as well as information about who is sending the data.*
>
> *One U.S. official says the agency doesn't itself "access" all the traffic within the surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering."*

117. Therefore, the data that is actually intercepted, processed and analysed in some way is far larger than the 1.6 per cent. There is no figure provided by NSA to estimate the size of this larger proportion of pre-filtered data handled by the agency, but the Wall Street Journal has reported that NSA systems have the capacity to reach roughly 75% of all U.S internet traffic. As NSA's mission is foreign intelligence, and in theory they are constrained from spying on Americans, it is feasible the number the number for non-US internet traffic could be much higher.

---

[74] Gorman and Valentino-Devries, "New Details Show Broader NSA Surveillance Reach," *The Wall Street Journal* (20 August 2013).

**The parameters of the UK's access to US signals intelligence**

118. Through its PRISM and UPSTREAM collection programmes, the US has access to any communications pertaining to a UK resident that transit through cables that are being intercepted by the NSA, both within the US or in its bases overseas. A significant proportion of the communications sent and received by a UK resident will transit through such cables. This would likely include all communications sent by or searches made using a US-based service provider (Gmail, Yahoo, Facebook, Twitter, etc.), as well as many more communications that transit through the US simply because a large percentage of the world's fibre optic cables land in or traverse the US. All of these communications are collected, stored and index in any number of NSA programmes. It is also clear that GCHQ has access to much of the information.

119. There is conflicting information available in the public domain over the type and kind of access that GCHQ has had to NSA interception programmes and it is likely that slightly different rules apply to each programme in order to take account of the sensitivity of the programme and the wishes of any corporate partners involved, among other issues.[75] It is plain though that the relationship is not simply that the US may "share" potentially relevant and targeted information that they obtain, but that GCHQ has historically had access to all information, and that, more recently, at least on certain occasions and potentially on a regular basis, the UK directly accesses the data collected by the US PRISM and UPSTREAM programmes. There is no legal regime or published policy to indicate when and how this access will occur. The UK Government to date has provided limited information about the conditions under which it directly accesses US signals intelligence, including policies or procedures concerning retention or sharing of data with third parties. However, GCHQ documents quoted by *The Guardian* on 21 June 2013 confirm that "GC*HQ analysts effectively exploit NSA metadata for intelligence production, target development/discovery purposes*," and "*GCHQ and NSA avoid processing the*

[75] Hopkins, "UK gathering secret intelligence via covert NSA operation," *The Guardian* (7 June 2013).

*same data twice and proactively seek to converge technical solutions and processing architectures*."[76]

120. According to an article published by *The Guardian* on 7 June 2013, GCHQ has had access to the PRISM system since at least June 2010, and generated 197 intelligence reports from the system in 2012.[77] On 17 July 2013 the ISC issued a three-page statement, reporting on its investigation into the allegations regarding PRISM. It absolved GCHQ of circumventing national law by using PRISM, but hinted at the existence of secret internal policies and legal interpretations relied upon by GCHQ: "*In some areas the legislation is expressed in general terms and more detailed policies and procedures have, rightly, been put in place around this work by GCHQ in order to ensure compliance with their statutory obligations under the Human Rights Act 1998[...].*"[78] The ISC also acknowledged that its investigation had only focused on intelligence from PRISM that GCHQ had specifically requested from the US on particular individuals. As such it did not seek to conclude whether or not PRISM data was being shared with the UK through other means.

