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

BETWEEN:

(1) PRIVACY INTERNATIONAL
(2) BYTES FOR ALL

Claimants

-and-

SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS and OTHERS

Defendants

WITNESS STATEMENT OF ERIC KING

I, ERIC KING, Deputy Director of Privacy International of 62 Britton Street, London EC1M 5UY SAY AS FOLLOWS:

1. I remain the Deputy Director of Privacy International. I am authorised to make this statement on behalf of Privacy International and Bytes for All.

2. The purpose of this witness statement is to provide information and evidence to assist the Tribunal in deciding whether any interception of the Claimants' communications is justified as necessary and proportionate. I also provide an update as to the material that is now in the public domain about the TEMPORA programme and other bulk interception activities by the UK Security and Intelligence Agencies.

3. Much of my first witness statement is also relevant to these issues. This statement should be read alongside my first statement, the contents of which are not repeated.

Mass surveillance

4. Mass surveillance programmes like PRISM, UPSTREAM collection and TEMPORA run by British and American intelligence agencies are now premised on one fundamental objective – to "collect it all," "exploit it all", "process it all" and "know it all", where "all" represents everyone's private telephone, email and internet communications.[1] The logic is that everyone's communications and communications data must be intercepted (even those about whom these is no suspicion or reason to subject to surveillance) in order to find the 'needles in the haystack'.

5. The volume of data collected is enormous and so most of the material cannot be reviewed by a person. Instead, intelligence agencies mine the data for correlations and patterns, suspicious words or phrases, relationships or connections using powerful computers. Even when data does not immediately yield interesting or useful intelligence, agencies seek to store as much of it as possible, with the intention of returning to it and applying retrospective analyses at some point in the future when it might be newly interesting or useful. The objective is to strive to build an ever-larger haystack, in order to improve both the intelligence agencies' current and future capacity to find needles. This mind-set, coupled with dramatically decreasing costs of data storage and exponentially increasing volumes of communications, has created what some at NSA call "the golden age of SIGINT."[2]

6. It is important to recognise that the capabilities now enjoyed by the security and intelligence agencies offer them the ability to achieve an unprecedented degree of information about individuals that could never previously have been collected. Almost all communications are now transmitted electronically, with email and mobile phone calls having replaced traditional communications like post as the primary means of communication a long time ago. The effort and risk of a bulk postal interception operation and to pay people to read everyone's mail for key words and topics of interest would, in practice, make that an impossible exercise. Such information could never previously have been collected and mined. Similarly, a database of continuously updated location information about everyone's mobile telephones provides a level of detail about individual activities equivalent to giving

---

1 Greenwald, "No Place to Hide", Macmillan, (2014) p 97

2 Risen and Poitras, "N.S.A. Report Outlined Goals for More Power", *The New York Times*, (22nd November 2013) available at: http://www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html

everyone with a mobile telephone a tracking device. Again that is something that would have been impossible to do a decade ago. These are new capabilities, enabled by modern technology, permitting more intrusive and more invasive surveillance than has previously been feasible.

7. As UN Special Rappouter for the promotion of human rights while countering terrorism Ben Emmerson QC stated in his 2014 report:

"The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether. By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis.

[…]

The technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17.

The scale of of TEMPORA interception

8. Operating primarily out of Bude in Cornwall, the GCHQ mass surveillance programme TEMPORA includes the first "full take" internet fibre-optic interception site in the world and claims to provide the single "biggest internet access" enjoyed by any intelligence agency worldwide[3].

9. Designed to act as an "Internet Buffer" that "slows down a large chunk of Internet data",[4] TEMPORA's goal is to allow intelligence agencies "retrospective analysis" of any communication they wish to examine that flows through the internet past their sensors. By deploying a high speed filtering and exploitation system called

[3] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

[4] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

"XKEYSCORE" the agency is able to ingest, search and analyse exceptionally large quantities of private communications. When access to the GCHQ programme was first provided to NSA, it was described as "World's Largest" which "contains more data than all other XKEYSCORE'S combined" [5] and "more than 10 times larger than the next biggest XKEYSCORE."[6]

10. Indeed, the vast number of private communications being intercepted requires a special kind of processing known as "Massive Volume Reduction" to make sense of the collected private communications. In 2009 internal GCHQ documents stated "this massive site uses over 1000 machines to process and make available to analysts more than 40 billion piece of content a day."[7]

