Witness: GCHQ Witness
Party: 3rd Respondent
Number: 3
Exhibits: GCHQ 4 to 8
Date: 2/03/17

Case No, IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATION HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

WITNESS STATEMENT OF GCHQ WITNESS

I, GCHQ WITNESS, Deputy Director in the Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1) I am Deputy Director Mission Policy at GCHQ. In that role, I am responsible for drawing up the operational policies that underpin GCHQ's intelligence gathering activities and for ensuring that they are complied with. I have been in this role since 5 January 2015, having previously served as Deputy to my predecessor. I have worked for GCHQ in a variety of roles since 1997.

2) I am authorised to make this witness statement on behalf of GCHQ, MI5 and SIS ("the Agencies"). The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within both GCHQ and also MI5 and SIS.

3) I make this statement in order to respond to the contention that the Claimant makes in these proceedings to the effect that safeguards prescribed by the CJEU in the *Tele2*

Sverige/Watson and others case could and should apply to the Agencies' BCD and BPD regimes.

4) Attached to this statement and marked Exhibit GCHQ4 to GCHQ8 are five relevant documents page and paragraph numbers below are references to these exhibits.

5) In summary the use by the Agencies of bulk data including BCD and BPD typically involves complex analysis achieved by running iterative queries over multiple data sources to discover individuals, organisations and networks that pose threats to national security. This analysis must be conducted at a pace which would be completely unachievable if it were necessary for queries to be subject to prior independent authorisation. The outcome would be the effective crippling of capabilities which David Anderson QC has recognised as having contributed significantly to the disruption of terrorist operations and, though that disruption, almost certainly the saving of lives.

6) The ability to access Communications Data and Bulk Personal Data – and, critically, the ability to access such data utilising complex and repeated searches at speed - is fundamental to the ability of the Agencies to identify and manage threats, to progress investigations quickly and conduct the array of operational work with which they are tasked. This bulk data is utilised on a daily basis and is of upmost importance to provide the tapestry of information on which the Agencies operate. In their 2014 report *Privacy and Security: a Modern and Transparent Legal Framework* (exhibited as Exhibit GCHQ4), the Intelligence and Security Committee of Parliament noted (page 32):

"It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats"

7) The Agencies' investigative and operational activity covers a broad spectrum. The approach to investigation or operations will therefore be quite different depending upon the scenario. In consequence, the uses made of bulk data are also very varied: in some cases it will be used to expand an understanding of an identified individual, in others the emphasis will be on filtering subsets of the bulk data according to fragmentary information in order to attempt to identify an individual, an organisation or a network. In all circumstances the Agencies fully respect the obligation to limit their intrusion into privacy to what is necessary and proportionate. However the nature of the technical and procedural safeguards to ensure that the tests of necessity and proportionality can be met will vary, in light of the different aims of the activity and uses of the data, and as appropriate to the particular type of request.

8) The method the Agencies utilise to undertake this work routinely involves a complex array of simultaneous or consecutive steps each of which will involve accessing one or more datasets. Some of these processes may be more linear but many will involve the meshing of data which would not be possible through a specific, targeted and linear

approach. Further, it is very often the case that the Agencies are working under considerable time pressures, often involving a threat to life, whilst undertaking these processes.

Utility of Bulk Data

9) Although the Agencies utilise bulk data in different ways, the three stages of security and intelligence work to which bulk data is said be relevant (though not followed in a strictly linear way) have been expressed previously, for example in both the Government's *Operational Case for Bulk Powers* (exhibited as Exhibit GCHQ5) and in David Anderson QC's *Report of the Bulk Powers Review* (exhibited as Exhibit GCHQ6):

IDENTIFY: This is the process by which initial 'seed' information is analysed and developed to the point where it is clear that there is e.g. a potential terrorist threat, a possible candidate for recruitment as an agent, or a source of exploitable intelligence meeting current requirements. The initial 'seed' information may come from anywhere: open source (a tweet claiming responsibility for an activity, say); a humint tip-off; forensic data from seized media; information from a foreign liaison partner. Bulk data is vital at this stage in the process and may often be one of the only sources of information available to the Agencies.