121. It certainly appears that GCHQ is seeking broader access to PRISM data than is reflected by the numbers reported by *The Guardian* on 7 June 2013. An April 2013 NSA document, published by *The Intercept* on 30 April 2014, reveals that GCHQ had requested broad new authority to access signals intelligence collected under section 70 of the FISA Amendments Act 702, which pertains to both PRISM and UPSTREAM collection data.[79] It is unclear whether the NSA ultimately granted GCHQ's request, although the document suggests that the NSA was supportive of the idea.[80]

122. The document also shows that GCHQ was permitted extensive unsupervised access to PRISM during the 2012 London Olympics. At least 100 GCHQ operatives were given unsupervised access to PRISM throughout the Olympics. *The Intercept* reported that an NSA presentation slide states that in

---

[76] MacAskill, Borger, Hopkins, Davies and Ball, "Mastering the internet - how GCHQ set out to spy on the world wide web," *The Guardian* (21 June 2013).
[77] Hopkins, "UK gathering secret intelligence via covert NSA operation," *The Guardian* (7 June 2013).
[78] "Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme," *Intelligence and Security Committee of Parliament* (17 July 2013).
[79] Gallagher, "British Spy Chiefs Secretly Begged to Play in NSA's Data Pools," *The Intercept* (30 April 2014).
[80] Leppard, "GCHQ tried to plunder US email database," *The Sunday Times,* 1 June 2014.

a single six-day period in May 2012, GCHQ received 11,431 "cuts of traffic" from communications intercepted using PRISM ("cuts" is a term used by the NSA to describe extracts of conversations that it collects). [81]

123. Documents reported by *The Intercept* suggest that GCHQ had hoped that this level of access would be permanent, and that GCHQ was close to concluding an arrangement to gain supervised direct access to PRISM and UPSTREAM communications collected as part of a programme called "Triage 2.0." According to the documents seen by *The Intercept,* this deal, under unspecified conditions imposed by the NSA, was "awaiting signature" from the British agency in April 2013.[82]

124. Other documents show that GCHQ has higher levels of access to other programmes operated by the NSA. Programmes like DISHFIRE, which contain unredacted records of UK phone numbers and communications, can be searched directly by GCHQ under "supervision" and with very few restrictions. It is unclear what supervised access means, but I speculate it will entail the generation of logs that are inspected by the NSA.

125. A note from GCHQ's operational legalities team dated 2008, excerpted in *The Guardian,* explains to GCHQ analysts: "You may run a search of UK numbers in DISHFIRE in order to retrieve only events data." It continues: "this will now enable you to run a search without displaying the content of the SMS, especially useful for untargeted and unwarranted UK numbers."[83] In an attempt to protect content, GCHQ staff, analysts are asked to remember to use to search form's yes/no toggle to ensure that content is not returned from the search result. The Guardian confirmed that "*GCHQ has made use of the NSA database to search the metadata of "untargeted and unwarranted*" communications belonging to people in the UK. [84]

## V. THE UK'S MASS INTERCEPTION PROGRAMMES

[81] Gallagher, "British Spy Chiefs Secretly Begged to Play in NSA's Data Pools," *The Intercept* (30 April 2014).
[82] Gallagher, "British Spy Chiefs Secretly Begged to Play in NSA's Data Pools," *The Intercept* (30 April 2014).
[83] Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian* (16 January 2014).
[84] Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian* (16 January 2014).

126. In addition to accessing raw and refined signals intelligence collected by the NSA through the PRISM and UPSTREAM collection programmes, the UK operates numerous programmes that enable the mass interception and collection of communications content and data. These programmes fall within the agency's MASTERING THE INTERNET and GLOBAL TELECOMS EXPLOITATION projects. These were revealed by *The Guardian* on 21 June 2013,[85] drawing on the same sources that revealed the NSA PRISM and UPSTREAM programmes. These programmes enable GCHQ interception and collection of quantities of communications content and data so large that by 2010 UK officials could claim that GCHQ "produces larger amounts of metadata collection than the NSA."[86]

**TEMPORA**

127. TEMPORA is the name of a core mass surveillance programme within MASTERING THE INTERNET, designed to intercept mass internet traffic that flows through the undersea fibre-optic cables that land in the UK. The GCHQ mass surveillance programme, with assistance from the NSA, revealed by *The Guardian* on 21 June 2013, has, since 2008, steadily been building capability and now claims to provide the "*biggest internet access*" of any intelligence agency in the Five Eyes alliance. According to documents relied upon by *The Guardian*, in 2011 "more than 39bn events in a 24-hour period" were recorded.[87]