11. The Guardian reported TEMPORA potentially gives GCHQ access to 21 petabytes of data a day. A petabyte is approximately 1,000 terabytes (which is in turn 1000 gigabytes). To put this in perspective, this is the equivalent of sending all the information in all the books in the British Library 192 times every 24 hours. In a presentation to GCHQ analysts, it was put simply that "[t]his is a massive amount of data!"[8]

The increase in TEMPORA interception

12. Although Britain has a long history of gaining access to communications via the interception of undersea cables, the volume of communications that is being intercepted and analysed under TEMPORA is orders of magnitude greater than GCHQ's previous capacity. Indeed, according to internal GCHQ documents since 2009 there has been a 7,000% increase in the information obtained from fibre optic undersea cables through the use of TEMPORA.[9]

---

5 "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

6 "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

7 "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

8 MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications" *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

9 Hopkins and Borger. "NSA pays £100m in secret funding for GCHQ", *The Guardian"* (1st August 2013, available at: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

13. This has been achieved under the ambit of a GCHQ programme named "Mastering the Internet," which saw GCHQ receive new technologies and funds from the NSA, including £15.5 million towards redevelopments at GCHQ Bude,[10] to achieve TEMPORA's extraordinary expansion in capability. Some of these funds have been used to pay telelcommunications companies for their co-operation including £6 million paid to Cable and Wireless in 2009.[11]

14. As of May 2012, there are TEMPORA capabilities at multiple processing centres, each of which intercept different undersea cables based within the UK and overseas. In the descriptors below, the numbers refer to the interception capacity in gigabytes of the centre.

    a. CPC TEMPORA 16 x 10g[12] - Central Process Centre, GCHQ Cheltenham

    b. RPC1 TEMPORA 23 x 10g[13] - Remote Processing Centre,[14] GCHQ Bude

    c. OPC1 TEMPORA 7 x 10g[15] - Overseas Processing Centre, Oman

    d. OPC2 TEMPORA (planned)[16] – location unknown.

15. In 2011 "more than 39bn events in a 24-hour period" were recorded through TEMPORA.[17]

---

[10] Hopkins and Borger. "NSA pays £100m in secret funding for GCHQ", *The Guardian"* (1st August 2013, available at: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

[11] Obermaier, Moltke, Poitras and Strozyk, "Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts", *Süddeutsche Zeitung*, (Nov 25, 2014) available at: http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsidiary-cable

[12] GCHQ Wiki entry on TEMPORA, *Der Spiegel*, available at http://www.spiegel.de/media/media-34103.pdf

[13] GCHQ Wiki entry on TEMPORA, *Der Spiegel*, available at http://www.spiegel.de/media/media-34103.pdf

[14] Campbell, "Interception Capabilities 2014", *Der Spiegel*, available at: http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf

[15] GCHQ Wiki entry on TEMPORA, *Der Spiegel*, available at http://www.spiegel.de/media/media-34103.pdf

[16] Campbell, "GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base", *The Register*, (3 June 2014). Available at: http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middle east_internet_spy_base/?page=2

[17] MaacAskill, Borger, Hopkins, Davies and Ball, "Mastering the internet: how GCHQ set out to spy on the world wide web," *The Guardian,* (21st June 2013) http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

16. The scale of this operation is several orders of magnitude than the far more targeted operation found to be unlawful in *Liberty v UK*. That operation involved the interception of a single microwave link, only carrying calls between the United Kingdom and the Republic of Ireland. It is unlikely that any internal telephone calls would have been collected and the use of the internet was then in its infancy. In *Weber & Saravia v Germany*, the satellite interception operation only covered international telephone calls made by satellite link. Land line international and domestic telephone calls were not covered. Only a very small percentage of communications were subject to intercept.

Automatic processing and analysis

17. With such vast quantities of information being intercepted under TEMPORA, it is not possible to immediately determine what will be of interest to GCHQ, nor is it possible to immediately filter out the private communications of perfectly innocent people who are not suspected of anything. Instead, GCHQ treats every piece of information intercepted as potentially suspicious, pieces it back together, and subjects it to intrusive processing, filtering, and analysis.

18. In this way, the private communications of everyone who is caught up in this net are subjected to experimentation in an attempt to determine how suspicious a certain person, about who nothing previous was known, may or may not be. Emails between close friends, phone calls between family members, internet searches about medical conditions, the browsing of news websites for political views will all be examined and graded. In practical terms, an operation such as TEMPORA is equivalent to a law requiring everyone to send a cc: of all their emails to GCHQ, and any other intelligence organisation operating a similar operation. Equally, when browsing the internet, the effect is similar to GCHQ having a camera pointed at the screen, recording each page that onlt the person views, and how long they spend there.

