On Behalf Of: The Applicants
Name: Ian Brown
Number: First
Exhibit: IB1
Date: 27 September 2013

Application No: 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

B E T W E E N :

(1) BIG BROTHER WATCH;
(2) OPEN RIGHTS GROUP;
(3) ENGLISH PEN; and
(4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

WITNESS STATEMENT OF
DR IAN BROWN

I, Doctor Ian Brown, of **Oxford Internet Institute, University of Oxford, 1 St. Giles', Oxford OX1 3JS, United Kingdom**, will say as follows:

INTRODUCTION

1. I am a Senior Research Fellow at the Oxford Internet Institute at the University of Oxford and Associate Director of its Cyber Security Centre. I make this statement in support of the application brought by the Applicants and in order to assist the Court with matters within my expertise. Where the contents of this statement are within my knowledge, I confirm that they are true; where they are not, I have identified the source of the relevant information, and I confirm that they are true to the best of my knowledge and belief.

2. I am an ACM (Association for Computing Machinery) Distinguished Scientist and a BCS (British Computer Society Chartered Institute) Chartered Fellow. I am also a member of the UK Information Commissioner's Technology Reference Panel. I have consulted for the US Department of Homeland Security, the United Nations Office on Drugs and Crime, Council of Europe, the OECD, JP Morgan, the BBC, the European Commission, the British Government's Cabinet Office and other major regulators and corporations. I am an adviser to Open Rights Group and have acted as a trustee and adviser to a number of other non-governmental organisations. I have particular expertise in the fields of Internet technologies, cyber security, surveillance and regulation. My detailed academic curriculum vitae is available should it be requested.

3. In this statement I briefly address the following matters:

   3.1. The growth of Internet surveillance in the UK;

   3.2. The recent disclosures in the Guardian newspaper regarding the UK Government's Internet surveillance activities and the subsequent UK Government response;

   3.3. How the disclosed programmes are likely to operate;

   3.4. The legal basis for the programmes under UK law; and

   3.5. Brief commentary on the significance of this information.

4. The recent disclosures of information have also concerned programmes of the United States' National Security Agency ("**NSA**"). I understand that Cindy Cohn of the Electronic Frontier Foundation will address these in detail in a separate witness statement. However, I comment briefly on them below as UK cooperation with the US programmes is also relevant to the issues above.

5. There is now produced and shown to me a paginated bundle of true copy documents marked "IB1". All references to documents in this statement are to Bundle IB1 unless otherwise stated, in the form [**IB1/Tab/Page**].

INTERNET SURVEILLANCE IN THE UK

6. Internet surveillance in the UK is primarily carried out by Government Communications Headquarters (GCHQ). GCHQ produces signals intelligence or 'sigint' for the UK Government. Its roots extend to before the first world war, when predecessor organisations intercepted German communications. The then Government Code and Cypher School's code-breaking played a highly significant role in the outcome of the second world war. Thereafter, and with the advent of the cold war, GCHQ was increasingly important in supplying secret information to successive governments. With the advent of personal computing and the Internet, the role of GCHQ and the scope of its activities has continued to expand.

7. Over the last 20 years, the Internet has developed from a specialist network of academic researchers into a mainstream communications mechanism. In 2013, 83% of British households (21 million) had Internet access, according to the UK Government's Office for National Statistics. Alongside the development in communications technology that has driven the growth of the Internet, we continue to see exponential increases in computing capability and data storage capacity. Processing power has doubled roughly every two years, increasing approximately one million-fold since 1965. Bandwidth and storage capacity are growing even faster.

8. With greater Internet use has come a greater appetite on behalf of policing and intelligence agencies to put Internet users under surveillance. New surveillance technologies exploiting these capabilities include "bugs" and tracing technologies that can access the geographical position of mobile phones and act as a remote listening device; and hard-to-detect (even with anti-virus tools) "spyware," surreptitiously installed on a suspect's PC by the authorities, that can remotely and secretly monitor a suspect's online activities, passwords and e-mail, and even the PC's camera and microphone. Such surveillance technology is, by its nature, relatively targeted in its scope. However, surveillance technologies have also permitted GCHQ to monitor, screen and analyse, in a much less targeted, indeed pervasive manner, records of billions of telephone and e-mail communications. There has been a commensurate expansion in "dataveillance": the monitoring of the "data trails" left by individuals in numerous transactions, through access to communications and other databases containing such trails. It is now clear that both email content and metadata have been surveilled in this manner.

9. In the words of Professor Edward Felten, the first Chief Technologist at the US Federal Trade Commission, metadata can often be a "*proxy for content*". I exhibit, with his permission, a copy of his Declaration in ongoing litigation brought in the US by the American Civil Liberties Union (ACLU) in relation to some of the recent press disclosures as Exhibit **IB1/1/pp.543-577**. In this document he provides the example of calls to support hotlines for victims of domestic violence and rape, people considering suicide, addictions etc.; and of text donations to particular causes. He states:

> "46. Although it is difficult to summarize the sensitive information that telephony metadata about a single person can reveal, suffice it to say that it can expose an extraordinary amount about our habits and our associations. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations."

10. He also correctly observes that aggregated metadata is even more revealing, stating as follows:

> "48. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a social graph. By building a social graph that maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group's membership, donors, political supporters, confidential sources, and so on. Analysis of the metadata belonging to these individual callers, by moving one "hop" further out, could help to classify each one, eventually yielding a detailed breakdown of the organization's associational relationships…
>
> …52. Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.
>
> 53. Likewise, although metadata revealing a single telephone call to a bookie may suggest that a surveillance target is placing a bet, analysis of metadata over time could reveal that the target has a gambling problem, particularly if the call records also reveal a number of calls made to payday loan services."

11. He also points to mass surveillance – so called "big data" – as heralding even more intrusive surveillance. He observes, and I agree, that "*the power of metadata analysis and its potential impact upon the privacy of individuals increases with the scale of the data collected*". He concludes as follows:

> "64. The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of

days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals."

12. Professor Felten describes the process of metadata analysis as follows:

> "22…the structured nature of metadata makes it very easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances over the past 35 years in computing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyze personal communications, including metadata.
> 23. Innovations in electronic storage today permit us to maintain, cheaply and efficiently, vast amounts of data. The ability to preserve data on this scale is, by itself, an unprecedented development—making possible the maintenance of a digital history that was not previously within the easy reach of any individual, corporation, or government.
> 24. This newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing."

13. He provides an example based on commercially available analysis software named "Pen-Link" and IBM's Analyst's Notebook:

> "27…Pen-Link can perform automated "call pattern analysis," which "automatically identifies instances where particular sequences of calls occur, when they occur, how often they occur, and between which numbers and names." As the company notes in its own marketing materials, this feature "would help the analyst determine how many times Joe paged Steve, then Steve called Barbara, then Steve called Joe back."

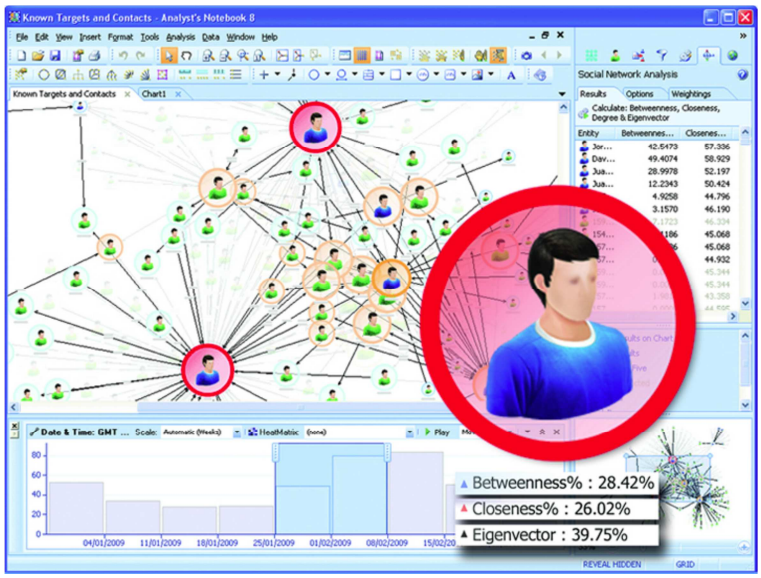


Figure 1: Screenshot of IBM's Analyst Notebook.