128. TEMPORA utilises probes, attached to more than 200 undersea cables, which perform Deep Packet Inspection, allowing the huge volume of traffic to be rapidly filtered and subsequently stored.[88] *The Register*[89] revealed on 3 June 2014 that GCHQ is intercepting more than 18 undersea cables landing in Britain; those specifically identified in GCHQ documents include an Irish connection, Hibernia Atlantic, landing in Southport, as well as three

[85] MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian* (21 June 2013).
[86] MacAskill, Borger, Hopkins, Davies and Ball, "Mastering the internet - how GCHQ set out to spy on the world wide web," *The Guardian* (21 June 2013).
[87] MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian* (21 June 2013)
[88] MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian* (21 June 2013)
[89] Campbell, "Revealed: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base: Snowden leaks that UK.gov suppressed," *The Register* (3 June 2014).

European connections landing at Yarmouth, Dover, and Brighton.[90] In addition, GCHQ's Overseas Processing Centre 1, codenamed CIRCUIT, which is located at Seeb, on the northern coast of Oman, taps into nine undersea cables passing into the Persian/Arabian Gulf. GCHQ operates three interception facilities in Oman.

129. As much as 11 per cent of global internet bandwidth travels through UK internet exchanges.[91] *The Guardian* has reported that interception of fibre optic cables potentially gives GCHQ access to 21 petabytes of data a day. A petabyte is approximately 1000 terabytes (which is in turn 1000 gigabytes). To put this in perspective, the US Library of Congress in 2009 had 15.3 million documents available online, which approximately totalled 74 terabytes. The comparison provided by *The Guardian* was that this was the equivalent to sending all the information in all the books in the British Library across the internet 192 times every 24 hours.

130. TEMPORA stores all intercepted content for three days, and metadata for 30 days. Once content and data are collected, they can be filtered to ascertain, grade and define information. The precise nature of the filters GCHQ has put in place remains secret. Filters could be applied based on type of traffic (e.g. Skype, Facebook, Email), origin/destination of traffic, or basic keyword searches among many others. Reportedly, approximately 40,000 selectors have been chosen and applied by GCHQ, and another 31,000 by the NSA.[92]

131. Data collected by GCHQ, utilising undersea fibre optic cable interception, is thereafter directly accessible by the NSA. A 2011 GCHQ document, reported by *The Guardian*, boasted that GCHQ had "*given the NSA 36 per cent of all the raw information the British had intercepted from computers the agency was monitoring*."[93] The GCHQ documents explained "*we can now interchange 100% of GCHQ End Point Projects with NSA*." Another document quoted by *The*

---

[90] Campbell, "Revealed: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base: Snowden leaks that UK.gov suppressed," *The Register* (3 June 2014).
[91] According to Bill Woodcock, president of PCH, a non-profit internet organization that tracks and measures and documents fibre infrastructure around the world. See Esposito, Cole, Schone, and Greenwald, "Snowden docs reveal British spies snooped on YouTube and Facebook," *NBC News* (27 January 2014).
[92] MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian* (21 June 2013).
[93] Hopkins and Borger, "Exclusive - NSA pays £100m in secret funding for GCHQ," *The Guardian* (1 August 2013).

*Guardian* admits that "*NSA analysts effectively exploit GCHQ metadata for intelligence production, target development/discovery purposes. GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures.*" [94]

132. Similarly to the NSA's UPSTREAM collection programme, TEMPORA is implemented through partnerships with telecommunication companies who provide access to undersea fibre optic cables. *The Register* reported that GCHQ pays telecommunications companies tens of millions of pounds to install and maintain the optical fibre taps that feed data into TEMPORA, and to install probes into equipment belonging to other companies without their knowledge. Documents seen by *The Register* suggest that the interception of two cables passing through FLAG (Fibre optic Link Around the Globe), for example, was conducted without the knowledge of the cables' owners, with GCHQ instead installing tapping connections and "backhauling" the data to its facilities in Bude, Cornwall.[95]

