Claimant
G Danezis
Second
GD-2
17 April 2019

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Claim No: CO/1052/2017

B E T W E E N:

THE QUEEN
on the application of
THE NATIONAL COUNCIL FOR CIVIL LIBERTIES

Claimant

- and -

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(2) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

Defendants

SECOND WITNESS STATEMENT OF GEORGE DANEZIS

I, **GEORGE DANEZIS**, Professor in the Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom, will say as follows:

1 I have made one previous statement in these proceedings dated 29 June 2018 (my "**First Statement**").

2 I make this statement in support of the claim brought by the Claimant, Liberty, challenging powers under the Investigatory Powers Act 2016 (the "**IPA**") to respond to two matters raised in the Defendants' evidence and pleadings.

3 I am authorised by Liberty to make this statement. I am not authorised to, and I do not by anything said below, waive any privilege on behalf of Liberty.

4 The contents of this statement are within my knowledge, save where I indicate otherwise. 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 they are true to the best of my knowledge and belief.

5 My employment and experience remains as set out in my previous statement, save that I now work at Facebook Inc in London, UK, and retain my professorship and a 20% appointment at University College London in the Department of Computer Science. My evidence reflects my own experience, knowledge and views. I make this statement in a personal capacity. I do not, and should not be taken, to speak on behalf of my employers.

6 There is now produced and shown to me, and I exhibit, a consecutively paginated bundle of documents marked "**GD-2**", divided into various tabs, containing the documents to which I refer. I refer to these documents in the format **[GD-2/*x*]** where "*x*" is the page number.

7 I have been provided with, and have reviewed, the Defendants' witness statements dated 4, 5 and 6 February 2019 and their exhibits.

8 In this statement I address:

(1) the expansive interferences with privacy that can be achieved by exercise of thematic and bulk hacking (equipment interference) powers, which the Defendants' evidence appears significantly to understate; and

(2) comments made in the Defendants' evidence about concepts used in the IPA.

9 I should not be taken to agree with anything in the Defendants' evidence because I do not address it here.

EXTENT OF INTERFERENCES FROM THEMATIC AND BULK HACKING POWERS

10 **Dix 1 ¶¶54 and 58** purports to summarise the targeted and thematic hacking powers and the bulk hacking powers under the IPA. He says that he is giving a "brief overview" of these powers: **Dix 1 ¶51.**

11 Mr Dix's "brief overview" may be inaccurate in part. It also omits to mention:

(1) ways in which hacking powers are even wider, and thus interfere with privacy to an even greater extent, than bulk interception powers and powers to obtain bulk communications data; and

(2) the additional dangers of hacking powers as compared with interception powers, which again expand the extent of the interference with privacy they create.

12 I address these points below.

The extent of the interference under hacking powers

13 Bulk and thematic hacking warrants under the IPA enable the United Kingdom Government to "secure interference with any equipment" for the purpose of obtaining any information (see sections 99(2) and 176(1)(b)), although they are subject to further limits. The powers may not be used to authorise interception of communications in transmission from the United Kingdom, which must instead be done under targeted or bulk interception powers: sections 3(1), 99(6) and 176(6).

14 Mr Dix is correct to say at **Dix 1 ¶182** that equipment interference "provides insight, intelligence, investigative and evidential opportunities into a suspect's digital life", which he says is its first "operational benefit".

15 However, Mr Dix does not explain the greater intrusion of hacking powers into privacy than that enabled by bulk interception powers.

16 Equipment interference allows:

(1) Access to any electrical device, even if it is not connected to any public (or other) telecommunications network;

(2) Access to a person's information on any electrical device, even if that person has never themselves chosen to transmit it across the internet or any other telecommunications network, for example, photographs, diary entries, notes and other files; and

(3) The remote control of devices (as **Dix 1 ¶180** acknowledges), for example, enabling a mobile phone with a camera to record and transmit anything it picks up back to the United Kingdom government.