14. Professor Felten applies these observations to an organisation such as the ACLU:

> "55. With an organization such as the ACLU, aggregated metadata can reveal sensitive information about the internal workings of the organization and about its external associations and affiliations. The ACLU's metadata trail reflects its relationships with its clients, its legislative contacts, its members, and the prospective whistleblowers who call the organization. Second-order analysis of the telephony metadata of the ACLU's contacts would then reveal even greater details about each of those contacts. For example, if a government employee suddenly begins contacting phone numbers associated with a number of news organizations and then the ACLU and then, perhaps, a criminal defense lawyer, that person's identity as a prospective whistleblower could be surmised. Or, if the government studied the calling habits of the ACLU's members, it could assemble a detailed profile of the sorts of individuals who support the ACLU's mission…
> …57. Metadata analysis could even expose litigation strategies of the plaintiffs. Review of the ACLU's telephony metadata might reveal, for example, that lawyers of the organization contacted, for example, an unusually high number of individuals registered as sex offenders in a particular state; or a seemingly random sample of parents of students of color in a racially segregated school district; or individuals associated with a protest movement in a particular city or region."

In my opinion, these observations are equally applicable to the Applicants in these proceedings, given their work in protecting civil liberties and doing so, in many cases, on behalf of anonymous persons.

15. The recent disclosures give us a much greater understanding of the extent of GCHQ's Internet surveillance programmes. Their scale and scope has taken many experts by surprise. The targets of the programmes include foreign governments, even those allied with the US/UK. However, we still do not know which citizens have come under

surveillance and for what reasons. That underlines the importance of ensuring that known practices and systems are proportionate and in accordance with the law, which I understand to be the purpose of the applicants' complaint.

16. Before the Guardian revelations, many experts thought that the continued dramatic growth in levels of Internet traffic would outstrip the capacity of signals intelligence agencies to monitor this data flood. We now know that NSA and GCHQ have developed technology that is able to record and filter through very large volumes of traffic; there is no technological reason why they should not be able to continue to do this.

RECENT DISCLOSURES REGARDING UK INTERNET SURVEILLANCE

17. There have been a large number of recent disclosures of UK and US Internet surveillance programmes in the media, the vast majority of which arose as a result of leaks by former Booz Allen Hamilton employee, Edward Snowden. I understand these disclosures form the basis of the applicants' main complaints in these proceedings. I set out a brief timeline of the disclosures below:

6 June 2013 – Order of the US Foreign Intelligence Surveillance Court (FISC) requiring Verizon Corporation to hand over metadata from US citizens' phone calls ("**IB1/2/pp.578-587**")

6 June 2013 – Details of NSA PRISM programme, alleging that NSA gained direct access to major US Internet companies' servers. ("**IB1/2/pp.594-600**")

7 June 2013 – President Obama Orders US to draw up overseas target list for cyber-attacks. ("**IB1/2/pp.601-605**")

8 June 2013 – 'Boundless Informant': NSA tool to summarise global surveillance data is disclosed. ("**IB1/2/pp.606-618**")

9 June 2013 – Edward Snowden reveals his identity as source of leaks. ("**IB1/2/pp.619-625**")

13 June 2013 – NSA hacking of civilian computer networks in Hong Kong and mainland China. ("**IB1/2/pp.626-629**")

16 June 2013 – NSA and UK (Government Communications Headquarters (GCHQ)) monitoring foreign diplomats. ("**IB1/2/pp.630-634**")

19 June 2013 – Project Chess, by which Skype permits access to the NSA. ("**IB1/2/pp.635-638**")

20 June 2013 – FISC documents detailing NSA arrangements for warrantless access to US data. ("**IB1/2/pp.639-657**")

21 June 2013 – GCHQ Tempora programme, tapping into fibre-optic cables and storing data. ("**IB1/2/pp.658-678**")

27 June 2013 – NSA programmes for 'harvesting' online user metadata revealed, including how GCHQ-collected metadata is transferred to NSA. ("**IB1/2/pp.679-681**")

29 June 2013 – US bugging of EU offices in New York, Washington DC and Brussels, and European Government embassies. ("**IB1/2/pp.682-683**")

30 June 2013 – NSA surveillance of 500 million data connections in Germany every month. ("**IB1/2/pp.684-685**")

6 July 2013 – US using 'Fairview' programme of foreign telecoms' partnerships with US telecoms to gain access to Internet and telephone data of foreign citizens. ("**IB1/2/pp.686-690; IB1/2/pp.693-696**")

8 July 2013 – Australian monitoring stations aiding in NSA collection of data. ("**IB1/2/pp.691-692**")

10 July 2013 – Further details of NSA 'Upstream' programme, tapping fibre-optic cables. ("**IB1/2/pp.697-701**")

20 July 2013 – Germany's Federal Intelligence Service contributing to NSA's data collection network. ("**IB1/2/p.702**")

31 July 2013 – Xkeyscore NSA data collection tool, using 500 servers around the world. ("**IB1/2/pp.703-713**")

1 August 2013 – NSA paid GCHQ c.$155 million between 2010 and 2013. ("**IB1/2/pp.714-718**")

2 August 2013 – GCHQ provided with direct access to seven telecom companies' fibre optic cable networks (including BT, Vodafone and Verizon). GCHQ pays for compliance costs. ("**IB1/2/pp.719-736**")

9 August 2013 – NSA changes to data minimisation rules may permit viewing of US citizens' data without a warrant. ("**IB1/2/pp.737-741**")

16 August 2013 – NSA violations of US law/internal rules. ("**IB1/2/pp.742-743**")

21 August 2013 – NSA declassifies three secret court opinions showing widespread surveillance of US citizens not connected to terrorism. ("**IB1/2/pp.749-752**")

23 August 2013 – GCHQ station in the Middle East collecting information from fibre optic cables. ("**IB1/2/pp.753-755**")

30 August 2013 – NSA spending hundreds of millions of dollars paying private companies for access to fibre optic hubs. ("**IB1/2/pp.756-757**")

30 August 2013 – details of 231 cyber-attacks carried out by the US in 2011. ("**IB1/2/pp.758-763**")

31 August 2013 – NSA carried out surveillance on Al-Jazeera. ("**IB1/2/p.766**")

1 September 2013 – NSA carried out surveillance of Brazilian and Mexican presidents. ("**IB1/2/pp.767-775**")

5 September 2013 – NSA and GCHQ successfully broke through a number of encryption methods in 2010. ("**IB1/2/pp.776-806**")

7 September 2013 – NSA can spy on smartphone data, including emails, contacts, notes and location. ("**IB1/2/p.807**")

9 September 2013 – NSA surveillance of private computer networks belonging to Google, Petrobras, French Foreign Ministry and SWIFT, contradicting earlier claims the NSA did not engage in corporate espionage. ("**IB1/2/pp.808-811**")

11 September 2013 – NSA shares data with Israel. Full memorandum of understanding published. ("**IB1/2/pp.812-822**")

16 September 2013 – Financial networks monitored by NSA programme, including VISA and the SWIFT network, violating a 2010 agreement with the EU. ("**IB1/2/pp.823-825**")

18. The most significant of these disclosures concerned the UK's Tempora programme, the NSA's PRISM programme, offensive operations, and cracking cryptographic protection systems through technical and 'HUMINT' means.

STATEMENTS BY THE UK GOVERNMENT

19. The UK government and Parliament's response to these disclosures has been circumspect. On 7 June 2013, the Intelligence and Security Committee (ISC) of Parliament issued a short statement indicating that it was investigating the allegations regarding UK use of the NSA's PRISM programme (at that time, the details of the Tempora programme had not been disclosed). Subsequently, on 10 June 2013, the Foreign Secretary, William Hague, made a statement to Parliament ("**IB1/3/pp.826-830**") in which he addressed the disclosures. He asserted the propriety of GCHQ's activities and the warranting process, but without specifying how that process had operated nor how oversight mechanisms had operated at the time.

20. On 1 July 2013 the ISC postponed a planned public hearing with the intelligence agencies until after the summer recess; but in the meantime, on 17 July 2013, the Chairman of the committee, Sir Malcolm Rifkind MP, issued a three page statement ("**IB1/3/pp.831-833**"), reporting on an ISC investigation into the allegations regarding PRISM. The investigation absolved GCHQ of the allegation that it had circumvented statutory mechanisms by using PRISM, on the evidence that it had seen. However, it did

not say how the mechanisms had operated and appeared to acknowledge that the regulatory framework was lacking, leading to the promulgation of secret policies by GCHQ:

> "7. 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..."

The ISC indicated that further consideration would be given to these issues. In a press briefing for the report (see *Inquiry into snooping laws as committee clears GCHQ,* Guardian, 18 July 2013 ("**IB1/3/pp.834-836**")), the Chair of the ISC acknowledged that the ISC's investigation had only focused on intelligence that GCHQ had specifically requested from the US on particular warranted suspect individuals. It did not therefore cover whether PRISM data was being shared with the UK through other means, such as pursuant to broader generic warrants, or the provision of unsolicited information from the US to the UK. Nor did the inquiry cover communications *metadata* obtained through PRISM: it only looked at the sharing of *content* information.

