Witness: CGW
Party: Claimant
Statement Number: 2
Date: 2 May 2017

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/15/110/CH**
B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

SECOND WITNESS STATEMENT OF CAMILLA GRAHAM WOOD

I, Camilla Graham Wood, of Privacy International, 62 Britton Street, London, EC1M 5UY, WILL SAY as follows:

1. I am a solicitor and a legal officer at the Claimant. I am duly authorised to make this statement on the Claimant's behalf. 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, I have indicated the source of the information and I confirm that the information is true to the best of my knowledge and belief.

2. There is a lack of publicly available information in relation to the processing required by PECNs and technical requirements that may be imposed as a result of a section 94 Direction, including:
   a. The breadth of technical and/or processing obligations and how onerous or expensive the set of obligations might be;
   b. How and what processes are required to deliver BCD;
   c. How the data is acquired / transferred from the PECN to MI5 and/or GCHQ;
   d. Related to this, in what format the data is transferred from the PECN to MI5 and GCHQ;
   e. How the data is prepared in advance for transfer; and
   f. What categories of data are acquired using section 94 Directions.

3. I have asked individuals who have worked at telecommunications operators which may have been served with section 94 Directions the relevant questions as to what is involved in processing BCD pursuant to a section

94 Direction. Because of the secrecy requirements that accompany section 94 Directions, those who have been in receipt of such directions and those who have worked at telecommunications companies where bulk communications data was processed and transferred to the agencies pursuant to such Directions have stated they are unable to assist me.

4. On that basis, the Claimant has sought to analyse what processing is likely to be required in response to a section 94 Direction, based on its understanding of the operation of communications systems and other large databases. The Claimant considers that the processing involved in compliance with a Section 94 Direction is likely to include:
    a. File formatting;
    b. Formatting for transfer;
    c. Pre-processing to extract, remove or collate data, e.g. deep packet inspection ('DPI');
    d. Compression;
    e. Encryption; and
    f. Error checking and correction.

5. The purpose of this statement is, firstly, to explain some of the activities the Claimant considers are likely to take place when BCD is obtained and transferred pursuant to a Section 94 Direction.

6. In addition, this statement will address the evidence contained in the third witness statement of the GCHQ witness (dated 2 March 2017), which suggests that it would be impractical to comply with the safeguards identified in the judgment of the CJEU in *Watson* in the context of the Agencies' work.

Processing

7. The major PECNs are likely to offer a number of different products and services, and have large subscriber bases. Their networks are likely to consist of various interacting devices and platforms.

8. Communications data is generated every time a customer uses a PECN i.e. makes a call, creates a text or uses the internet. Often, communications data will be created without any action by the customer. For example, a mobile telephone will regularly and automatically contact the PECN to maintain its connection with the network. Services (such as email or social networks) will automatically update. Each time such a connection is made, communications data (including location data) will be generated. Users generate vast quantities of communiations data. Each piece of communications data contains information about a customer's activity. Communications data may be recorded on different devices as it passes through a network. Communications data related to transactions may be recorded and encoded in different formats.

9. The requirements imposed by a section 94 Direction will likely necessitate

additional processing and the use of additional storage media beyond what would otherwise be created in the PECNs' normal course of business. There may be demands as part of section 94 Directions, for instance, for reliable back-up of BCD to be made, leading to the need for additional storage facilities and back-up locations together with power sources and independent communication lines and servers.

10. The database systems used by a PECN and indeed by the intelligence agencies are likely to have changed over the years during which section 94 Directions have been imposed.

11. Section 94 BCD Directions have been in use since 1998. Since that period, the internet has become popularised and there have been dramatic changes in communications technology. The quantity of data now transmitted over the internet by smartphones alone is very large:

> '*In 2014, the Smartphone mobile data traffic alone stood at 1.73 EB per month (69% of global mobile data traffic)...Tablet mobile data traffic will grow 20-fold from 2014 to 2019 to reach 3.2 EB per month.*'[1]

12. Numerous new database languages/formats and systems have been developed in that period including PostgreSQL and SQL.

13. Given the variety of database formats available, it is unlikely that every CSP uses the same database system or the same format/language for data in their database system, much less the same system as the intelligence agencies. Thus, there may be a requirement to convert data prior to transfer or to store the data in a particular format/language in order to comply with a section 94 Direction.