17 The power to gain remote control of devices is particularly significant: it enables, for example, the carrying out of any operations on a terminal device (say a mobile phone, laptop or Apple Watch, or smart home devices such as Alexa) remotely (such as switching a camera or microphone on or off or removing or altering data), keylogging (so that passwords say to decrypt files or access email/online accounts, as well as any other

information entered, can be recorded and sent to a recipient), access to cryptographic keys used to protect data at rest (such as in backup tapes) or in transmission, and alteration of network infrastructure (for example, the routers that determine how communications are set over the internet, as I explained in paragraphs 25–26 of my First Statement, so that communications that pass through them can be (more easily) intercepted).

18 An example of the remote control that can be achieved via equipment interference occurred in 2004–05 in Greece. Inbuilt subsystems that can be used for lawful interception were activated remotely in several Vodafone mobile network routers, so that they would send the contents of intercepted calls to "shadow phones" for a group of phone numbers: see my translation of the February 2006 Greek government press conference explaining this **[GD-2/1–7]**.[1] The phone numbers that were tapped in this way included those of the Greek Prime Minister.

19 Further, the power to access stored data is meaningfully wider than the power to intercept data in transmission: it enables data to be retrieved when it has never been transmitted over a public network. This can be especially invasive if the stored data of service providers that maintain regular backups were accessed, as this would allow access to information that users may have "deleted" from the primary service.

20 The powers are therefore significantly more intrusive than those for bulk interception. They are not limited to authorising interception only at the point where a person choses to use a public telecommunications network (or a communication is stored in such a network). Instead, they may authorise any other kind of "interference" with electronic equipment of any kind.

21 **Dix 1 ¶58** appears to imply that <u>all</u> data captured via equipment interference "[h]istorically ... may have been available during its transmission through bulk interception". That is, however, incorrect. As just explained, the thematic and bulk equipment interference powers under the IPA allow the state to access information that <u>was not</u> actually intercepted when it was transmitted and, more importantly, <u>has never</u> been transmitted. This is implicit in Mr Dix's description of examples of equipment interference at **Dix 1 ¶¶181–182**.

---

1 This is available at <https://web.archive.org/web/20060627195712/http://homes.esat.kuleuven.be/~gdanezis/intercept.html>.

22 I note that **Dix 1 ¶58** says that bulk hacking "involves the acquisition of communications and equipment data directly from computer equipment overseas" (emphasis added). I am not a lawyer (nor is Mr Dix), but that appears to understate the scope of the bulk hacking power.

23 Under sections 176(5) and 178(1)(a) of the IPA, as long as the "main purpose" of the warrant is to obtain "overseas-related communications", "overseas-related information" or "overseas-related communications data", the conduct authorised by the warrant may include the obtaining of information from (or other interference with) equipment in the United Kingdom if necessary. I note that **Dix 1 ¶225** more accurately explains the scope of bulk hacking warrants, although he does not mention that interference with domestic devices may be permitted.

The additional dangers of hacking powers for individual privacy

24 **Dix 1 ¶182** indicates that the second "operational benefit" of equipment interference is that "when combined with other warranted investigative powers, such as lawful interception, it provides a wider range of tools to access the communications of criminals that might otherwise be out of reach of traditional interception".

25 This is somewhat obscure. But Mr Dix seems to be saying that equipment interference enables the United Kingdom government to crack or altogether bypass encryption or other security that otherwise would make the contents of communications inaccessible when they are intercepted under bulk (or targeted) interception powers.

26 Mr Dix does not refer to the inherent dangers that any form of hacking presents, namely, that (1) any exploit or vulnerability must pre-emptively be placed, or on being discovered allowed to remain, on all devices or in all instances of software to be effective (even if it is desired to use the exploit or vulnerability only in particular cases), (2) states and actors other than the United Kingdom government may discover and take advantage of the exploits and vulnerabilities, and (3) this can have with far-reaching and disastrous consequences, including, for example, the proliferation of know-how and vulnerabilities that place the online security of innocent internet users in danger. (I explain this in more detail in paragraphs 31–32 below.)

27 I note also that Mr Dix does not at any point in his evidence mention that the United Kingdom government has publicly suggested it uses bulk hacking powers in ways that give rise to these dangers. I explain this immediately below.