21. Since that time, the disclosures have continued, most notably those of 21 June 2013 regarding the Tempora programme, but with little further official comment. It has been reported that on 20 July 2013 the Guardian newspaper destroyed computer hardware containing GCHQ files at the request of the UK Government ("**IB1/2/pp.744-748**"). Subsequently, in a written statement to the High Court regarding the detention of the partner of one of the Guardian journalists, Britain's Deputy National Security Adviser for Intelligence, Security and Resilience, Oliver Robbins, stated that "*real damage has in fact already been done to UK national security by media revelations*" ("**IB1/2/p.764**"). But he did not substantiate this claim further.

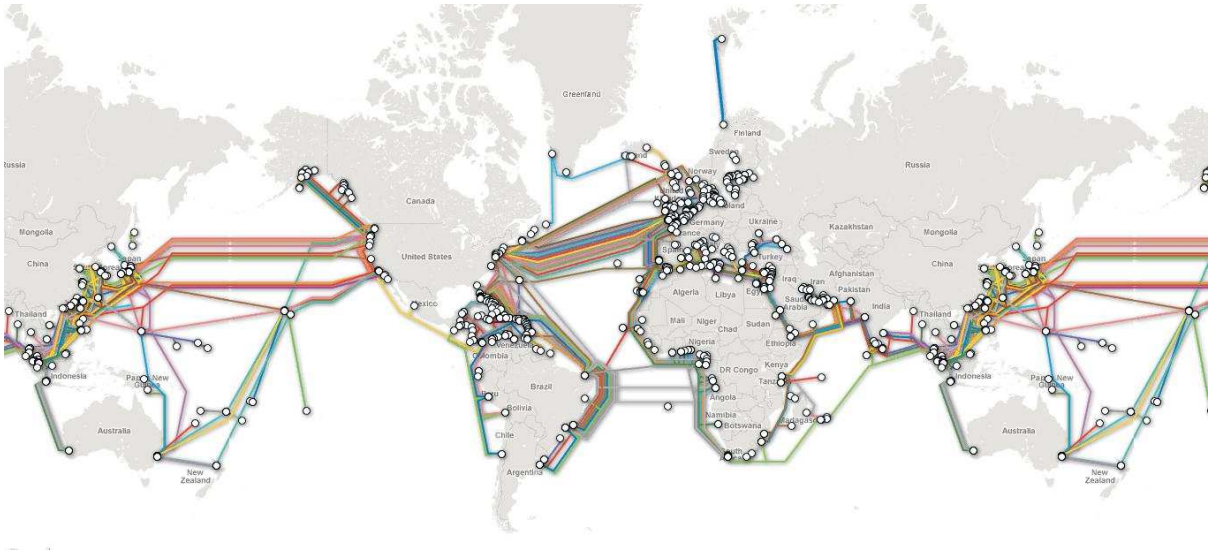
THE OPERATION OF THE PROGRAMMES

Tempora Programme

22. The Guardian newspaper's report of 21 June 2013 disclosed that GCHQ had placed data interceptors on fibre-optic cables conveying Internet data in and out of the UK. These UK-based fibre optic cables include transatlantic cables between the US and Europe. It is believed that interceptors have been placed on at least 200 "wavelengths" (data channels) carried by fibre optic cables, near to the points where they come ashore. This appears to have been done with the secret co-operation of the companies that

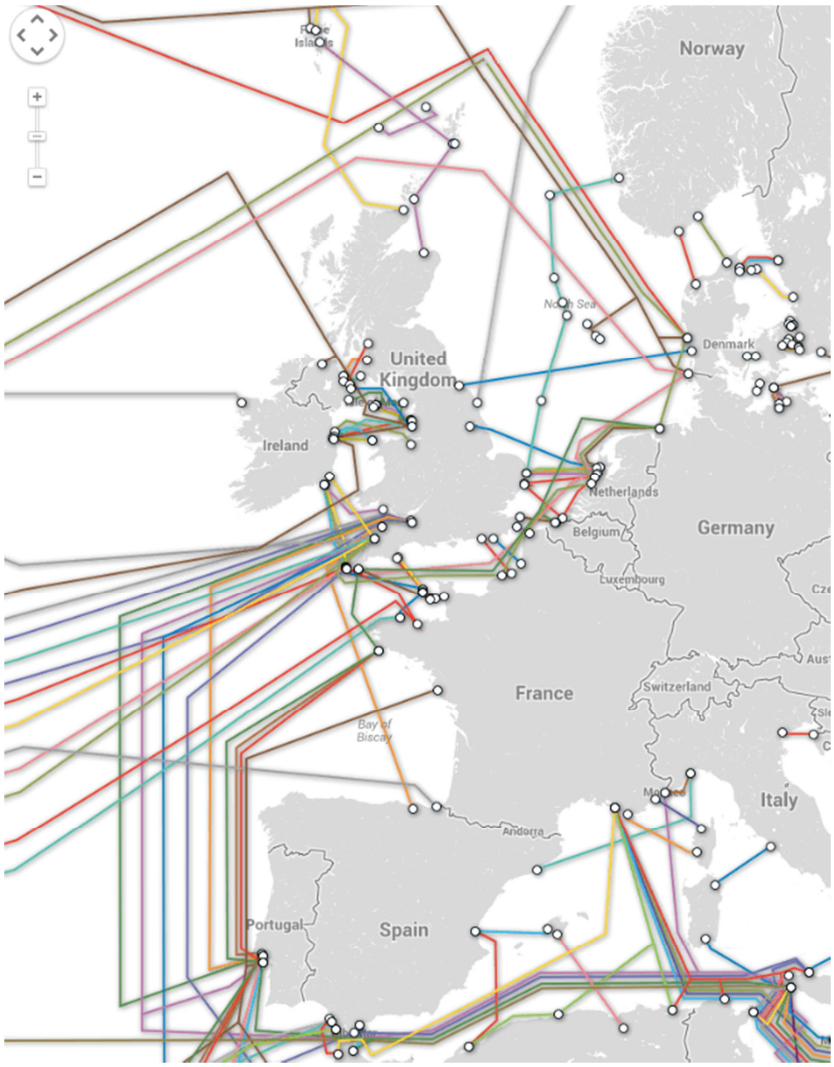
operate the cables. The programme is reported by the Guardian to have been operational since 2011[1].

23. Global submarine cables are the main arteries of the Internet worldwide. If they can be successfully tapped, then they provide a 'fast track' to total Internet surveillance, without the need to target an individual user with more specialised surveillance methods. I exhibit a map of showing their location around the world[2] ("**IB1/4/p.848**").



24. One consequence of monitoring of cables entering and exiting the UK will be that a large quantity of communications relating to the rest of the world will be caught. Much of the rest of Europe's external Internet traffic is routed through the UK, as this is the landing point for the majority of transatlantic fibre-optic cables. I reproduce below an enlargement of the map at Exhibit **IB1/4/p.848** showing this concentration:

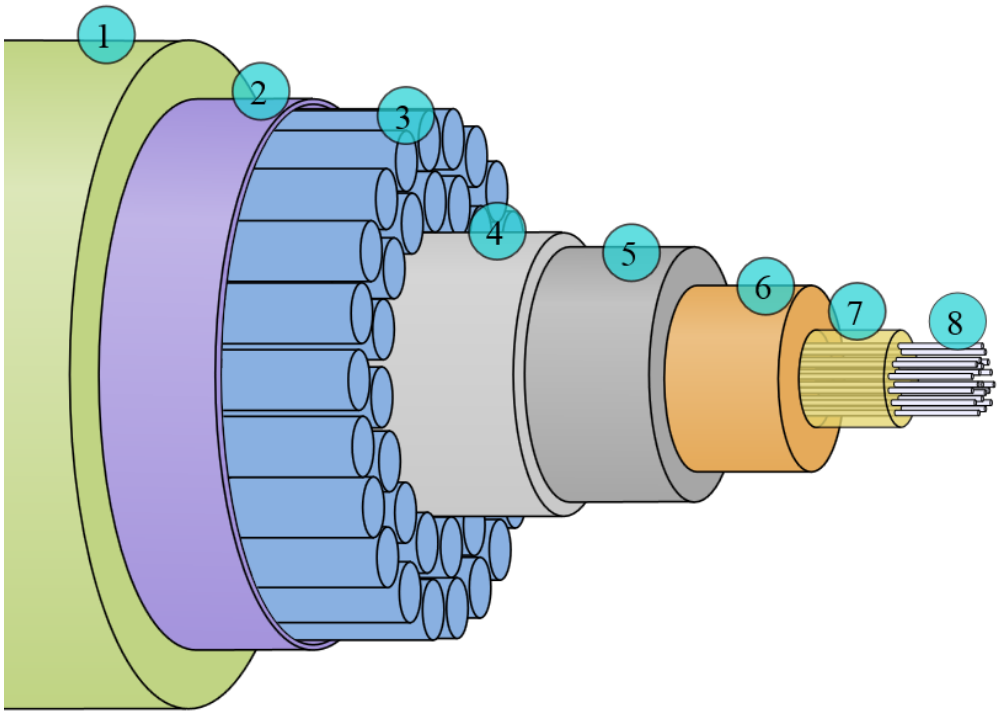
[1] *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 June 2013 ("**IB1/2/pp.658-663**")
[2] Reproduced by permission: Submarine Cable map, Telegeography © 2013 PriMetrica, Inc (at http://www.submarinecablemap.com)