14. Even if the BCD sought were in a format that was compatible with the intelligence agencies' database systems, to transfer the data it is likely that a PECN would need to re-format the data or files. It is unlikely that a PECN would use the same format for storing, manipulating and processing the data as they would to transfer it. MySQL and PostgreSQL are examples of commonly used database systems, whereas XML[2] and CSV[3] are used widely used for transferring data. Processing is required to change data into different formats.

15. There is likely to have been consideration as to what formats are compatible with agency systems, which may change over the years as systems change and are updated.

---

[1] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-rise-of-on-demand-content.pdf

[2] Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable

[3] **CSV:** comma separated value

Comma delimited: A record layout that separates data fields with a comma and usually surrounds character data with quotes.

16. When section 94 was initially used, the PECNs might have been transferring large amounts of data to the intelligence agencies physically using hard drives (or other physical media). However, as technology has developed to allow the transfer of higher volumes of data quickly machine to machine, and given that disclosed documents refer to 'regular feeds', it is likely transfer takes places by electronic means as technology has developed and the volume of communications data has increased.

17. If data is transferred machine to machine, basic principles will need to be considered such as interruptions to data transfer and the need to check the logging and correction of data.

18. Given the volume of communications data, there is likely to be a requirement on the PECNs to compress the data before it is transferred. The *Computer Glossary* provides a useful definition:

> **Data compression** is defined as encoding data to take up less storage space. Digital data is compressed by finding repeatable patterns of 0s and 1s. The more patterns that can be found, the more the data can be compressed. Text can generally be compressed to about 40% of its original size and graphics files from 20% to 90%.[4]
>
> 'Data compression schemes fall into two categories. Some are lossless, others are lossy. Lossless schemes are those that do not lose information in the compression process. Lossy schemes are those that may lead to the loss of information.'[5]

19. In relation to the developments in technology that affect the volume of communications data, David Anderson Q.C. in *A Question of Trust* commented[6]:

> *'4.5 As recently as 1989, letters and landlines were the main methods of communication. By 2014, fewer than three in ten 16 - 24 year olds used a landline during a week. 16% of UK households do not have one, and the latest UK Communications infrastructure Report suggests the increasing use of internet telephone may eventually lead to the landline network (the public switched telephone network) being turned off.*
>
> *4.6 The mass uptake of digital technology is progressing at extraordinary speed:*
> *(a) In 2014, 82% of UK homes were connected to the internet compared to 25% in 2000, and 93% of adults owned a mobile phone in 2014 compared to 50% in 2000.*
> *(b) In 2014, for the first time, there were estimated to be more mobile*

[4] The Computer Glossary, Alan Freedman, 8th edition, ISBN 0-8144-7978-2
[5] Computer Science, an overview, 12th Edition, J.Glenn Brookshear, Pearson, ISBN 10: 1-292-06116-0, pg 75
[6] A Question of Trust, Report of the Investigatory Powers Review, by David Anderson Q.C. Independent Review of Terrorism, June 2015

phone subscriptions than people in the world.

(c) Ownership of smart phones is soaring: 61% of adults owned a smart phone in 2014 compared to 27% in 2011. A comparison across the generations is even more striking, with 88% of 16 - 24 year olds owning a smart phone, compared to 14% of those over 65.

(d) This explosion in the smart phone market is driving the growth of people accessing the internet using their mobile phone: 57% did so in 2014 compared to 28% in 2011.