28 GCHQ's Technical Director of the National Cyber Security Centre and its Technical Director for Cryptanalysis said in a November 2018 blog post **[GD-2/10]**:

> "Under UK law, government has the power to authorize Equipment Interference. That includes everything from covertly entering a suspect's house to copy data through to more technical things like 'lawful hacking.'"

29 They argued for five principles, the first of which was **[GD-2/9]**:

> "Privacy and security protections are critical to public confidence. Therefore, we will only seek exceptional access to data where there's a legitimate need, that access is the least intrusive way of proceeding and there is appropriate legal authorisation."

This "principle" restates some of the requirements that must be met for a bulk hacking warrant under the IPA.

30 The senior GCHQ staff also explained one way of bypassing encryption of the kind that exists, for example, in software such as WhatsApp,[2] a very popular messaging platform marketed to its users as offering end-to-end encryption (that is, encryption that the software maker of WhatsApp cannot itself break and that only the two devices on either "end" of the communication can decode). They said **[GD-2/11]**:

> "In a world of encrypted services, a potential solution could be to go back a few decades. It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call. The service provider usually controls the identity system and so really decides who's who and which devices are involved — they're usually involved in introducing the parties to a chat or call. You end up with everything still being end-to-end encrypted, but there's an extra 'end' on this particular communication. This sort of solution seems to be no more intrusive than the virtual crocodile clips that our democratically elected representatives and judiciary authorise today in traditional voice intercept solutions and certainly doesn't give any government power they shouldn't have.
>
> We're <u>not</u> talking about weakening encryption or defeating the end-to-end nature of the service. In a solution like this, we're normally talking about suppressing a notification on a target's device, and only on the device of the target and possibly those they communicate with. That's a very different proposition to discuss and you don't even have to touch the encryption." [original emphasis]

---

2 WhatsApp is owned by Facebook, my current employer. I do not in my role have access to any non-public information about WhatsApp relevant to this statement.

31 Bruce Schneier, a US security technologist who is a Fellow at the Harvard Kennedy School of Government and now advises IBM Security, responded on 17 January 2019 as follows **[GD-2/12]**:

> "Basically, making this backdoor work requires not only changing the cloud computers that oversee communications, but it also means changing the client program on everyone's phone and computer. And that change makes all of those systems less secure. Levy and Robinson [the senior GCHQ staff] make a big deal of the fact that their backdoor would only be targeted against specific individuals and their communications, but it's still a general backdoor that could be used against anybody.
>
> The basic problem is that a backdoor is a technical capability — a vulnerability — that is available to anyone who knows about it and has access to it. Surrounding that vulnerability is a procedural system that tries to limit access to that capability. Computers, especially internet-connected computers, are inherently hackable, limiting the effectiveness of any procedures. The best defense is to not have the vulnerability at all." [emphasis added]

32 Mr Schneier's explanation of the dangers of hacking powers reflect the standard understanding in academia and the professional computer science world of hacking and exploitation of vulnerabilities (known in the industry as the "kill chain" and originally developed by the United States aerospace and defence company Lockheed Martin), which comprises the following steps:

(1) **Step 1:** Conducting reconnaissance in relation to the target, using metadata to understand the programs, locations and media it is using;

(2) **Step 2:** Deploying an exploit so as to gain access to this (and any other similar) system and then elevate privileges so the hacker can take over;

(3) **Step 3:** With those privileges, inserting something that enables the hacker to continue to have a presence in the system (that is, to take over whenever it wants to do so, without having to repeat the steps above); and

(4) **Step 4:** Deploying a payload, which carries out the functionality that is ultimately desired (for example, adding an "end" to communications via WhatsApp that cannot be seen by the users, encrypting files until a ransom is paid, or sending keystrokes or other data back to a recipient).

33 Mr Schneier discusses the dangers resulting from security services inserting vulnerabilities into software to facilitate equipment interference. However, there are also dangers in exploiting "pre-existing" vulnerabilities or exploits in software and hardware. Pre-existing vulnerabilities and exploits such as these are on occasion discovered by GCHQ or other intelligence services and can be used for the purposes of equipment interference (in Step 2 above), if they are kept secret and not disclosed to hardware and software vendors to be patched (that is, fixed by a software or firmware update).