25. In the UK and the rest of Europe, many 'intra-European' communications will nevertheless pass through offshore cables as they are routed to Internet and communications servers based overseas (often in the US). Although the unnamed intelligence source stated to the Guardian that "*There is no intention in this whole programme to use it for looking at UK domestic traffic – British people talking to each other*"[3], it is clearly within GCHQ's capabilities, and there is no suggestion in the source materials reported by the Guardian that 'purely domestic' (UK-internal) traffic was being excluded.

26. The cables themselves consist of a number of protective layers around a series of fibre optic cables. Typically, they are around 10cm in diameter. The following diagram shows the construction of a typical cable.

[3] Supra, note 1



The fibre optic cables themselves are labelled “8”. The other layers are 1 – Polyethylene; 2 – Mylar tape; 3 – Stranded steel wires; 4 – Aluminium water barrier; 5 – Polycarbonate; 6 – Copper or aluminium tube; and 7 – Petroleum jelly.

27. Although it would be speculative to predict exactly how GCHQ is tapping these cables, this could be done using an ‘optical splitter’, which duplicates the light signals flowing through the cables. I expect that these duplicated signals are transported over further fibre optic cables to GCHQ’s storage and processing centres in Bude, Cheltenham and elsewhere.

28. The Guardian reported that “*by the summer of 2011, GCHQ had probes attached to more than 200 Internet links, each carrying data at 10 gigabits a second*”[4]. As to the location of this tapping, I expect that it will be near to where the cables make landfall (see below). The Guardian reported that the tapping had been carried out in cooperation with the companies who own the cables, reporting that: “*companies have been paid for the cost of their co-operation and GCHQ went to great lengths to keep their names secret. They were assigned "sensitive relationship teams" and staff were urged in one internal guidance paper to disguise the origin of "special source" material in their reports*

[4] Supra, note 1

for fear that the role of the companies as intercept partners would cause "high-level political fallout""[5].

29. The Guardian reported that this mode of surveillance potentially gives GCHQ access to 21 petabytes of data a day.[6] A petabyte is approximately 1000 terabytes (which is in turn 1000 gigabytes). To convey an idea of the scale, the US Library of Congress had, in 2009, 15.3 million documents available online, the approximate size of which totalled 74 terabytes. The comparison made by the Guardian was that this quantity of data was equivalent to sending all the information in all the books in the British Library 192 times every 24 hours. It was reported that this programme gave GCHQ the largest Internet access out of the "Five Eyes" group of countries referred to in the classified documents (Australia, New Zealand, Canada, the USA and the UK).[7]

30. The data will flow from the cable probe along fibre-optic cables to GCHQ's monitoring stations. There the information is reportedly stored using GCHQ's "Internet buffers".[8] These will be massive data storage facilities searched using GCHQ's own internal servers. Even using high compression and capacity of modern data storage drives, it would require a very large area in order to store the large number of data storage facilities necessary. This storage is likely to be based, in whole or in part, in the four underground computer halls at GCHQ in Cheltenham, three of which are larger than Wembley football pitch[9] and possibly at other GCHQ sites around the country. The Guardian named GCHQ Bude (Cornwall) and one other overseas site, and quoted from an internal GCHQ document which stated that the NSA had provided £15.5m of funding to "radically enhance the infrastructure at Bude".[10]

31. The Guardian reported that the thus-obtained massive amounts of Internet data could be stored for up to three days (for content) and thirty days (for meta content).[11] "Content" refers to the entirety of the communicated data (so the content of an email or instant message, all Internet pages viewed, all information accessed and shared through social networking sites like Facebook, documents edited in "cloud" computing services like Google Docs, etc. – all of the activities carried out by individuals online, not just

[5] Supra, note 1
[6] Supra, note 1
[7] Supra, note 1
[8] Supra, note 1
[9] *GCHQ. Cracking the Code*, BBC Radio 4, 4 April 2010 (at http://www.bbc.co.uk/programmes/b00rmssw)
[10] *GCHQ: inside the top secret world of Britain's biggest spy agency*, The Guardian, 1 August 2013 (**"IB1/2/pp.723-736"**)
[11] Supra, note 1

"communications" in the traditional sense). "Meta content" is 'data about the data' i.e. data recording the means of creation of transmitted data, the time and date of its creation, its creator, the location on a computer network where it was created and the standards used. Meta-content can however be extremely revealing, as I set out above.

32. Under the Tempora programme, both metadata and content data are sifted using a technique called Massive Volume Reduction (MVR). Peer-to-peer downloads of music, films and computer programmes for example, are classed as "high-volume, low-value traffic" and filtered out, reducing the volume of data by 30 percent. The remaining data is then searched using keywords, email or other addresses of interest, or the known names or aliases of targeted persons and phone numbers. The Guardian reported that many of these keywords have been supplied by the US Government. It was reported that GCHQ and the NSA have respectively identified 40,000 and 31,000 such "selectors"[12]. An "intelligence source" described the process to the Guardian:

> "Essentially, we have a process that allows us to select a small number of needles in a haystack. We are not looking at every piece of straw. There are certain triggers that allow you to discard or not examine a lot of data so you are just looking at needles. If you had the impression we are reading millions of emails, we are not.
>
> He explained that when such "needles" were found a log was made and the interception commissioner could see that log."[13]

33. I anticipate that such sifting is partly automated, with an ever-expanding list of keywords and selectors being added to the list that is searched. It is unclear when a log will be created – whether it is when information is read by a searcher, or whether it is when useful information is found by a searcher – but in either case, it appears that the logs may not provide a complete picture of the searching activities and the surveillance carried out, since automated analysis of large quantities of data without human intervention are less carefully audited. From what the Guardian has reported about the NSA's "XKeyScore" programme, it is also likely that GCHQ staff can undertake broad categories of searches through captured data in a process akin to using standard Internet search engines.

34. Much Internet traffic these days is encrypted to protect it from interception, especially since large companies such as Google and Microsoft enabled encryption for their webmail and other services. However, GCHQ and the NSA have also reportedly

[12] Supra, note 1
[13] Supra, note 1

succeeding in decrypting data protected using many of the commonly used encryption standards (see [48] below for further details). Communications identified during searches may therefore have to be decrypted before they can be read and further used.

35. The Guardian reported that around 300 GCHQ and 250 NSA operatives are tasked with sifting through this data. The numbers of people who subsequently have access to this data are no doubt much larger. The NSA's access to the data is believed to be substantial. Citing original documents, the Guardian reported as follows:

> "In 2011, the agency [GCHQ] boasted that sharing this database with the Americans highlighted 'the unique contribution we are now making to the NSA in providing insights into some of their highest priority targets'. GCHQ also boasted that it had given the NSA 36% of all the raw information the British had intercepted from computers the agency was monitoring. The intelligence had been "forwarded to NSA", the document explained. It added: "We can now interchange 100% of GCHQ End Point Projects with NSA." This suggests the NSA potentially has access to all the sifted and refined intelligence gathered by GCHQ…
> …In the mid-year review for 2010/11, GCHQ proclaimed: "Our partners have felt the impact of our capability too, with NSA in particular, delighted by our unique contributions against the Times Square and Detroit bombers." What those contributions were is not explained. We know the NSA is forbidden from spying on American citizens; in the case of Shahzad, this question remains – was GCHQ doing it for them?"[14]

36. It is not known what use the NSA make of data obtained through access to the Tempora programme. However, there is clearly a possibility that such data may find its way into the hands of third states, whether other members of the "five eyes" group of states collaborating on Internet surveillance (the US, the UK, Australia, Canada and New Zealand) or Israel. The Guardian reported on 11 September 2013 that the NSA routinely shared raw 'sigint' data with the Israeli intelligence authorities pursuant to a memorandum of understanding between the two countries.[15]