133. Germany's *Suddeutsche Zeitung* newspaper published the identities of the companies providing GCHQ with access to their systems, along with their GCHQ codenames (in brackets):

    a. *BT ("Remedy"),*

    b. *Verizon Business ("Dacron"),*

    c. *Vodafone Cable ("Gerontic"),*

    d. *Global Crossing ("Pinnage"),*

    e. *Level 3 ("Little"),*

    f. *Viatel ("Vitreous"); and*

    g. *Interoute ("Streetcar").*

**MUSCULAR**

---

[94] MacAskill, Borger, Hopkins, Davies and Ball, "Mastering the internet - how GCHQ set out to spy on the world wide web," *The Guardian* (21 June 2013).
[95] Campbell, "Revealed: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base: Snowden leaks that UK.gov suppressed," *The Register* (3 June 2014).

134. NSA and GCHQ also jointly run a programme named MUSCULAR,[96] located and operated from the UK, which is designed to covertly infiltrate internet companies' infrastructure and intercept data directly as it transits to and from Google's and Yahoo's private data centres which host their "cloud" services. This programme is operated concurrently with PRISM, which allows the NSA and GCHQ to overtly access data handled and stored by Google and Yahoo, suggesting that the intelligence services are "hedging their bets" by simultaneously requesting access to data, and intercepting it directly. This programme is referred to as a "full take," "bulk access" and "high volume" operation against Yahoo and Google networks. According to one internal NSA document, reported by *The Washington Post,* tapping the Google and Yahoo data centres allows the interception of communications in real time and permits the NSA and GCHQ to take "a retrospective look at target activity."[97] One of the reasons operations like this are so concerning is the sheer amount of data, both current and historical can be shunted between companies private data centers. To operate effectively, the cloud networks that are so common, have to synchronise large volumes of information about their users. Entire email archives, full search histories going back a decade and private documents, spreadsheets financial information that is stored in the cloud are copied across to new servers to guard against data loss and system slowdowns.

135. Similarly to the operation of TEMPORA, all data is passed into a "buffer" that can hold three to five days of traffic. From this "buffer", NSA tools read the proprietary data formats that the two companies use inside their clouds. The content, which will include emails, internet searches, and pictures hosted by the companies, is then inspected and analysed before being further processed.

136. It is not known how many selectors GCHQ uses to filter the extraordinary quantity of data that is being intercepted, but one weekly report on MUSCULAR says GCHQs allow the NSA to contribute 100,000 "selectors," or search terms, to the programme, more than twice the number in use in the

[96] Gellman and Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post* (30 October 2013).
[97] Gellman and Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post* (30 October 2013).

PRISM programme.[98] An internal NSA accounting document shows that, within one 30 day stretch, NSA field collectors had processed and sent back 181,280,466 new records from the MUSCULAR programme to NSA's headquarters at Forte Meade.[99] It is not known what, if any, safeguards were put in place to protect British citizens.

**OPTIC NERVE**

137. Under the OPTIC NERVE programme, GCHQ intercepted substantial quantities of sexually explicit communications from private video conversations.[100] According to documents viewed by *The Guardian,* in one six-month period in 2008, GCHQ collected webcam imagery from more than 1.8 million Yahoo user accounts globally. Rather than collecting webcam videos in their entirety, the programme saved one image every five minutes to avoid overloading GCHQ's servers. The individuals whose communications were intercepted and analysed were not specifically named or targeted; rather, the collection constituted "unselected" material. GCHQ also reportedly applied facial recognition technology to the collected video chats.

138. From the webcam imagery harvested by this programme, documents reveal that between 3% and 11% contained "undesirable nudity". The large amount of private sexually explicit webcam imagery was noted by GCHQ but an internal guide explained to intelligence analysts that "*there is no perfect ability to censor material which may be offensive. Users who may feel uncomfortable about such material are advised not to open them.*"[101] The programme began in 2008 and was still active in 2012.