34 GCHQ in November 2018 published its "Equities Process" **[GD-2/15]**.[3] Mr Dix does not refer to this document. It explains GCHQ's policy on when it will disclose a pre-existing vulnerability to a vendor and when it will keep such an exploit or vulnerability secret. It states that "[t]he starting position is always that disclosing a vulnerability will be in the national interest", but also indicates that, if GCHQ decides that there is "a clear and overriding national security benefit in retaining a vulnerability" having regard to "possible remediation", "operational necessity" and "defensive risk", GCHQ will suppress and may itself use the vulnerability or exploit **[GD-2/15–16]**. The Equities Process also indicates that GCHQ will not apply the process in that document (and, it seems, will keep secret and use a vulnerability or exploit) when it has "already been subjected to similar considerations by a partner and shared with us", where the software or server design is inherently vulnerable, or "where the software in question is no longer supported by the vendor". The last of these is a potentially wide exception, because older versions of operating systems (such as Windows XP) are no longer supported by vendors but frequently used for important infrastructure, medical devices or industrial control devices and have many vulnerabilities.

35 In addition, when any (pre-existing or newly created) exploit is deployed, there is an inherent danger that a target may identify it, analyse it, reverse engineer the exploit, and then use it to their own advantage in order to attack other systems, including in the UK. Equipment Interference based on exploiting technology inherently suffers from the danger of proliferation of attack know-how and techniques, which lowers the security of computer systems and networks as a whole.

36 **Dix 1 ¶17** gives as an example of the dangers faced by the United Kingdom the "Wannacry" exploit. As Mr Dix rightly says, this was an "indiscriminate ... cyber-attack in 2017 [that] affected many individuals and organisations, including the National Health Service". The exploit targeted old and unpatched versions of the Microsoft Windows

---

3 This is available at <https://www.gchq.gov.uk/information/equities-process>.

operating system (including Windows XP and Windows Server 2003), which are commonly loaded (in a way that cannot in practice be updated) onto important infrastructure, such as medical hardware. As was widely reported at the time, it encrypted files unless a ransom in bitcoin was paid.

37 I am surprised that Mr Dix gives this example. He omits to mention that the vulnerability that enabled the "Wannacry" attack was widely reported and believed within the industry to have been discovered and concealed by the United States National Security Agency ("**NSA**") — GCHQ's United States counterpart — then stolen from the NSA, released publicly, and used by the hackers who carried out the attack. Microsoft's President, Brad Smith, said in response: "We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. ... We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits." **[GD-2/22]**

38 This is therefore exactly the kind of risk that the existence and use of bulk hacking powers under the IPA — and the approach advocated by the senior GCHQ staff — creates. If the United Kingdom carries out hacking under Part 5 or Part 6 Chapter 3 of the IPA, it is entirely possible that existing vulnerabilities or exploits, or those the United Kingdom creates, may come to be used by third parties for malicious ends.

39 In addition, it would not be necessary for the exploit to be "stolen" from or "leaked" by the United Kingdom intelligence services for third parties to take advantage of it. It is possible for an actor with the required technical capability (there are many) to identify the code giving effect to an exploit or vulnerability, for example the exploit suggested by the senior GCHQ staff mentioned above, if this were rolled out in an update to (say) a popular mobile app such as WhatsApp.

40 The consequences of these risks include that third parties (such as other states or malicious actors) may obtain, alter and use an individual's data without that individual or the United Kingdom government knowing. They also include potentially far reaching and devastating effects on infrastructure, such as the "Wannacry" attack.

41 I believe that, in considering the privacy implications of bulk hacking powers under the IPA, it is important to take into account these additional risks.

CONCEPTS USED IN THE IPA

42 I wish to respond to some observations Mr Dix makes about concepts used in the IPA that relate to my previous statement.