37. A Der Spiegel article on 16 September 2013, regarding surveillance of global financial transactions by the NSA and GCHQ, noted an admission from a GCHQ presentation that the data being shared with the US was extremely wide-ranging:

> "*a document from the NSA's British counterpart -- the Government Communications Headquarters (GCHQ) -- that deals with "financial data" from a legal perspective and examines the organization's own collaboration with the NSA. According to the document, the collection, storage and sharing of "politically sensitive" data is a highly*

[14] Supra, note 1
[15] *NSA shares raw intelligence including Americans' data with Israel*, The Guardian, 11 September 2013 ("**IB1/1/pp.812-822**")

invasive measure since it includes "bulk data -- rich personal information. A lot of it is not about our targets."[16]

38. The US' access to Tempora also opens up the possibility that the UK may, by accident or by design, cooperate with the NSA to enable US intelligence gathering on UK targets and may, in turn, receive further reports from the US regarding UK citizens, based on UK surveillance (but without any individuated warrant having been issued). The actions of the NSA fall outside the purview of the provisions of RIPA outlined above, and are not overseen by the ISC, the IPT or the Interception of Communications Commissioner (see further below).

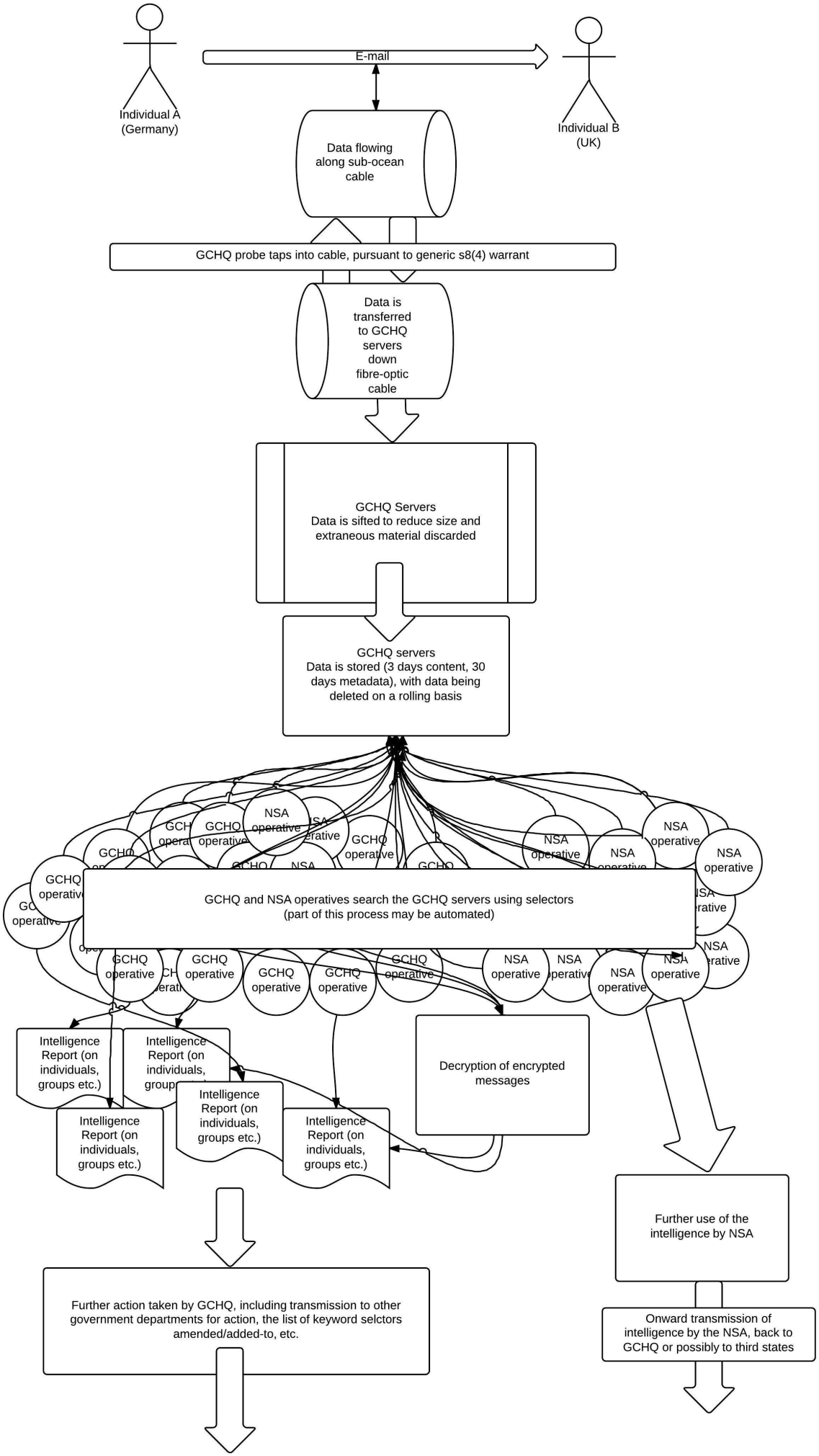
39. The Guardian reports appear to me to be credible. Some of the details have been confirmed by the US government, and by previous leaks (including by statements by former senior NSA officials such as William Binney.) Much of the technology used (such as optical splitter equipment) is commercially available. The budgetary resources required fit within the publicly known budgets of the UK and US intelligence agencies. NSA has recently completed building a widely reported data centre in Utah, costing an estimated $1.5-$2bn, with extremely large data storage and computation capabilities.[17]

40. I set out overleaf a simple diagram with a summary of how the process of gathering information via Tempora is likely to operate, in light of the information disclosed. Although informed by my knowledge of cyber-security technology and Internet surveillance, it is based on the recent disclosures. This is because there are very few other information sources regarding GCHQ's practices. I therefore do not offer the following as a confirmed example, but as an illustration of how surveillance may operate, in light of what is now known. The diagram shows an individual in Germany communicating with a person in the UK. An email is sent by him, the data passing through under-sea cables via US servers. The data is tapped in the way I described earlier and sent to GCHQ's servers, where it is buffered along with a large amount of other data. That data might then be sifted before being picked up through the use of keyword/indicator searches. GCHQ operatives then use the content to compile intelligence reports which are then transmitted elsewhere for further action. It is probable that such a communication would then be stored, or a copy made, before the content data that it was 'buffered' alongside is deleted. The meta-data would, it appears, be available to be searched for a longer period before being deleted.

[16] *Follow the Money': NSA Monitors Financial World*, Der Spiegel, 16 September 2013 ("**IB1/2/pp.823-825**")
[17] *Welcome to Utah, the NSA's desert home for eavesdropping on America*, The Guardian, 14 June 2013 ("**IB1/3/pp.844-846**")

41. As the Guardian has reported, it is possible that use of seized email content may also be made by the US authorities, and this is also represented in the diagram. Indeed, it is possible that the German national in question may be a person in whom the US is interested and in respect of whom the US has made a specific request to the UK for access to Tempora material generated by him. He may therefore find himself amongst the many keyword selectors used to sift Tempora data. The US may then have access to substantial content data from his emails, messages and other traffic, apparently without restriction. This material may be stored and, if it is likely to be useful in the future, perhaps indefinitely.

42. This also points up another problem with the vast use of keyword searches of the Tempora data. In reality, these may amount to targeted surveillance of a number of individuals, through inclusion in a rapidly growing list of keywords. However, it appears that the generalised warranting process for the Tempora programme does not treat such searches as targeted individual searches under RIPA. Although section 16 of RIPA points provides some protections for material obtained under a general section 8 (4) warrant which could otherwise have been obtained under an individuated warrant, these protections only apply to individuals located in the British Isles at the time. It would therefore offer no protection in the illustration I have given, other than to limit the period of surveillance to a maximum of six months.