**XKEYSCORE**

139. The XKEYSCORE system is an NSA-developed "analytic framework" which enables a single search to query the previous three days worth of raw signals

[98] Gellman and Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post* (30 October 2013).
[99] Gellman and Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post* (30 October 2013).
[100] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," *The Guardian* (27 February 2014).
[101] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," *The Guardian* (27 February 2014).

intelligence, stored at 150 global sites on 700 database servers.[102] The system draws from SIGINT collected by the NSA through various interception and collection programmes, including PRISM and UPSTREAM. As a result, it indexes almost all NSA signals intelligence data sources, including e-mail addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions, including searches queried among many other types of data that flows through collection points. The tool is used widely throughout GCHQ operations; *The Guardian* reported that, for example, GCHQ used XKEYSCORE to filter and search information as part of OPTIC NERVE.[103]

140. XKEYSCORE is described by former NSA analyst Edward Snowden as a "one-stop-shop" and a "front end search engine", covering what an internal NSA document describes as "nearly everything a typical user does on the internet."[104] In an interview with German public television network ARD, Edward Snowden explains:

> *"You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information."*
>
> *…You can tag individuals… Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity."*

---

[102] NSA XKEYSCORE presentation, retrieved from *The Guardian.*
[103] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," *The Guardian* (27 February 2014).
[104] Greenwald, "XKeyscore - NSA tool collects 'nearly everything a user does on the internet'," *The Guardian* (31 July 2013).

141. One presentation[105] explained that using the system allows the intelligence analyst to attempt to answer questions such as

- "*My target speaks German but is in Pakistan – how can I find him?*" (Here the presentation also notes: "*Not possible in any other system but XKEYSCORE, nor could it be[…]").*

- "*Show me all the Microsoft Excel spread sheet containing MAC addresses coming out of Iraq so I can perform network mapping*"

- "*Show me all the encrypted word documents from Iran*"

- "*My target uses Google Maps to scope target locations – can I use this information to determine his email address? What about the web-searches – do any stand out and look suspicious?*"

## VI. THE "CULTURE OF COMPLIANCE"

142. In his statement (paras 51-54) Mr Farr emphasises the seriousness with which the intelligence services take their legal duties, and refers to a "culture of compliance" within British intelligence agencies that ensures agents faithful adherence to the relevant legal and policy framework. There are, however, serious questions about this "culture of compliance".

143. Journalist John Lanchester, upon viewing leaked GCHQ documents provided by *The Guardian* and writing in an article dated 3 October 2013, described the superficiality of legal compliance with respect to targeting under TEMPORA programme in the following terms:

> "*This process is not without supervision, of course. In order to target you via one of these "selectors" – that's the technical term – the agent of the state will have to type into a box on his or her computer screen a Miranda number, to show that the process is taking place in response to a specific request for information, and will also need to select a justification under the Human*

[105] NSA XKEYSCORE presentation, retrieved from *The Guardian.*

> *Rights Act. That last isn't too arduous, because the agent can choose the justification from a drop-down menu."*[106]

144. Indeed, documents obtained by the Guardian and described in an article dated 1 August 2013 reveal the weakness of the UK legal regime is a "'*selling point' for the Americans*."[107] GCHQ describes itself as "*less constrained by NSA's concerns about compliance*" and dedicated to exploiting "*to the full our unique selling points of geography, partnerships [and] the UK's legal regime*." In a confidential briefing, referenced in an article from *The Guardian* dated 21 June 2013, one of GCHQ's senior legal advisers noted that "*We have a light oversight regime compared with the US."* The Investigatory Powers Tribunal has "*so far always found in our favour,"* the document noted.[108]

145. GCHQ's loose adherence to legal safeguards is well illustrated by the agency's Optic Nerve programme, revealed by *The Guardian* on 28 February 2014. Optic Nerve, operated through TEMPORA, is designed to intercept and store still images derived from Yahoo webcam transmissions at five-minute intervals, on a bulk scale.[109] The programme, ostensibly authorised under the section 8(4) regime, involves the collection of "undesirable images", including "undesirable nudity." Analysts confronted by such undesirable images are advised by GCHQ:

> "*It is possible to handle and display undesireable images. There is no perfect ability to censor material which may be offensive. Users who may feel uncomfortable about such material are advised not to open them.*
>
> *You are reminded that under GCHQ's offensive material policy, the dissemination of offensive material is a disciplinary offence.*

---

[106] Lanchester, "The Snowden files - why the British public should be worried about GCHQ," *The Guardian* (3 October 2013).
[107] Hopkins and Borger, "Exclusive - NSA pays £100m in secret funding for GCHQ," *The Guardian* (1 August 2013).
[108] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world," *The Guardian* (21 June 2013).
[109] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," *The Guardian* (27 February 2014).

*Retrieval of or reference to such material should be avoided; see IB 150 for guidance on dealing with offensive material*."[110]

146. Internal GCHQ documents from 2008 acknowledge the dubious legality of Optic Nerve:

> "*It was agreed that the legalities of such a capability would be considered once it had been developed, but that the general principle applied would be that if the accuracy of the algorithm was such that it was useful to the analyst (ie, the number of spurious results was low, then it was likely to be proportionate).*
>
> *This is allowed for research purposes but at the point where the results are shown to analysts for operational use, the proportionality and legality questions must be more carefully considered*."

147. The lawfulness of activities carried out by the NSA, GCHQ's closest intelligence partner and the provider of the vast majority of signals intelligence relied upon by British intelligence services, have also been called into question on numerous occasions. Similar information is not published about GCHQ employees but it would be surprising if similar problems have not occurred in the UK.

148. For example, on 2 March 2009 the Foreign Intelligence Surveillance Court ("FISC") issued an opinion in relation to incidents of non-compliance with respect to an authorisation issued by the FISC under the "Business Records" metadata collection programme operated by the NSA. The Court noted that, in a 5 day period in April 2008, 31 NSA analysts had queried the metadata collected under the programme using 2,373 foreign telephone identifiers in contravention of the procedures ordered by the FISC.[111] Numerous subsequent incidents of non-compliance occurred in the following months. As a result, the FISC noted, "*authorisations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata*."[112] The Court remarked: "*To approve such a program, the Court must have every*

[110] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," *The Guardian* (27 February 2014).
[111] US Foreign Intelligence Surveillance Court, Docket Number BR 08-13, Order (2 March 2009), p. 9.
[112] US Foreign Intelligence Surveillance Court, Docket Number BR 08-13, Order (2 March 2009), p. 10.

*confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. The Court no longer has such confidence.*"[113]

149. In another FISC document, the Court considered the NSA's use of an "alert list" – a list of phone numbers of interest that the agency queried every day as new data was collected and stored in NSA databases. The Court had ordered that the NSA only query numbers that pertained to a "reasonable articulable suspicion" of connection with terrorism (often referred to as "RAS-approved"). As of 16 January 2009, only 1,935 of the 17,835 numbers on the alert list were RAS approved.[114]

150. An October 2011 FISC ruling, published on 21 August 2013, accused the NSA of engaging in "*systemic overcollection*" for years,[115] and committing "*longstanding and pervasive violations of the prior orders in this matter*".[116] Another FISC order lambasts the NSA's "*apparent widespread disregard of [Fisa court imposed] restrictions.*"[117]

151. Not only has the NSA displayed an institutional disregard for compliance with statutory and court-ordered legal requirements, it has also witnessed numerous incidents of "intentional and wilful misuse of surveillance authorities" by intelligence agents. Twelve such incidences were described in a letter from the NSA to Senator Charles Grassley, including:

    *a.* Two agents who performed SIGINT queries on the telephone number of their girlfriends;

    *b.* An agent who tasked six email addresses belonging to a former girlfriend;

---

[113] US Foreign Intelligence Surveillance Court, Docket Number BR 08-13, Order (2 March 2009).
[114] US Foreign Intelligence Surveillance Court, Docket Number BR 08-13, Declaration of Lietenant General Keith B Alexander, United States Army, Director of the National Security Agency (13 Febaruy 2009), p. 8.
[115] US Foreign Intelligence Surveillance Court, Docket Number PR/TT REDACTED, Memorandum Opinion, date redacted, p. 20.
[116] US Foreign Intelligence Surveillance Court, Docket Number PR/TT REDACTED, Memorandum Opinion, date redacted, p. 115.
[117] US Foreign Intelligence Surveillance Court, Docket Number PR/TT REDACTED, Order, date redacted.