19. The automatic analysis can be thought of as the creation of large lists, with information and individuals ranked by how suspicious they are based on the criteria GCHQ has determined are important.

20. People are categorised and grouped together based on possible associations. How many times their mobile phones were identified as being in the same proximity for a

certain period of time or the cross-correlation of address books with Facebook friends with email correspondence. In this way, links are established between people, places and topics.

21. Even when using the system to try and track a specific person, huge numbers of "potential leads" are generated[18] from TEMPORAs buffer, so even after analysis and processing "the analyst is often left with too many identifiers of possible interest."[19] In attempts to address this problem, everyone's whose communications placed them onto the "potential leads" list is subjected to what one NSA slide referred to as "Bulk Lead Triage via Behavior Analytics."[20]

22. One such further analytic process, GHOSTMACHINE, which was used extensively throughout the Olympics shows criteria assessing the "potential leads" on whether a person had ever phoned someone who was already on a GCHQ list, and their name found in an electronic address book of anyone on a GCHQ list, and whether that person had ever been to France.

23. This kind of invasive analysis is all done before a human has ever looked, read or listed to anything, and before the data is stored for any length of time.

Human analysis

24. It is not by accident that so much analysis is done automatically. One strategy document set out the 2012 – 2016 goals of the NSA to "[r]evolutionize analysis – fundamentally shift our analytic approach from a production to a discovery bias" and to achieve this "[t]hrough advanced tradecraft and automation."

25. With so much of the intrusive analysis automatically done by various processing and analytic frameworks, the task of the human analyst has changed considerably. Now human analysts simply have to search through the pre-filtered, processed and analysed information for what it is they want. This tends to make the invasion of

[18] "GHOSTMACHINE: Identifier lead triage with ECHOBASE", *The Intercept,* available at: https://firstlook.org/theintercept/document/2014/04/30/ghostmachine-identifier-lead-triage-echobase/
[19] "GHOSTMACHINE: Identifier lead triage with ECHOBASE", *The Intercept,* available at: https://firstlook.org/theintercept/document/2014/04/30/ghostmachine-identifier-lead-triage-echobase/
[20] "GHOSTMACHINE: Identifier lead triage with ECHOBASE", *The Intercept,* available at: https://firstlook.org/theintercept/document/2014/04/30/ghostmachine-identifier-lead-triage-echobase/

privacy more not less serious because of the power of the automated tools. The automated tools, by sifting over vast amounts of data, are able to build detailed pictures about the lives of individuals which no human analyst could do.

26. According to Edward Snowden, using tools like XKEYSCORE means "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."[21]

Authorisations required for GCHQ analysts

27. Under the 8(4) certificated warrant regime a person or premises does not need to be specifically targeted. An 8(4) warrant can authorise the collection of an entire undersea fibre optic cable, and permit the examination of all the communications flowing through the cable, so long as it meets a statutory purpose such national security, or the economic wellbeing of the United Kingdom.

28. It was this certificated warrant scheme that was put to use in 2009 to authorise the first deployment of TEMPORA. While the full terms of such warrants have not been published some information is known:

    a. It has been reported that there are 10 basic certificates, including a "global" one that covers GCHQ's key bases in Bude, Menwith Hill and Cyprus.[22]

    b. These certificates do not name specific individuals or premises. Internal GCHQ documents state they "cannot list numbers or individuals as this would be an infinite list which we couldn't manage."[23]

    c. Instead "[t]he certificate is issued with the warrant and signed by the Secretary of State and sets out [the] class of work we can do under it" which

[21] Interview with Edward Snowden, *Tagesschau*, Available at: https://www.tagesschau.de/snowden-interview-englisch100.pdf

[22] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

[23] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

is designed to "cover the entire range of GCHQ's intelligence production."[24] Currently these certificates include authorisations for GCHQ to collect information about the "political intentions of foreign powers", terrorism, proliferation, mercenaries and private military companies, and serious financial fraud.

d. Certificates are re-issued every six months.[25]

29. As long as a GCHQ analyst believes the targeting of an individual falls within the scope of these broad certificates, no additional authorisations, certificates or warrants are required.