Individual A
(Germany)
E-mail
Individual B
(UK)
Data flowing
along sub-ocean
cable
GCHQ probe taps into cable, pursuant to generic s8(4) warrant
Data is
transferred
to GCHQ
servers
down
fibre-optic
cable
GCHQ Servers
Data is sifted to reduce size and
extraneous material discarded
GCHQ servers
Data is stored (3 days content, 30
days metadata), with data being
deleted on a rolling basis
GCHQ and NSA operatives search the GCHQ servers using selectors
(part of this process may be automated)
Intelligence
Report (on
individuals,
groups etc.)
Intelligence
Report (on
individuals,
groups etc.)
Intelligence
Report (on
individuals,
groups etc.)
Intelligence
Report (on
individuals,
groups etc.)
Intelligence
Report (on
individuals,
groups etc.)
Decryption of encrypted
messages
Further use of the
intelligence by NSA
Further action taken by GCHQ, including transmission to other
government departments for action, the list of keyword selctors
amended/added-to, etc.
Onward transmission of
intelligence by the NSA, back to
GCHQ or possibly to third states

Global Telecoms Exploitation

43. The Guardian has also reported another GCHQ programme named "Global Telecoms Exploitation". It is believed that this programme has also been achieved by tapping fibre-optic cables. The Guardian reported that by 2012 GCHQ was handling "600m 'telephone events' each day".[18] It is unclear to me whether this extends beyond metadata to content, but, as I explained earlier, metadata can often be very revealing as to the content of a call and other relevant intelligence associated with that call.

UK Use of PRISM Programme

44. The details of the PRISM programme are, I understand, explained in another witness statement. Through this programme, the NSA gains access to data held on the private servers of well-known US Internet companies such as Google, Facebook, Microsoft, Apple, Yahoo and Microsoft subsidiary Skype. These companies state they have not provided a 'back door' to servers; they are instead transferring (large) quantities of specific data (likely matching the "selectors" described earlier) in response to legal orders[19]. The PRISM programme therefore does not involve tapping of communications 'in transit' but gaining access via the servers of major Internet companies. The fact that the UK also seeks access to PRISM suggests that it is able to access data which it is unable to reach through Tempora, either because the information has been deleted from GCHQ's servers, has not passed through UK-based fibre-optic cables, or was encrypted in transit.

45. When the Guardian disclosed details of this programme on 7 June 2013 it also disclosed that GCHQ had had access to that programme and had generated 197 intelligence reports from it in 2012[20]. It was alleged that the UK had circumvented the Regulation of Investigatory Powers Act ("RIPA'") warranting processes using PRISM. As noted above, the ISC subsequently investigated this allegation and concluded that there had been no circumvention. As noted above, the ISC found that PRISM data had been requested in cases subject to existing warrants. However, the breadth of the terms of those warrants is not known. Nor does it follow that the UK authorities consider PRISM requests require a warrant, nor did the ISC's investigation examine whether PRISM intelligence is also

[18] Supra, note 1
[19] See, for example, *Google: There is no PRISM Back Door to Our Servers, No Open-Ended Access to User Data*, techcrunch.com, 7 June 2013 ("**IB1/3/p.847**")
[20] Supra, note 1

provided to the UK authorities on an unsolicited basis or pursuant to general requests from the UK authorities. It also appears that until the disclosure of the UK's use of the PRISM programme the ISC was unaware of it and the programme itself[21].

46. In addition to requested information, the PRISM programme may also benefit the UK through unsolicited intelligence provided by the US authorities, or provided pursuant to general UK requests only, regarding UK and other European citizens. If information is 'volunteered' by the US authorities, then its receipt by the UK authorities would appear not to be subject to any warranting procedure. Indeed, the ISC clarified that its investigation into the UK's use of PRISM only looked at cases in which a specific warrant had been requested and granted by the UK authorities. In reality what is supplied pursuant to a request and what is 'volunteered' may be a grey area: given that the UK and US authorities effectively work as a team, the former hardly need to specifically request information of interest to them from the latter: the US authorities are fully aware of the UK authorities' areas and persons "of interest".

47. These facts highlight the limited effectiveness of the warranting and oversight process set out in RIPA. Based on the known facts it is possible that under the UK's use of the US PRISM Programme, PRISM data can be specifically requested of the US authorities by the UK authorities or supplied by the US pursuant to a more generalised request or even supplied unsolicited by the US. This information will have been obtained by GCHQ by a form of interception and, as it is external US material, is subject to few US law targeting protections and can have been obtained by a wide trawl for data. Further, this could include situations where one person is in the UK or even where all communications are in the UK (but stored on US servers). The restrictions on the receipt, use and dissemination of such material are insufficient.

Cracking Cryptographic Protection Systems

48. On 5 September 2013 the Guardian published further disclosures regarding GCHQ and the NSA's cracking of commonly used encryption systems used to protect emails, banking and medical records, and other private information. These disclosures are significant, not only for the further intrusion into the intentionally private communications and records of individuals, but also because of the historical context and methods used. The US Government had attempted to restrict the use of common encryption methods

[21] Sir Malcolm Rifkind, ISC Chair: "*No, I didn't know it, nor would I have expected to any more than I would any other country's process.*…" Frontline Club Debate, 9 July 2013 (http://www.frontlineclub.com/the-trade-off-individual-privacy-and-national-security/ at 58:30).

from the late 1970s until 2001, and this was roundly rejected at the time[22]. However, these allegations suggest that commonly used encryption systems have in any event been defeated by GCHQ and the NSA. The methods used are also of note: they have been achieved through covert influencing of encryption standards; through liaison with technology companies selling products to government; through 'HUMINT' – i.e. covert human intelligence means – i.e. personnel at selected private stakeholders; and through massive investment in computing capacity. The Guardian reported that funding for the programme - $254.9m for 2013 – dwarfed that for the PRISM programme ($20m per year).

49. The reported cracking of commonly used encryption standards is no doubt of importance for other programmes such as Tempora, as stored communications may require decryption before their content can be analysed.

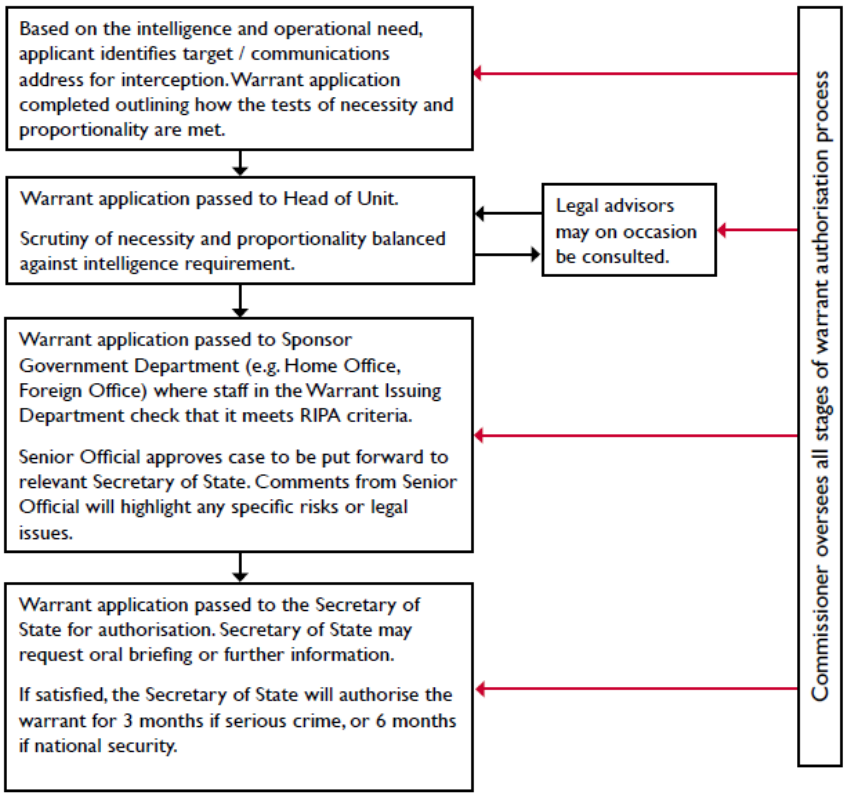
LEGAL AUTHORISATIONS

The Warranting Process

50. Surveillance of communications comes under two separate regimes in UK law. Interception of content (what is said in a letter, phone call or e-mail) is authorised for three or six months (depending on the purpose) by a warrant specifying an individual or premises from the Secretary of State under Part I Chapter 1 of the Regulation of Investigatory Powers Act 2000 (RIPA). Access to "communications data" — subscriber information; records of calls made and received, e-mails sent and received, websites accessed, the location of mobile phones — is regulated under Part I Chapter 2 of RIPA, with a large number of government agencies able to self-authorise access to some of this data. The diagram below sets out the interception of content authorising process according to the report of the Interception of Communications Commissioner:[23]

[22] See e.g. *UK and US spy agencies undermined encryption standards,* Wired, 6 September 2013 ("**IB1/3/pp.837-840**")
[23] Source: 2012 Annual Report of the Interception of Communications Commissioner ("**IB1/4/pp.851-920**").

Figure 2 - The Warrantry Authorisation Process



51. During 2012, 3,372 intercept warrants were issued using RIPA Part 1 Chapter 1, according to the 2012 report of the Interception of Communications Commissioner (para 6.3 ("**IB1/4/p.866**")).