4.7 Phone calls and texts are being joined by other communication platforms such as instant messaging, video calls and communication through social networking sites. Whilst the adult population in general spent 33% of their total daily communications time using email, this reduced to 19% amongst 16-24 year olds, who favour social networking sites over email. Instant messaging apps have overtaken traditional SMS services. In 2012, 19 billion messages were sent per day on instant messaging apps, compared to 17.6 billion text messages. Since 2012 the number of instant messaging apps has grown considerably.

4.8 A further trend is the growing proportion of customers in the UK using Voice Over Internet Protocol [VOIP]: making a phone call over the internet. The number almost tripled between 2009 and 2014, from 12% to 35%. The upsurge in use of VOIP services is linked to the increased ownership of smart phones and tablets, as these devices have integrated VOIP apps. Household take-up of tablets almost doubled between 2013 and 2014, from 22% to 44%.

4.9 Also striking is the increasing pace of adoption of new technologies. Whilst it took 15 years for half the UK population to get a mobile phone, newer technologies, such as social networking sites, reached these figures in four years.'

4.10 Overall, there are trends towards an increasing variety of communication methods, an increasing number of devices and an increasing pace of adoption of new technologies with young adults leading the way."[7]

20. When transferring data, it is likely that security and encryption measures will be required, as well as checking to ensure data integrity and transfer without error.

21. If a PECN is required to provide BCD then there may be requirements in place should there be a loss of data or corruption of data. These requirements may include back ups. These are defined in the *Computer Glossary* as follows:

Back up: To make a copy of important data onto a different storage

[7] A Question of Trust, Report of the Investigatory Powers Review, by David Anderson Q.C. Independent Review of Terrorism, June 2015

medium for safety.[8]

22. It was noted by Vodafone in evidence to the Joint Committee on the Draft Communications Data Bill that it is necessary to have two independent communications data storage sites in case one goes down in order to provide a reliable back up:

> *"Q.453 Mark Hughes (Vodafone): No. We must have two sites. We must have a resilient site in case one site goes down."*[9]

23. In order to ensure the integrity of BCD, PECNs may mirror the data to a separate database server in order to comply with s.94 Directions.

24. In order to extract communications data from internet traffic, it may be necessary to conduct a detailed automated inspection of internet data. This process is known as Deep Packet Inspection. To use a physical analogy, DPI requires opening a letter and reading the contents to deduce the sender and recipient, rather than simply looking at the envelope. This requires extensive (and expensive) processing:

> **Deep Packet Inspection:** operates on packets instead of files. That is, instead of merely examining the headers in packets that pass into the site, a DPI mechanism also examines the data in the packet payload. Because a packet payload in an Ethernet frame can be over twenty times larger than a packet header, DPI can require twenty times more processing than header inspection. Furthermore, the payload is not divided into fixed fields, which means that DPI mechanisms must parse contents during an inspection.[10]

25. In providing communications data for internet communications in oral evidence to the Joint Committee on the Draft Communications Bill, Professor Peter Sommer stated in response to a question on the distinction between communications data and content:

> *"…communication on the internet takes place in a series of packets. Each packet contains information about where it has come from, the IP address of the originator, the IP address where it is supposed to be ending up and some supervisory information, so that if the packets arrive slightly out of order, they can be reassembled. The rest of it is what we call the payload…. the CSP …is carrying out the requirements of the legislation to separate communications data from content, so the requirement on the kit is absolutely fantastic. That is why it costs a great deal of money."*[11]

---

[8] The Computer Glossary, Alan Freedman, 8th edition, ISBN 0-8144-7978-2

[9] https://www.parliament.uk/documents/joint-committees/communications-data/Oral-Evidence-Volume.pdf

[10] Computer Networks and Internets, 5th edition, 2009, ISBN 10: 0-13-504583-5 pg 524 - 525

[11] https://www.parliament.uk/documents/joint-committees/communications-data/Oral-Evidence-Volume.pdf

26. Using Deep Packet Inspection will often be necessary if the section 94 Direction requires the extraction of a full record of the relevant communications data. For example, simply looking at the internet packets will often just show a communication between a mobile telephone and a company's servers. All that would be disclosed was that a particular smartphone was using a particular service (e.g. Gmail, Google, Twitter, Facebook etc.) at a particular time. It would be necessary to look inside the packet to identify who the communication was with. It may also be necessary to attempt to remove encryption to obtain this information.