30. Internal GCHQ documents acknowledge that British law "creates flexibility"; a senior GCHQ legal advisor has boasted that "we have a light oversight regime compared with the US."[26]

31. Internal training documents show that GCHQ analysts are presented with simple interfaces to query the large volume of private communications they have intercepted. To look up all the historic emails of a target's email addresses, analysts simply have to select a start and end date, and type in an email address or subject of the email. This search will return every email address GCHQ (and possibly some Five Eyes partners) has ever collected and stored that match the search terms.

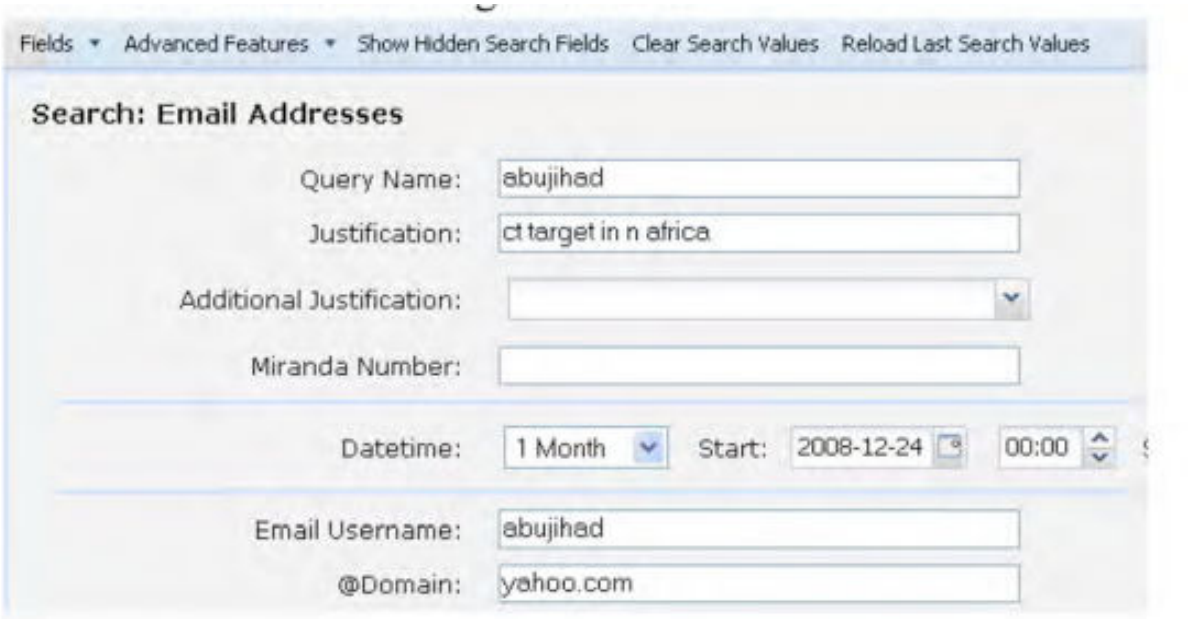
---

[24] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

[25] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

[26] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

32. For this search to be "legal", additional information is required. Analysts are presented with two boxes to fill in and the option to select from a drop down menu.



33. As can been seen in the screenshot above,[27] the example justification is "ct target in n africa" which presumably is shorthand for "counter-terrorism target in north Africa." This kind of shorthand example is common, with other screenshots showing the justification as "aqi in iran sample" presumably referring to Al-Qaeda in Iran.[28] The target is described as "abujihad". It is regrettable that GCHQ's trainers use such crude stereotypes in their training materials which are designed to evidence the seriousness and care with which they justify serious intrusions on privacy.

34. An additional justification is required to be selected from a drop down menu. Although a full list of available justifications is not public, it is believed they refer to justifications under the Human Rights Act.[29] Finally, a Miranda number is required to be typed to record the search category the query is being made under.[30]

---

27 Greenwald, "No Place to Hide", 2014, available at: https://www.aclu.org/files/natsec/nsa/20140722/Creating%20Email%20Address%20Queries.pdf

28 Greenwald, "No Place to Hide", 2014, available at: https://www.aclu.org/files/natsec/nsa/20140722/Creating%20Email%20Address%20Queries.pdf

29 Lanchester, "The Snowden files: why the British public should be worried about GCHQ", *The Guardian,* 3rd October 2013, available at: http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester

30 Lanchester, "The Snowden files: why the British public should be worried about GCHQ", *The Guardian,* 3rd October 2013, available at: http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester

35. Once entered, no additional authorisation or review is required; the results of the search will immediately begin filling the analyst's screen.