52. An interception warrant need **not** specify an individual or premises if it relates to the interception of communications external to the UK and if an authorizing certificate has been issued by a Secretary of State which also describes the classes of material to be examined (RIPA section 8(4)). This appears from the Guardian reports and statements of the Chair of the ISC[24] to be the mechanism by which the government authorises GCHQ to undertake automated searches of communications that originate or terminate outside the British Isles, such as through the Tempora programme. Yet "external" communications could include the transmission of data to or from servers outside the UK. This would include traffic to the facilities of most of the large companies (such as Facebook, Google and Microsoft) to whom reference has been made in the NSA's PRISM programme. The Guardian reported from an internal GCHQ legal document which stated that "*The certificate is issued with the warrant and signed by the secretary*

[24] Supra, notes 1, 21.

of state and sets out [the] class of work we can do under it … [It] cannot list numbers or individuals as this would be an infinite list which we couldn't manage." Such certificates "*cover the entire range of GCHQ's intelligence production*".[25] The Guardian reported that "*Lawyers at GCHQ speak of having 10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus*."[26] It is possible therefore that a typical warrant authorising the Tempora programme may be as wide as "'*all traffic passing along a specified cable running between the UK and the US*".

53. In practice, these warrants, whilst time limited under RIPA section 9 to periods of three or six months, may in effect be "rolling" warrants, a new warrant being granted upon the expiry of the preceding warrant. This is because, by necessity, generalised warrants will not refer to particular individuals or a specific threat, but generalised threats only. The UK Government has passed a Code of Practice for the Interception of Communications ("**IB1/4/pp.921-962**"), Chapter 5 of which provides guidance for the issue of section 8 (4) warrants. It includes a requirement (at 5.2) that consideration be given to "*any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application*." However, it appears that in practice, such considerations have been insufficient to prevent the coming into being of a series of rolling warrants authorising a broad "big data" programme such as Tempora.

54. Based on RIPA, the Code of Practice and the recent disclosures, I expect that the following stages would apply to the issue of a s8(4) warrant:

    1. GCHQ applies to the Secretary of State for a warrant authorising the interception of an external communications link, such as a submarine cable, or a number of submarine cables between the UK and mainland Europe. This warrant is duly granted, pursuant to RIPA section 8 (4).
    2. The Secretary of State issues a certificate describing the categories of information to be searched. The Guardian reported that these were "broad" categories, stating that "the categories of material have included fraud, drug trafficking and terrorism"[27]. The

[25] *The legal loopholes that allow GCHQ to spy on the world*, The Guardian, 21 June 2013 ("**IB1/2/pp.664-668**")).
[26] Ibid
[27] Supra, note 1

certificate is highly unlikely to name the many thousands of potential targets and locations.

3. Tempora then gains access to this material. The use of the many thousands of keywords and selectors will not be referred to in the certificate.

55. In contrast, a warrant under the RIPA regime governing communications "internal" to the UK under section 8 (1) RIPA must name either a single person or a single set of premises as its target, and it must schedule the addresses, numbers and other factors that are to be used to identify the communications that are to be intercepted.

56. Section 12 RIPA gives the Home Secretary the power to require that communications providers facilitate lawful interception of their network. This would include requirements to install interception devices that provide specific functionality, such as the ability to intercept communications in real-time and to hide the existence of other simultaneous wiretaps from each intercepting agency. Communications Service Providers may appeal these requirements to a Technical Advisory Board, constituted by representatives of intercepting agencies and CSPs, who will report to the Secretary of State on the technical and financial consequences of the order. The order may then be withdrawn or renewed.

57. Under section 94 of the Telecommunications Act 1984, the Secretary of State may give providers of public electronic communications networks "directions of a general character… in the interests of national security or relations with the government of a country or territory outside the United Kingdom", which may be protected against disclosure.

58. Through the combination of several pieces of legislation (Section 10 of the Computer Misuse Act 1990, section 32 of RIPA, Part III of the Police Act 1997 and section 5 of the Intelligence Services Act 1994), government agencies can also be authorised to remotely break into computer systems to access data on those systems.

59. In addition to the above, under section 7 of the Intelligence Services Act 1994, the actions of GCHQ outside the UK are exempted from civil and criminal liability under UK law if done pursuant to an authorization of the Secretary of State under that section.

60. GCHQ may not be able to exploit relationships with the largest Internet companies in the same way that the NSA has apparently done through its PRISM programme, since very few of them are headquartered within the UK, although they do retain UK locations and

UK-sited infrastructure. But it clearly has conducted large-scale surveillance of communications entering or leaving the UK. The agency has reportedly already spent several hundred million pounds expanding its capabilities to intercept ISP networks in its "Mastering the Internet" programme (of which Tempora is part), with claims of a total budget of over £1bn ($1.5bn) to give analysts "complete visibility of UK Internet traffic, allowing them to remotely configure their deep packet inspection probes to intercept data – both communications data and the communication content – on demand"[28]).

OPINION

The Proportionality of the Disclosed Methods

61. It is not my role as an expert in Internet technologies, cyber-security and surveillance to determine whether or not the above-mentioned methods are a proportionate mode of surveillance. However, I feel I can note the main features of the surveillance framework and practices that I would assume will have a bearing on this question. In my opinion, the main aspects in this respect are:
    - the vast (and until the Snowden revelations unimagined) scale of the operations;
    - the fact that the offences and activities in relation to which surveillance may be (and clearly is) undertaken are not spelled out in a clear and precise manner;
    - the fact that surveillance is not targeted at specific, pre-identified individuals or even categories of individuals: under the Tempora programme, the communications and Internet activity of *all* citizens whose data flows through the UK-originating fibre cables are subjected to scrutiny (even if not all of it is read or examined by a human agent);
    - the fact that there are no clear limits on the duration of the surveillance; on the contrary, under the Tempora programme effectively *all* the data that flow through the "split" fibre cables is collected, on an on-going basis;
    - the fact that the "policies and procedures" that currently cover the surveillance are by the authorities' own admission unclear and vague;
    - the fact that these policies and procedures are not published and not subjected to Parliamentary or public democratic scrutiny;
    - the fact that there are no serious safeguards against abuse, with the current oversight regime having been shown to be unable to check the growth of the massive suspicionless surveillance that has been put in place;

[28] *Jacqui's secret plan to 'Master the Internet'*, Christopher Williams, The Register, 3 May 2009 ("**IB1/3/pp.841-843**")

- the fact that there are no known clear rules limiting the uses and disclosures of the captured data, or the sharing of the data with other agencies, including the USA's NSA or other "FIVE EYES" agencies;
- the fact that there are no known clear rules that ensure, on the one hand, that captured data are not unduly retained when they are no longer needed or relevant, and on the other hand, that data are not destroyed at a time or in such a way that errors cannot be remedied after the fact;
- more specifically, the fact that there is no requirement for victims of surveillance to be informed of the fact that they have been spied upon;
- the fact that there has not been any public or parliamentary debate on the construction and operation of the massive surveillance programmes (outside secret inquiries by the Intelligence and Security Committee), and more generally;
- the fact that most of the safeguards applied to the UK's intelligence agencies in respect of access to data collected from a large proportion of European Internet traffic, are hidden from view, making it impossible to ascertain whether they do achieve that aim;
- the fact that GCHQ exercise significant surveillance over European citizens outside the UK (and share this data with other governments) with little effective oversight for such persons, due only to the UK's advantageous access to sub-ocean cables.

62. Also important in terms of the Convention, is the fact that the US National Security Agency reportedly has direct access to Tempora and other GCHQ programme data, for purposes going far beyond those that have been accepted by the Court to justify the intrusiveness of "strategic" surveillance systems (in *Klass v. Germany, Weber and Saravia v. Germany* and other decisions). Any limits on NSA use of this data concerning UK residents are contained in secret treaty agreements. It is difficult to see how this is compatible with the UK's positive obligations to protect the privacy of those in its jurisdiction.

<u>Alternatives that impose less far-reaching interferences:</u>

63. I have consulted on issues of Internet privacy and cyber-security with both corporations and governments. In my opinion, it is possible to construct a system that accords sufficient respect to individual privacy rights whilst permitting proportionate, targeted surveillance for narrowly circumscribed purposes. Whilst the tensions in such a system cannot be eradicated, they can be managed sufficiently through oversight mechanisms that do permit public scrutiny.

64. Better protection could be achieved with notification of surveillance targets once investigations have concluded; judicial rather than executive warranting of targeted surveillance; publication of aggregate information on requests made to each Internet service provider and by investigation type and purpose; and the removal of confidentiality requirements that block Internet companies from publishing details of the procedures they apply when they receive surveillance orders.