27. As technology has changed over the years since section 94 was first utilised, it is likely that the methods by which section 94 Directions are implemented, such as the way BCD is retained, processed and transferred has changed, particularly with: the growth of the use of smartphones; the move away from use of landlines; and the impact of the use of online video-streaming on traffic data volumes. Given the volume of communications data that results from video streaming, it may be a requirement for PECNs to remove this traffic data prior to transfer to the intelligence agencies:

> *'Most of this data growth is attributed to different digital media especially the entertainment services like video, audio etc. Globally video and audio traffic has dominated the internet data consumption for some years now. The devices used to access digital content have evolved in the last few years that have increased the array of platforms on which a user can stream audio and video content. Netflix share of internet traffic in North America increased further and accounted for 34% of data flowing to consumers during the peak times in first half of 2014. Over-the-top (OTT) service providers like YouTube and Subscription-based digital content providers like Spotify have also acted as a catalyst in the growth of audio/video data streaming. The global audio and video traffic combined is expected to reach 82% of all internet traffic by 2018.'*[12]

28. The Snowden disclosures include a document titled 'Mobility Business Records Flow Significantly Increases Volume of Records Delivered Under BR FISA'[13] which refers to extensive dialogue, repeated testing and extensive coordination to receive AT&T mobile phone records:

> **Title:** Mobility Business Records Flow Significantly Increases Volume of Records Delivered Under BR FISA

[12] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-rise-of-on-demand-content.pdf

[13] https://search.edwardsnowden.com/docs/MobilityBusinessRecordsFlowSignificantlyIncreasesVolumeofRecordsDeliveredUnderBRFISA2015-08-15nsadocs
https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0

Description: This 30 August 2011 post from the NSA internal newsletter SSO Weekly reveals that AT&T (FAIRVIEW) began sending over 1.1bn US mobile phone records to the agency every day: see the New York Times article AT&T Helped U.S. Spy on Internet on a Vast Scale, 15 August 2015.

Document: (TS//SI//NF) Mobility Business Records Flow Significantly Increases Volume of Records Delivered Under BR FISA By Hon 2011-08-30 1440

(TS//SI//NF) On 29 August, FAIRVIEW started delivering Mobility Business Records traffic into MAINWAY under the existing Business Record (BR) FISA authorization.

The intent of the Business Records FISA program is to detect previously unknown terrorist threats in the United States through the cell chaining of metadata. This new metadata flow is associated with a cell phone provider and will generate an estimated 1.1 billion cellular records a day in addition to the 700M records delivered currently under the BR FISA.

After extensive dialogue with the consumers of the BR data, repeated testing, a push to get this flow operational prior to the tenth anniversary of 9/11, and extensive coordination with external entitites via our OGC (to include: FBI, DOJ, ODNI, and FISC) NSA received approval to initiate this dataflow on August 29, 2011. Analysts have already reported seeing BR Cellular records in the Counter Terrorism call-chaining database queries.

Document Date: 2011-08-30

Release Date: 2015-08-15

Complying with safeguards

29. The third witness statement of the GCHQ Witness dated 2 March 2017 was provided to respond to the Claimant's position that safeguards required by the CJEU in the *Tele2 Sverige/Watson and others* case apply to the Agencies' BCD and BPD regimes. The purpose of the GCHQ evidence was to suggest that it would be impractical to comply with such safeguards in the context of the Agencies' work. Such evidence could have been (but was not) adduced in *Tele 2 Sverige/Watson and others*.

30. There is no such impracticality. The Respondents will need to introduce substantial safeguards for communications data generally in response to the judgment in *Tele 2 Sverige/Watson*. There is no reason why the solutions for compliance in other contexts cannot be applied to the Agencies' work.