36. There is no requirement for authorisation by the Secretary of State, still less judicial authorisation. Indeed, the requirements are less than for obtaining communications data under Part I, Chapter II of RIPA, which would require the authorisation of a senior officer and the involvement of a Single Point of Contact to ensure that the request was as narrowly targeted and proportionate as possible. None of these safeguards are present. The analyst is given a simple interface and with no more than a couple of boxes of justification can examine the communications of a particular individual, or a large number of individuals. The Tribunal is invited to compare this process to the detailed process required for obtaining a warrant against an individual present in the United Kingdom, including the preparation of a detailed written justification for the interference on privacy, and the identification of measures to mitigate the impact of the interference.

37. The inadequate nature of this process can be seen by comparison with sample Chapter II application forms, which has been previously published by the Home Office[31].

Receipt of information from the NSA.

38. The exchange of finalised intelligence reports, or 'analysed intercepted' material is just one part of intelligence liaison and exchange. The practice that affects a far greater number of individuals is the exchange of raw intercept material. Under broad FISA and EO12333 authorities the NSA operates a number of collection programs. My earlier witness statement includes references to the material known to be exchanged at paras 90 – 125.

39. A short summary of the scale of communications NSA could make available to GCHQ include:

    a. The NSA CO-TRAVELLER programme collects nearly five billion mobile phone location records a day "outpacing [NSA] ability to ingest, process and store" the data.[32]

[31] https://www.gov.uk/government/publications/chapter-ii-application-for-communications-data

b. The NSA DISHFIRE programme collects an average of 194 million text messages daily and stores stores "pretty much everything it can."[33]

c. The NSA undersea fibre optic interception programmes UPSTREAM accounts for the largest collection activity undertaken by the agency. One NSA BOUNDLESS INFORMANT slide shows that just the top five programs within UPSTREAM created 160 billion records in one month. This collection has permitted NSA Special Source Operations to collect in a single day 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[34]

The Tribunal is invited to determine whether the UK has access to any of these programs (or others of which the Respondents will be aware) and ensure that all these potential sources of data are investigated and analysed for their proportionality.

---

32 Gellman and Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," The Washington Post (4 December 2013) available at: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

33 Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," The Guardian (16 January 2014) available at: http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

34 Gellman and Soltani, "NSA collects millions of e-mail address books globally," The Washington Post (14 October 2013). Available at: http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

NCND

40. The fact that GCHQ has capability to intercept private communication from international communications cables is not a secret. Official accounts of GCHQ's predecessor GC&CS activities during the First and Second World War described the targeting of telegraph cables for exactly this.[35] The continuation of many of those arrangements between GC&CS and cable companies such as Cable and Wireless Ltd were made public by Chapman Pincher in the 1960s and confirmed by the Radcliffe Report on the D-Notice affair which stated there was "a regular collection of copies of messages transmitted by the Post Office and other cable offices with a view to the total collected being sorted and certain defined categories of them being set aside for inspection by the intelligence agents of Her Majesty's Government."

41. Since my earlier statement, further official information has come into the public domain about the TEMPORA operation. The modern day continuation of this practice has also been addressed by the ISC[36] in their report on the murder of Fusilier Lee Rigby. The report explains:

> "GCHQ also has access to communications as they move over the internet via the major internet cables. This provides the capability to intercept a small proportion of internet traffic: in theory, GCHQ can access around ***% of global internet traffic and approximately ***% of internet traffic entering or leaving the UK."
>
> […]
>
> "GCHQ can potentially access external internet communications (i.e. one or both ends outside the UK) via their intelligence capabilities. This includes their ability to access the material travelling through the fibre-optic cables carrying information to and from the UK."