The limited nature of "selection for examination" (and safeguards that follow on it) as explained by Mr Dix

43 It seems from **Dix 1 ¶55** that the United Kingdom government takes the view that "selection for examination" under the IPA occurs only when an actual person searches for and retrieves data that has been collected via bulk warrants or authorisations. I take this from Mr Dix's references to the safeguards that apply "[b]efore an analyst can select for examination any data obtained under a bulk warrant" (my emphasis).

44 That indicates that the safeguards that apply to selection for examination, in particular the requirements for targeted examination warrants where data is selected for examination using criteria referable to a person known to be in the British Islands for the purpose of identifying their communications or other information, do not constrain any of the processing of data that occurs before an analyst seeks to examine data.

Secondary data and significant intrusion of electronic processing

45 In paragraphs 99–100 of my First Statement, I explained certain kinds of information that, in my experience, could readily be derived from the content of communications by automated processes that are sometimes assisted by machine learning. Mr Dix's response to my evidence in paragraphs 203–205 of his statement is confused.

46 It seems that Mr Dix does not disagree with my analysis but instead seeks to qualify it. He appears to be trying to say (**Dix 1 ¶203**) that, if it is necessary for a person to examine content to derive information that could on its own be considered "secondary data", then this would be subject to the safeguards that attach to "selection for examination". For example, he says: "*Taking the example of the language a person speaks being secondary data, if you needed to read the text of an email or listen to a call to establish the language than this would not be within the scope of secondary data.*"

47 It is obvious that, if a person must look at content, then the safeguards for "selection for examination" ought to apply. However, this does not answer the point I made in my First Statement, which was that:

(1) information of the kinds I identified, such as the language a person speaks, the names of the people who are communicating and their future locations and events, the nature of their relationship, and details of financial transactions, potentially reveals a great deal about a person; and

(2) this information can now reliably be derived from content automatically and without a person looking at an email or listening to a conversation.

48 If automated processing of this kind occurs, the results would be "secondary data" under the IPA.[4] I believe Mr Dix accepts this (see **Dix 1 ¶203**). He expressly accepts (as I have explained above) that the requirement of a targeted examination warrant applies only where content is "selected for examination" by a person, not before that point.

49 In addition, under the IPA, secondary data can be selected for examination without the safeguard of a targeted examination warrant under any circumstances, including where criteria referable to a person known to be in the British Islands in order to identify their communications or information: see sections 152(1)(c) in relation to bulk interception and section 193(1)(c) and 193(9) for bulk hacking warrants.

50 I have been provided with the Defendants' Detailed Grounds of Resistance dated 5 February 2019. Paragraph 78(7) of that document states:

> "The above workable and sensible distinction [between "content" and "secondary data"] does not permit extraction of secondary data from content under some supposedly 'wide and intrusive process'. Any meaningful intrusion into privacy rights occurs at the stage when content or secondary data is selected for examination."

51 I do not understand the first sentence of this statement. I am not aware of any safeguard that prevents extraction of secondary data that I have explained above to be technically possible and potentially highly intrusive. Indeed, Mr Dix again seems to agree that such data can be intrusive, at least in general: he accepts that "certain categories of non-content data, including certain categories of secondary data, can be more intrusive than the least intrusive content" (**Dix 1 ¶208**).

52 The second sentence quoted above, that any meaningful intrusion occurs only where content or secondary data is selected for examination (read, listened to or viewed) is in my view incorrect. This is so for the following reasons:

---

[4] I do not know whether the United Kingdom security and intelligence agencies carry such analysis out, but it is technically possible, as I previously explained.

(1) First, the process that defines what can be "selected for examination" (which Mr Dix does not explain at all) effectively determines the extent of the "meaningful intrusion" into privacy that Mr Dix accepts to occur at the point of "selection for examination". It is artificial to divide up that process and to argue that the stages that lead to examination by an individual are not a "meaningful" interference with privacy. The automated processing applied is determined by people, namely, the UK intelligence services. The UK intelligence services decide the algorithms, selectors or other search criteria that are applied, which determine the data available to analysts. They have discretion as to how this is done, which may be exercised, for example, to carry out forms of profiling. The process happens entirely in secret, and all parts of it contribute to interference in privacy.