UNDERSTAND: This is the process by which the intelligence picture is developed and enriched to the point where decisions can be taken about resourcing and prioritisation. Bulk data is used to help assess potential threats and opportunities, and where appropriate to seek authorisation for targeted intelligence collection to supplement bulk data.

ACTION: This action encompasses a wide range of activities, which bulk data will have helped to inform. The output of the 'identify' and 'understand' phases might be the production of intelligence reports, the running of recruitment operations, or the launching of a disruption activity, such as through arrests to prevent e.g. a terrorist attack plan.

10) This allows the following to be undertaken, rapidly and resulting in lesser intrusiveness:

a) Target discovery – identifying individuals who may be subjects of intelligence interest from lead intelligence.

b) Target development – enriching understanding of a subject of intelligence interest, their connections, networks and patterns of activity, in order to understand potential threat or opportunities.

c) Anomaly detection – a technology-based process by which patterns in bulk data are identified and analysed to assist in the detection of e.g. malware and cyber-attack signatures. This is essential for Cyber Defence.

d) Network Analysis – this is a technology-based process by which information is gathered from interception to develop understanding of the network environment to provide context to the intercepted data and enable more effective operation of e.g. the bulk interception process.

e) Triage and prioritisation – at all stages bulk data helps to inform decisions about prioritisation of resources by the Agencies, including the allocation of scarce technical, analytic, human or other collection resources.

11) Each of these stages - Identify, Understand and Act - may involve both single and iterative searches of individual or multiple datasets depending on the investigative or operational requirements. For example, a piece of 'seed' information may need to be run against multiple datasets held on several different systems with the results of initial searches enabling the refinement of further queries with the aim of both identifying legitimate leads and eliminating false trails and dead ends. Queries of bulk data can involve both searches of individual selectors (such as a telephone number or email address) and bespoke queries designed by expert analysts to undertake complex analysis of datasets in response to a complex investigative or operational requirement. These queries will often need to be run at speed against potentially fast-moving operational situations, such as terrorist attack planning or hostage situations. All staff with access to systems which search bulk datasets have received training appropriate to the tasks they will be undertaking and the data they have been given access to including on the importance of using access to data in the most proportionate manner.

12) In his *Report of the Bulk Powers Review*, David Anderson QC supported the Agencies' use of bulk data, both bulk acquisition and bulk personal data, and noted that *"alternatives would be slower, less comprehensive or more intrusive. The value of accurate information, obtained at speed, is considerable."* [§5.54d]

13) He ultimately concluded on bulk acquisition: [§6.47]

a) Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, though that disruption, almost certainly the saving of lives.

b) Bulk acquisition is valuable as a basis for action in the face of imminent threat, though its principal utility lies in swift target identification and development.

c) The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.

d) Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition.

14) On BPD, David Anderson QC noted:

> *"I have no hesitation in concluding that BPDs are of great utility to the SIAs. The case studies that I examined provided unequivocal evidence of their value. Their principal utility lies in the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat."*[§8.33]

Existing and alternative safeguards:

15) There currently exists a range of safeguards (with further safeguards coming into effect under the Investigatory Powers Act 2016 (IPA)). These were considered in detail by the Tribunal in its first judgment in this matter.

16) The Commissioners have the ability to audit and oversee the Agencies' use of tools and databases and establish the basis upon which they operate. In this context it may be helpful to quote the Interception of Communications Commissioner's Annual Report for 2014 (exhibited as Exhibit GCHQ7) in which he said (§1.6):

> *"I can report that I have full and unrestricted access to all of the information and material that I require, however sensitive, to undertake my review. I am in practice given such unrestricted access and all of my requests (of which there have been many) for information and access to material or systems are responded to in full. I have encountered no difficulty from any public authority or person in finding out anything that I consider to be needed to enable me to perform my statutory function."*

The willingness and ability of the Commissioners to investigate the use by the Agencies of their powers is also illustrated by the Interception of Communications Commissioner's Review of directions given under section 94 of the Telecommunications Act (exhibited as Exhibit GCHQ8) which the Commissioner himself was able to describe in his letter to the Prime Minister, included at the front of the published report, as *"comprehensive"*.