*c.* An agent who tasked a foreign telephone number she had discovered in her husbands cellular telephone;

*d.* An agent who tasked nine telephone numbers of female foreign nationals without a valid foreign intelligence purpose; and another who tasked the numbers of three female foreign nationals.[118]

152. These examples were mostly self-reported (during periodic polygraph tests), so thus are likely representative of far more pervasive activity that has gone undetected. They are also likely to be representative of some of the types of non-compliance perpetrated by GCHQ analysts. The very nature of GCHQ intelligence analyst's work – having sustained access to such extensive amounts and invasive types of intelligence, – renders inevitable the likelihood that such powers will be abused. Human nature being what it is, if individuals are given access to a vast amount of highly private information about virtually everyone in the country, and can, undetected, obtain information about partners, ex-partners, friends, colleagues, it is all but inevitable that, on occasions, and even just out of curiosity, they may check the communications or web searches of others even if it is not necessary to do so.

153. A Signals Intelligence Directorate Oversight and Compliance Memorandum dated 3 May 2012 and published by *The Washington Post* on 16 August 2013 attests to the occurrence of 2,776 compliance incidents related to errors in collection, dissemination, retention and unauthorised access within NSA from the second quarter of 2011 to the first quarter of 2012.[119] In addition, 3,032 files containing call detail records collected under the NSA's business records metadata programme had been retained in violation of the five-year retention period established for the programme.[120]

154. The number of compliance incidents reported by the NSA does not necessarily reflect actual number of incidents of error or abuse within the

---

[118] Letter from the NSA to Senator Charles E. Grassley (11 September 2013).
[119] SID Oversight and Compliance Memorandum, *NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – EXECUTIVE SUMMARY* (3 May 2012), p. 2.
[120] SID Oversight and Compliance Memorandum, *NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – EXECUTIVE SUMMARY* (3 May 2012), p. 11.

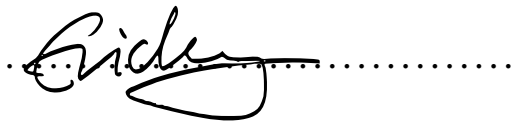
agency. For example, *The Washington Post* reported on 16 August 2013 that leaked NSA documents reveal that in one instance, an NSA analyst intercepted "a "*large number of calls placed from Washington when a programming error confused the U.S. area code 202 for 20, the international duality code for Egypt […].*" According to a "quality assurance" review, the incident was not reported to the NSA's oversight staff.[121]

155. It is likely that such incidents go unreported because, at the NSA, compliance merely requires an analyst to select from a number of pre-determined justifications for tasking and querying signals intelligence. In a screenshot from the XKEYSCORE programme, published by *The Guardian* on 31 July 2013, analysts are asked to "Build Targeting Request" by selecting from drop-down pre-filled lists the "Foreign Intel Purpose", "Foreign Factor" (from which the analyst might choose "The person has stated that he is located outside the US", or "Phone number is registered in a country other than the US", for example), and the start and end date for the targeting. That is all that is required to access the intelligence collected through the programme.

156. Above, I have given US examples because the nature of the errors reported to the Commissioners are not disclosed publicly. But there is no reason to think that the type and scope of misconduct committed in the US would be different from that which occurs in the UK.

**Statement of Truth**

**I believe that the facts set out in this witness statement are true.**



**Eric King**

**8th June 2014**

[121] Gellman, "NSA broke privacy rules thousands of times per year, audit finds," *The Washington Post* (15 August 2013).