31. On 14th March 2017 the Home Office via email to the Claimant stated:

The European Court of Justice handed down a judgment relating to the

UK's communications data regime in December. The matter must now be considered by the domestic courts and the consultation on the communications data code of practice has been deferred until this has taken place.

Part 3 of the Investigatory Powers Act 2016, which will replace those parts of the Regulation of Investigatory Powers Act 2000 (RIPA) which provide for access to communication data, has not yet come into force. Public authorities can continue to acquire data under RIPA and the associated Acquisition and Disclosure of Communications Data Code of Practice. The Retention of Communications Data Code of Practice, also published under RIPA, remains in place as published guidance and CSPs and the Secretary of State are expected to continue to follow the processes set out in that code until a new code is in force.

32. On 17th March 2017, the Home Office published on its Digital Marketplace that it was seeking:

Business change partner to supply service comprising project management, systems engineering, business analysts, business design, communications professional and PMO support for the deliver of the Investigatory Powers Act at work stream layer.

33. The budget range is £3,500,000 - £4,000,000.

34. In the 'about the work' section it states:

The passage of the Investigatory Powers Act has created significant business change impacts across government, law enforcement and intelligence agencies. The ECJ has recently upheld an appeal which challenges the current UK communications data retention and acquisition regime. This work package will provide a flexible dial-up / down support to the Home Office's delivery teams in designing and delivering business/IT change across impacted areas; setting requirements, coordinating change activities and contributing to/managing overall assurance of key products including business case, project plan, business system requirements, objective, benefits tracker, acceptance criteria, interface control documents, communications plans etc.

Workstreams already exist including law enforcement, the soon-to-be established Investigatory Powers Commissioner, and the ***independent communications data authorising body****. The two latter departments are initially the priority. These workstreams are at different levels of maturity and delivery will require business and IT design, business change and IT systems, planning, engagement with stakeholders and reporting.* **[emphasis added]**

35. The specification refers to the need for secure communications:

A number of stakeholders are impacted by delivery of the Act and require use of the systems and processes being delivered, e.g. to allow secure communication between public authorities and the Investigatory Powers Commissioner. Users include law enforcement agencies, government departments/public bodies, intelligence agencies, the Investigatory Powers Commissioner (IPC) and a new communications data independent authorising body.

36. In the 'Essential skills and experience' it includes *'Have experience of leading on complex IT system design and delivery with multiple user groups; Have experience of IT System Installation'.*

37. On the same date the Home Office published on its Digital Marketplace in relation to IP Act Implementation – Programme Layer, in 'About the work':

'The passage of the Investigatory Powers Act has led to significant business change impacts across government, law enforcement and intelligence agencies. A central team has been established to lead on the assurance of all elements of Act implementation. The primary focus is on legal compliance, involving more robust safeguards and a new oversight function. These requirements have led to significant business and IT change and substantial training across all impacted areas. This work package will provide support to the Home Office's implementation team; setting strategic requirements, coordinating and assuring planning and delivery of IP related change activities.

Implementing an Act of this nature is a challenging undertaking, creating change across the Intelligence sector, policing, public and local authorities. This requires significant direction and monitoring to ensure it is delivered within appropriate timescales without compromising public safety or operational purposes. There will be significant scrutiny internally, from parliament and the public. Implementing this work requires clear commissioning requirements and objectives, a comprehensive end to end design, ongoing monitoring, reporting and support, clear communication with bespoke engagement for each area and assurance from design through to post implementation review.'

'A wide range of stakeholders are impacted by the delivery of the Act and will require use of the systems and process being delivered i.e. to allow secure communication between public authorities and the Investigatory Powers Commissioner. These users include all law enforcement agencies, multiple government departments and public bodies, intelligence agencies, as well the Investigatory Powers Commissioner and new communications data independent authorising body itself. The users will employ provisions within the Act to support their ongoing capabilities and delivery will need to be managed without compromising operational objectives.'