17) Given the frequency with which BCD and BPD is required to support the Agencies' operations, the requirement to conduct complex analysis, and the need to work at pace – as highlighted by David Anderson's conclusions – it is of paramount importance that the Agencies are able to access data in an agile way. Introducing additional requirements beyond those already envisaged under the IPA for access to this data (such as independent authorisation by a judicial commissioner or other independent authoriser) would considerably impact our ability to work at the required pace and to conduct essential complex analysis – and thereby to carry out our functions and protect national security.

18) Any independent authorising body would need to be located in secure premises. It would be necessary to submit queries electronically (e.g. by email or through a bespoke workflow process) to the authorisers. Queries would need to be accompanied not only by a statement of necessity and proportionality, but often with additional detail on any

technical complexities of the queries, and potentially with information on the systems on which the queries would be run, including details of the datasets those systems contained. There would need to be a facility by which the authoriser could ask for clarification of any outstanding issues, either through further exchanges of text or potentially by telephone with the requesting analyst. Given the complexity and specialist knowledge leading to the consideration of data to be utilised, for requests to be independently considered and authorised would likely require either specialist knowledge or time for consideration, again impacting on the ability to deliver at speed. This is discussed further in the case studies below. The whole process would need to occur at pace while the analyst is potentially running previously-approved queries and analysing the results. The independent authorisers would need regular briefing on the capabilities whose use they are authorising. There will be a requirement for authorisation to be available 24 hours a day and 365 days a year. It is hard to see how even the slickest and best resourced operation would not add many hours of delay into operational work, and if there were technical problems with the authorising body's systems or communications work could be severely hampered. The effect would be to critically undermine the ability of the Agencies to tackle threats to national security by reducing their overall capacity to pursue investigations, as a result of the additional delay and the resource impact. In time-critical operations this could be the difference between the successful disruption of a threat or otherwise.

19) We should not discount the inevitable risks associated with widening the circle of knowledge of the Agencies most sensitive casework. Certain casework is dealt with on strict need to know principles to protect the information and security of operations; bulk data can, for example, be a vital tool to identify and protect the lives of agents who often operate in high risk environments and at personal threat from terrorist groups and highly capable state adversaries. Managing the security of this information and supporting independent authorisers to protect them from targeting by hostile state activities, are potential significant practical obstacles that would need to be overcome.

20) In relation to the CJEU's suggestion (in the context they were considering) that geographical criteria could be applied as a safeguard, this would be very difficult to undertake. By way of example the sophistication of terrorists and criminals in communicating over the internet in ways that avoid detection, whether that be through the use of encryption, the adoption of bespoke communications systems, or simply the volume of internet traffic in which they can now hide their communications makes such an approach entirely impracticable in the context of the Agencies' work. The internet is now used widely both to recruit terrorists, and to direct terrorist attacks, as well as by cyber criminals. Imposing such constraints would damage the Agencies' ability to safeguard national security at exactly the point when advances in communications technology have increased the threat from terrorists and criminals using the internet.

21) The judgment in *Tele2* also discusses a mechanism for notifying individuals whose privacy has been intruded upon. In the context of national security investigations such an approach could readily highlight those who remained under investigation and/or those to whom it would be undesirable to provide notification of a past or current interest

on the part of the Agencies. Furthermore the processes for both notification and considerations required within such a system would be unworkable given both the sophistication of the communications process described above and the iterative and multi-layered analytic approaches needed to tackle it. To the extent that notification assists in the provision of a right of redress, this Tribunal already meets that need.

22) Such questions highlight both the impracticality of such safeguards being considered, as well as the potential significant impact on the effectiveness of the Agencies, as they would necessitate the taking away from the operational front line of expert analysts in order to obtain prior approval for queries, reducing the number of queries, and thus the quantity of operationally effective intelligence available to the Agencies, or reduce the level of assurance deriving from the data to which they had access. The following examples are intended to provide context.