---

35 Hinsley, "British Intelligence in the Second World War", Abridged Version, (1993, HMSO)

36 "Report on the intelligence relating to the murder of Fusilier Lee Rigby", *Intelligence and Security Committee of Parliament* (25 November 2014) available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20141125_ISC_Woolwich_Report%28website%29.pdf?attachauth=ANoY7cq4q_1RuQPNuSskCSW5_JtGkdv5GcY0KCCeYK1k_QfabYnqfK4oWkM06d7b9l1T2-yL4opRZP8L1UecxIDNU9YRukq0PwgCm0CxrOaybD7Oe5wrFzGrlHrWCdb_TGXGWzUDGYpZjnq96kiJND9VyX7ynjnmZ1EPf1nuVAec2_gyRKfh04BjGHqL6PjAN0D7amrFIROa85mao2H-EywBa2A-lLdiC54usARz3d8kdTyowAoHha3Twu1t3DxbVQ5ZOTY2NgXx&attredirects=0

42. This represents official confirmation of the essential and key facts of the TEMPORA operation. Lord Butler, a member of the ISC said "The ISC has helped the public by putting a description of GCHQ's capability in the public domain." Although neither Lord Butler nor the ISC have confirmed the specific codename, the key features of the intelligence operation have been publicly admitted and confirmed[37]

43. Other Governments have also confirmed the practice of their intelligence agencies to intercept international communications cables.

44. In the US, the NSA UPSTREAM program has been confirmed by the NSA Civil Liberties and Privacy Office[38] and United States Foreign Intelligence Surveillance Court opinions describing the practice have been released into the public domain[39].

45. In Germany, considerable specific detail about international cable interception operations by the BND has been presented to the public in the course of an ongoing Bundestag inquiry. Interviews with senior BND officials were held in public, and the documents leaked by Edward Snowden were relied upon in questioning them. When considering whether national security would in fact be harmed by open argument on these issues, the Tribunal is invited to consider the extent to which German oversight authorities have been able to have meaningful debate in public. Full transcripts are available online in German.[40] A rough translation into English of just one section detailing the technical act of intercepting and filtering international cables is included by way of example:

> **Sensburg:** What is your background?
> **K .:** Engineer, electrical engineering education. I began at BND doing analysis of unknown signals, since about 2000 I have been in Central Pullach doing cable evaluation. 2007-2011 in another department.

---

37 Newman, Thatcher and Blair Cabinet Secretary: Intelligence committee has 'helped' public by confirming GCHQ's internet tap 'Tempora' powers, The Bureau of Investigative Journalism, (11th Jan 2015) available at: http://www.thebureauinvestigates.com/2015/01/11/thatcher-and-blair-cabinet-secretary-intelligence-committee-has-helped-public-by-confirming-gchqs-internet-tap-tempora-powers/

38 NSA Implementation of Foreign Intelligence Surveillance Act Section 702, *NSA Director of Civil Liberties and Privacy Office*, (April 16 2014) available at: https://www.nsa.gov/public_info/_files/speeches_testimonies/NSAImplementationofFISA70216Apr2014.FINAL.pdf

39 Foreign Intelligence Surveillance Court Memorandum opinion, available at: https://www.eff.org/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf

40 Meister, Live blog from the intelligence committee of inquiry, *Netzpolitik* (13th November 2014) available at: https://netzpolitik.org/2014/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-bnd-mitarbeiter-k-l-und-p-auf-der-zeugebank/

[…]
Sensburg: Your field is cable?
K .: Yes.
Sensburg: How does it work technically? How do you filter out the mass of data?
K .: We have a search profile, a series of predetermined criteria. It is possible to sort through the data based on these criteria. For example, place, route.
Sensburg: Beginning with the tap point. For example, DE-CIX. What does that mean?
K .: You mentioned DE-CIX. This is not relevant to investigation.
Sensburg: Fiber optic cable with light pulses are discharged. Do you then filter light pulses?
K .: It is very difficult.
Sensburg: How does BND attempt the first filtering process?
K .: First extraction is to pick the range and select specific fibers within the cable.
Sensburg: What range?
K .: From location to location.
Sensburg: Can it already be decided at the node for example?
K .: From Afghanistan to Pakistan.
Sensburg: They can decide that?
K .: Yes.
Sensburg: This is then forwarded on. Where to? Pullach? Bad Aibling?
K .: Depends on the place. If possible, there is already a second possible selection at the attack point.
Sensburg: Is it a computer algorithm that selects data?
K .: Yes.
Sensburg: The software decides what is needed and what is not?
K .: At the point, yes.
Sensburg: These are still large amount of data. Will it be buffered?
K .: Technical conditional caching at the front, few milliseconds, but no intervention,
[…]
Sensburg: How much data is estimated to come in at Pullach? 500 million traffic data or 20 messages a day?
K .: Selected content data after application of the search criteria, according to relevance and its necessity. That is already an order of magnitude. 500 million could only be metadata or factual data.

Statement of Truth

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

Eric King

19 January 2015