38. It is further noted that work commenced in August 2016 and that *Significant*

work is required in the communications space – although the creation of a communications and lines to take pack has started [sic].

39. The Claimant notes that the collection and use of bulk communications data is disproportionate and therefore unlawful. The Claimant's submissions have been set out elsewhere and are not repeated here. In this statement, however, I also address the assertion by the agencies that they cannot comply with the judgment in *Tele 2 Sverige / Watson*.

Prior independent authorisation

40. The GCHQ witness notes that an independent authorising body would need:
    a. Secure premises;
    b. Electronic submission of queries;
    c. Understanding of technical complexity of queries;
    d. Understanding of systems on which the queries would be run;
    e. Details of datasets the systems contained;
    f. Facility by which authoriser can seek clarification via text of telephone;
    g. Specialist knowledge;
    h. Regular briefings on capabilities;
    i. Procedures for urgent and out of hours authorisations;
    j. Backup communication lines in case of interruption to authorising body's systems or communications networks; and
    k. Protection of information.

41. It is unclear why any of these requirements cannot be dealt with in the modern era where the agencies themselves will be using secure communications and where the independent authorising bodies will require specialist knowledge and technical support in the context of their other duties, which including authorising warrants for interception and equipment interference. Indeed, all of the above arrangements will be required now that all warrants will require prior judicial approval under the Investigatory Powers Act 2016.

42. The GCHQ witness suggests, at paragraphs 5, 18 and 42, that there could not be prior independent authorisation because it would slow down the process of analysis. However, no attempt has been made by the witness to consider what procedures could be put in place, and the Claimant notes the above specification on the Home Office Digital Marketplace. It is the Claimant's position that manageable procedures could be put in place.

43. Nor is there any difficulty in dealing with urgent applications. In such cases, accommodations can be made, as is recognised in the judgment of the Court of Justice in *Tele2 Sverige AB / Watson.*

44. Independent authorisation is effectively accomplished in other highly sensitive investigatory contexts, including during criminal investigations (prior authorisation has been needed for many years from the Surveillance

Commissioners for property interference and computer hacking by the police and NCA under the Police Act 1997). In other countries such as the United States, the FISA court approves warrant applications which again suggests that it could be made to work here.

45. In relation to security concerns, the GCHQ witness suggests at paragraph 19 that there could not be authorisation because this would widen the circle of knowledge. This is a ridiculous argument. There is no case in which approval from an oversight body has led to a security leak. Again, the Investigatory Powers Act 2016 requires independent authorisation for other sensitive operations such as interception and equipment interference. The same precautions that will be taken to protect sensitive information revealed during that process should be applicable to the authorisation of communications data requests.

46. With regard to describing queries to the independent authoriser, I note that if the query cannot be described adequately to the authorising person, it is difficult to see how it can be shown to be necessary and proportionate:
    a. Queries exist and have to be formulated to then be run singularly or iterated (repeated) over datasets;
    b. Datasets have to be identified in order to have queries run against them; and
    c. To run automatically against a number of databases, the system still has to be set up with the queries and datasets.

47. The GCHQ witness also fails to consider how internal and external auditing of queries, datasets and databases operates and how this can complement safeguards. It is therefore difficult to understand why this level of detail could not be provided to facilitate independent authorisation.

Notification

48. The GCHQ witness fails to engage with the notification requirement as articulated in the *Watson* judgment. The CJEU required notification where it is no longer liable to jeopardise the investigation being undertaken. If the intelligence agencies can legitimately explain why notification would jeopardise an investigation, it could be postponed. Otherwise, notification is necessary to enable those affected to exercise their legal remedies.

Resources

49. Paragraph 22 suggests that all safeguards will take away resources from the front line. This is, to a certain extent, true of any safeguard at all. The key is to implement all those safeguards that are required by law and to develop the most effective procedures possible to implement them.

Statement of Truth

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

Signed: 

Name: CAMILLA GRAHAM WOOD

Date: 2 May 2017