Examples and Impact:

23) David Anderson QC's *Report of the Bulk Powers Review* and the *Operational Case for Bulk Powers* set out a wide range of scenarios and case studies where timely, reliable and secure access to bulk data has been essential in fast moving operations. Considering a handful of these in light of the potential safeguards suggested by the claimant, the potential impact has been highlighted:

MI5 Examples:

EXAMPLE 1: LONDON AND GLASGOW ATTACKS OF 2007 (FROM *THE REPORT OF THE BULK POWERS REVIEW*)

24) This case study related to the London and Glasgow attacks in 2007. Using bulk acquisition data, MI5 was able to establish within hours that the same perpetrators were responsible for both attacks. MI5 was also able, within a similarly short period, to learn more about the details of the attacks, including the methods used and the identities of those involved or associated with the attackers. The ability to conduct this analysis at pace enabled MI5 to support the police in responding swiftly to the attacks and to the threat of further, imminent attacks.

25) It would not have been possible to achieve the same results with comparable speed, using targeted queries. Speed was essential at the time, when the SIAs and police had to learn as quickly as possible whether other attacks were imminent. Bilal Abdulla was subsequently convicted of conspiracy to murder and conspiracy to cause explosions likely to endanger life. Kafeel Ahmed died of the injuries that he sustained at Glasgow Airport, having set himself alight.

26) Instituting a requirement for review by an independent authority of bulk data requests undertaken to identify the perpetrators and methods used could have hampered those timescales. This would have had a knock on effect on MI5's ability to carry out further analysis and put in place more intrusive activity, and thus MI5's ability to provide

external assurance over these matters at the earliest opportunity. If geographical limits had been placed on these searches based on the initial occurrence in London, this might have affected MI5's ability to connect the two locations in the most agile manner.

EXAMPLE 2 - PREVENTION OF BOMB ATTACKS AT NUMEROUS LOCATIONS (FROM *THE REPORT OF THE BULK POWERS REVIEW*)

27) In 2010 a network of terrorists comprising groups in Cardiff, London and Stoke-on-Trent planned a series of bomb attacks at several symbolic locations in the UK, including the London Stock Exchange. Complex analysis of BCD played a key role in identifying the network. The task was made particularly challenging by the geographical separation of the groups. Nine members of the network were subsequently charged and pleaded guilty to terrorism offences relating to the plot. Eight members of the network pleaded guilty to engaging in conduct in preparation for acts of terrorism.

28) This required complex analysis of large volumes of data in order to identify the attackers and understand the links between them in the shortest possible time.

29) Inserting an independent authoriser into the process would have created time delays that could have impacted MI5's ongoing assurance around this significant risk. If the acquisition of bulk data was restricted on a geographical basis, MI5 might not have fully drawn out the links between the groups, impacting the speed and agility of the investigation.

EXAMPLE 3 PREVENTION OF IRISH DISSIDENT ATTACK (FROM *THE REPORT OF THE BULK POWERS REVIEW*)

30) In this 2013 case, bulk acquisition data was used to foil an attack by Irish dissident republicans. It was suspected that members of the group had already obtained explosives and that their activities were increasing (a common sign of an attack being imminent). However, MI5 did not know the date of any proposed attack and the group's security awareness made it difficult to obtain further information.

31) The use of bulk acquisition data identified telephones being used by the group, and further enabled MI5 to identify previously unknown members of the group. MI5 was able to increase its coverage of this expanded group. As a result it became aware of a sudden further increase in activity from analysis of the group's communications activity and MI5 judged that an attack was imminent. Police intervened and recovered an improvised explosive device. A prosecution followed. Without bulk acquisition data, the telephones would not have been identified.

32) Any delay in the ability to acquire and carry out analysis of bulk data in such cases, such as through independent authorisation in advance of bulk data acquisition, could have impeded the operational effectiveness of MI5 and its ability to understand and react quickly to changes in the group's activity.