65. In addition to the flaws in the s8(4) warranting procedures I have referred to above, it is also worth highlighting that "Metadata"/"communications data", whilst being extremely revealing about individuals' lives, receives very low levels of legal protection under RIPA Part 1 Chapter 2. This has been partially recognised by the current government, which legislated in the Protection of Freedoms Act 2012 section 37 to require a magistrate to approve local councils' access to communications data. This requirement should be extended to all government agencies.

66. One example of a system that does sufficiently protect individuals' rights to privacy can be seen in the International Principles on the Application of Human Rights to Communications Surveillance[29] ("**IB1/4/pp.963-982**"), which have been translated into many languages. They are the outcome of collaboration between civil society groups, industry and international experts in communications surveillance law, policy and technology. The preamble to the principles expressly recognises the rise of mass surveillance due to public adoption of the Internet coupled with the removal of logistical barriers to surveillance. It highlights the limitations of outmoded regulatory frameworks. The principles themselves set out standards that, in my view, have not been met by the practices I have described in this statement and their regulation under RIPA. I invite attention to all of the principles but of particular relevance are the following:

> "Legality: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.
>
> Necessity: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the

[29] https://en.necessaryandproportionate.org/text

means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.
Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1.there is a high degree of probability that a serious crime has been or will be committed;
2.evidence of such a crime would be obtained by accessing the protected information sought;
3.other available less invasive investigative techniques have been exhausted;
4.information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5.information is accessed only by the specified authority and used for the purpose for which authorisation was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

1.other available less invasive investigative techniques have been considered;
2.information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3.information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

Competent Judicial Authority: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1.separate from the authorities conducting communications surveillance;
2.conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3.have adequate resources in exercising the functions assigned to them.

Due process: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

User notification: Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

Transparency: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

Integrity of communications and systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.

Safeguards for international cooperation: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications

> surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

67. The German state data protection authorities and the Federal Commissioner for Data Protection and Freedom of Information ("the DPAs") recently passed a resolution critical of Tempora and PRISM and endorsing principles akin to those above (see summary at "**IB1/4/p.983**"). The DPAs advocated the development and implementation of German, European and international laws to ensure that privacy is fully protected and called for the enforcement of Art 8 ECHR standards in relation to current practices.

The Effects of Surveillance

68. High levels of surveillance can damage trust in technology, reduce social mobility and cohesion, encourage conformity, and have a significantly constraining effect on political debate and protest.

69. The picture of an individual - and of groups of individuals - that can be built up from communications data is immensely detailed. There is little room for individual privacy or freedom of unmonitored association when state investigators can see with whom we communicate, what we read and watch online, and where we travel with mobile phones. Network analysis of communications data (including location data), i.e., the creation of very large datasets linking people through several communication hops, which can involve millions of people, constitutes a serious interference with the right to freedom of association. I commented on the implications of such trends in surveillance for psychological notions of identity in a recent report commissioned by the UK government ("**IB1/4/pp.984-1002**").

70. Immediately before the recent press disclosures, the UN Special Rapporteur on Freedom of Expression, Frank La Rue, published a report on surveillance of communications ("**IB1/4/pp.1003-1025**"), stating:

> "23. In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are

> received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation…
> …33. Modern surveillance technologies and arrangements that enable States to intrude into an individual's private life threaten to blur the divide between the private and the public spheres. They facilitate invasive and arbitrary monitoring of individuals, who may not be able to even know they have been subjected to such surveillance, let alone challenge it. Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."

71. Surveillance computers do not just surveil: they direct the attention of police and other authorities to "targets" identified by algorithm. At the time of disclosing details about the Tempora programme, the Guardian newspaper quoted an unidentified intelligence source as stating that "*The criteria are security, terror, organised crime. And economic well-being. There's an auditing process to go back through the logs and see if it was justified or not. The vast majority of the data is discarded without being looked at … we simply don't have the resources*."[30] If accurate, these are nevertheless relatively broad criteria. Further, as I explain below, the ever-expanding capacity of storage and sifting capabilities will lead to the temptation to expand search parameters to match capacity. The Guardian's Tempora report stated: "*An indication of how broad the dragnet can be was laid bare in advice from GCHQ's lawyers, who said it would be impossible to list the total number of people targeted because "this would be an infinite list which we couldn't manage"*".[31]

72. In areas such as counter-terrorism the aim is to prevent possible crimes by people who may commit them. But attempts to automatically identify very rare incidents or targets from a very large data set are highly likely to result in unacceptably large numbers of "false positives" (identifying innocent people as suspects) or "false negatives" (not identifying real criminals or terrorists). This is referred to scientifically as the "base-rate fallacy"; colloquially, as: "*if you are looking for a needle in a haystack, it doesn't help to throw more hay on the stack*". The fact that a supposedly sophisticated computer-generated algorithm replaces a coarse stereotype does little to prevent this. By being incomprehensible even to those that rely on it, and effectively unchallengeable by those that are targeted, such "data mining" can aggravate the risk of discrimination. A 2008 US

[30] Supra, note 1
[31] Supra, note 1

National Research Council report concluded: "*there is not a consensus within the relevant scientific community nor on the committee regarding whether any behavioral surveillance or physiological monitoring techniques are ready for use at all in the counterterrorist context given the present state of the science*" ("**IB1/4/pp.1026-1055**").[32]

73. Computer processing power is expected to continue develop following Moore's Law, doubling every 18-24 months – at least thirty-fold in the next decade, although by that point the fundamental limits of silicon engineering will be approaching. Computer storage capacity and communications bandwidth will likely continue increasing at least as quickly. These exponential increases will significantly enhance the capability of organisations to collect, store and process personal data, and further reduce the technical limits on intelligence and law enforcement agencies monitoring all aspects of day-to-day life that leave any digital trace.

Failures of oversight

74. In the light of the Guardian's revelations, the performance of the UK oversight bodies and officials has clearly been deficient. It is difficult for members of the public to have confidence that their privacy is being adequately protected by a system that operates with such little transparency. A global surveillance system of breathtaking scope has been built with no public debate, authorised under sweeping secret warrants from the Secretary of State, with opportunities only for classified discussion and scrutiny in-camera by the Intelligence and Security Committee, The system of internal GCHQ rules for human rights compliance is similarly designed and operated in secret, with nowhere near the level of detail of scrutiny published by the Interception of Communications Commissioner to command public confidence.

75. As regards oversight, it is notable that the Guardian reported, again citing original documentation, that the NSA was "*given guidelines for [Tempora's] use, but were told in legal briefings by GCHQ lawyers: "We have a light oversight regime compared with the US*"[33] and that "*when it came to judging the necessity and proportionality of what they were allowed to look for, would-be American users were told it was "your call*"". GCHQ legal advisers reportedly advised the NSA that "*The parliamentary intelligence and security committee, which scrutinises the work of the agencies, was sympathetic to the agencies' difficulties" and that "Complaints against the agencies, undertaken by the interception commissioner, are conducted under "the veil of secrecy". And the*

[32] http://www.nap.edu/openbook.php?record_id=12452
[33] Supra, note 1

investigatory powers tribunal, which assesses complaints against the agencies, has "so far always found in our favour"".

76. Much greater transparency is needed for these surveillance activities, with publication of details of all programmes (with minimum withholding of information for the protection of sources and methods), allowing the media, civil society and individuals to understand and if necessary criticise government activity. For large-scale surveillance system authorisation, a parliamentary decision-making role – as seen in other countries, particularly Germany – would be appropriate.

77. A broader membership of oversight panels could be one way to improve their ability to challenge disproportionate surveillance – in particular including individuals with the technical expertise required to understand complex surveillance systems, which we know from now-declassified orders has been a severe challenge for the US's Foreign Intelligence Surveillance Court. Requirements for individuals (although not parliamentarians) to undergo highly intrusive security vetting before participating in oversight activities will reduce the diversity of those willing to do so.

STATEMENT OF TRUTH

I believe that the facts stated in this Witness Statement are true.

SIGNED: Ian Brown .....

Ian Brown

DATE: 27/9/13 .....

Application No: 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

(1) BIG BROTHER WATCH;
(2) OPEN RIGHTS GROUP;
(3) ENGLISH PEN; AND
(4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

WITNESS STATEMENT OF IAN BROWN

Deighton Pierce Glynn Solicitors

Centre Gate

Colston Avenue

Bristol BS1 4TR

Tel: 0117 317 8133

Fax: 0117 317 8093

REF: DC/2265/001

www.deightonpierceglynn.co.uk