GCHQ Examples:

EXAMPLE 4: CHILD SEXUAL EXPLOITATION (FROM THE *OPERATIONAL CASE FOR BULK POWERS*)

33) While this and the following two examples primarily involve bulk communications data acquired pursuant to warrants issued under RIPA, the principles involved apply equally to the use of BCD acquired pursuant to a Direction under s.94 of the Telecommunications Act 1984, or to BPD.

34) In the single month of April 2016, as a result of hundreds of searches of bulk data, GCHQ identified several hundred thousand separate IP addresses worldwide being used to access indecent images of children on the open web. This figure is only a snapshot, and does not include access to such images through the dark web.

35) This insight has challenged some of the UK's existing thinking and plans as to how to counter online CSE. GCHQ has also used the same capability to analyse secondary data to assist the National Crime Agency (NCA)'s efforts to prioritise online CSE leads, for instance of those whose online behaviour suggests they pose the greatest risk of committing physical or sexual assaults against children. In seeking to identify users who should be investigated as a priority, GCHQ uses criteria that were developed by academics, law enforcement agencies and charities. The team was given two examples of arrests made as a result of GCHQ's CSE work. One of those arrested was an individual who operated anonymously online to avoid detection. After he used a VOIP provider to contact another suspect who was already under investigation, the NCA prioritised the investigation of his activities. Despite full cooperation from the service provider, attempts to identify him were unsuccessful. Although the NCA had discovered the anonymous online user name he had used, the details that he had used to register them did not allow him to be tracked back to his "real world identity" using conventional means.

36) GCHQ analysts applied advanced analytic techniques to secondary data that had been obtained under bulk interception warrants and was held within GCHQ databases. The analysts rapidly identified recent online activity by the individual and a number of current contact details. These were passed to the NCA which was then able to obtain a genuine name and address for the individual, leading to a swift arrest. The individual pleaded guilty to multiple charges, including two counts of sexual abuse, and received a custodial sentence of over 3 years as a result.

37) If the acquisition of bulk data were restricted on a geographical basis this would result in a far less accurate overall picture and would not be as effective as the use of geographically unrestricted bulk communications data in identifying technologically-sophisticated individuals engaged in online CSE. Furthermore, as in this example, individuals often use false details to avoid identification and also use multiple communications methods. A requirement to independently authorise each query of bulk data would take significantly more time to obtain results, delaying the safeguarding of children and giving the offender more time to target more victims. Furthermore, not all

individuals engaged in CSE will be successfully prosecuted. Any notification regime would have the potential to alert those not convicted that their activities are being monitored, and will seek to further obfuscate their activities.

EXAMPLE 5: TERRORIST ATTACKS OVERSEAS (ABSTRACTED FROM SEVERAL EVENTS)

38) There have been numerous cases in recent years of terrorist attacks overseas where UK interests are threatened. Examples include the attack on Mumbai in 2008, the attack on a shopping centre in Nairobi in 2013 and the attack in Sousse, Tunisia, in 2015. In such cases it is critical to understand what is going on, who the attackers are, what their command and control network consists of, and other details of the attack in as close to real time as possible so that it can most effectively be disrupted or contained. The principal capability available to achieve this end is bulk data acquired under RIPA or Telecommunications Act powers, or obtained as BPD.

39) It is not unusual when such attacks take place for attackers to abandon all previously used communications devices shortly before launching their attack. For this reason, even if attack planning has been detected, and targeted investigatory powers used against the attackers network, any such coverage will be lost, and the communications must be reacquired through target discovery (described in paragraph 12 above).

40) Target discovery may take as its starting point any available information. In some cases we may become aware of individuals who have knowledge about the attack, suggesting that they are in contact with the attackers or with those directing the attack. The analysis of bulk data makes it possible in some circumstances to make links through complex analysis that will enable us to establish who and where the attackers are. There may be indications in open source that there are individuals who appear to have an unusually high level of knowledge about the attack as it is unfolding, suggesting that they are in direct contact with the attackers or with those directing the attack. The analysis of bulk data makes it possible in some circumstances to link such open source indications to other communications channels used by individuals and from these it may be possible to identify who and where they are.

41) Such an approach will require the running of dozens if not hundreds of proportionate and iterative queries over many analytical systems. The queries themselves are unlikely to consist of simple searches for target identifiers, because those are precisely what we are seeking to discover. Instead they might well look like several lines of code.

42) For independent authorisation of queries to provide any sort of meaningful safeguard, the independent authoriser would need to have a comprehensive level of knowledge and expertise to interpret queries which would not be immediately comprehensible, or else require an explanation or discussion with the analyst/officer concerned. This would potentially take a considerable period of time and therefore have an impact on the pace at which the work could be delivered.

EXAMPLE 6: PROTECTING THE UK FROM CYBER ATTACK (FROM THE *OPERATIONAL CASE FOR BULK POWERS*)

43) GCHQ routinely uses bulk communications data to detect cyber-attacks against the UK, including large scale thefts of data and serious fraud by cyber criminals, and operations by hostile intelligence services and potential terrorists. Using electronic 'signatures', which operate in a similar way to electronic fingerprints, the agencies scan the technical detail of internet communications for evidence of incoming attacks to the UK. This approach can both identify known forms of computer malware and discover new forms of cyber-attack that the agencies have not previously encountered. Cyberspace is so large, and technical change so rapid, that analysis of bulk communications data is the only way for the agencies to monitor for such attacks as they occur: targeted approaches would be highly likely to miss an attack. The resulting intelligence is typically shared with industry partners, who in turn use it to protect UK citizens and businesses.

44) Hostile cyber actors will use the global internet to disguise their identity and location, making use of infrastructure (leased or compromised servers, for instance) around the world (and increasingly being provided by "cloud" services who themselves allocate server space without regard to geography). It would not therefore be possible to apply any geographical restriction on the data of most importance in countering this activity.

SIS Examples:

EXAMPLE 7: RECRUITING AN AGENT (FROM *THE OPERATIONAL CASE FOR BULK POWERS*)

45) The security and intelligence agencies were tasked by the UK's Joint Intelligence Committee to produce intelligence on a specific country threatening the UK's national security. They identified an individual with access to the required intelligence, but were unable to approach the individual directly due to the risk the individual would face from his country's own internal security service. Intelligence reporting showed that the individual was in contact with another person that the UK agencies might be able to approach with lower risk. The reporting, however, did not fully identify who this contact was. The security and intelligence agencies used BPD to identify that contact conclusively, enabling them to determine that they could safely approach the contact and seek support. The contact has been successfully recruited as an agent to help collect intelligence and protect the UK's national security."

46) Inserting a requirement for prior authorisation for each BPD access involved in this case would have critically disrupted targeting efforts. At multiple points and across relevant teams a series of BPD searches were required to establish the identity of the key target and to establish the biographical details of their contact. At any stage, a delay in proceedings could have prevented a successful approach.

EXAMPLE 8: ISIL MEMBERSHIP LIST (FROM *THE REPORT OF THE BULK POWERS REVIEW*)

47) In early 2016, SIS was tasked with collecting intelligence on members of ISIL. Sky News had reported there to be 22,000 names on the ISIL membership list but in most cases the information was not of sufficient quality for SIS to make a positive identification, with high confidence, that could be used as the basis for an investigation. The use of BPDs, in combination with open source reporting, enabled SIS to identify foreign fighters with links to the UK or other partner states.

48) The SIS response to the Sky News leak was to convene a dedicated team to investigate and analyse the membership list. Multiple and complex searches of BPD were carried out by the team, working closely with colleagues in partner agencies in the UK and overseas. To notify, or work through analysis of whether, 22,000 people (whose details were on the list) could be notified would be resource intensive and could require additional, disproportionate measures.

Statement of Truth

I believe that the facts stated in this witness statement are true.

SCHR Witness

.....

Dated: 2 March 2017