(2) Secondly, processing power and machine learning are now such that it is technically possible to extract sensitive personal information without ever looking at the underlying intercept material, that is, without any "selection for examination" of content or secondary data. As mentioned, I gave as examples of the kind of information that can be extracted language spoken, people with whom someone communicates, the nature of their relationship, financial transactions and future locations and events. A further example is that it is technically possible, using machine learning (with greater or lesser ongoing human input), to identify patterns in data of specified individuals and then to seek to identify other people who exhibit similar patterns. The output of this could be a list of names or other hard selectors linked to individuals. It would not be necessary for any analyst to look at any of the underlying data at any point. They would simply see the names or selectors related to individuals whose patterns were identified. Given the rich information contained in communications data and content, this might include physical locations (say proximity to a mosque, temple or church), people or servers communicated with, words, languages and media used, times and dates of communications, and financial transactions, to name just a few. Remarkably, according to the Defendants, there would not be any "meaningful" interference with privacy at all in such a situation, because there is no selection for examination (that is, reading, listening to or viewing) of the underlying material. I find that suggestion concerning.

Overseas-related communications, information and equipment data

53 I explained in paragraphs 87–95 of my First Statement that, because of the way in which the internet works and because of the limited information contained in a packet and technologies that can be used to obscure location, it is difficult to say that the purpose

of intercepting a certain bearer or set or bearers is to obtain overseas-related communications.

54 Mr Dix responds at **Dix 1 ¶¶195–199** but does not:

(1) disagree or otherwise challenge my technical explanation; or

(2) explain that in fact this can be or is done in a meaningful way.

55 Instead, Mr Dix quotes two paragraphs from the Interception of Communications Code of Practice and refers to safeguards at the point of "section for examination" (which are not relevant to this issue). However, that the Code of Practice purports to impose a requirement to "keep[] the interception of communications that are not overseas-related to a minimum", to quote Mr Dix (**Dix 1 ¶198**), does not somehow show that it is meaningfully possible in practice to do so. I have explained why it is not.

56 Mr Dix does not explain how the UK determines whether the "main purpose" of a bulk hacking warrant is to obtain "overseas-related communications", "overseas-related information" or "overseas-related equipment data", as required under section 176(1)(c) of the IPA. Depending on the interpretation, this may also set such a low bar as not to limit on the scope of the power in practice.[5] The International Telecommunications Union estimated in 2015 that 3.2 billion people have internet access **[GD-2/23]**.[6] The UK Office of National Statistics estimated the UK population to be around 63.2 million in 2011 **[GD-2/29]**,[7] of whom a proportion have internet access. If the main purpose of a warrant is gauged by the number of devices affected overseas versus domestically, the "main purpose" of any warrant that authorises an exploit such as that described by the senior GCHQ officers mentioned above (an exploit in a popular app or operating system used globally) will be to obtain overseas-related information, communications or equipment data. That will be so even where the conduct affects all or most UK internet-connected devices.

57 Finally, Mr Dix says in **Dix 1 ¶195 footnote 20** that the definition of "overseas-related communications" "excludes, for example, an individual in the UK doing a Google search where the server they are communicating with is overseas".

---

5 I do not know how the UK intelligence services in fact make this assessment.

6 This estimate is available at <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>.

7 This is available at <http://www.ons.gov.uk/ons/dcp171778_292378.pdf>.

58 This means that a communication sent from the UK is not "overseas-related" under the IPA unless the UK government can identify an individual who is overseas who receives it, and a communication sent from outside the UK is not "overseas-related" unless the UK can identify an individual as sender or recipient. Virtually all web-browsing does not involve any individual receiving the communications sent by the person browsing. Accordingly, the UK government's current approach, virtually all web-browsing does not involve "overseas-related communications".

59 It seems that this is a change in position under the IPA.

60 I have been provided with and reviewed a copy of the Witness Statement of Charles Blandforth Farr dated 16 May 2014,[8] made in proceedings in the UK Investigatory Powers Tribunal, which relates to bulk interception warrants under section 8(4) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). The statement includes the following:

> "133. A person conducting a Google search for a particular search term in effect sends a message to Google asking Google to search its index of web pages. The message is a communication between the searcher's computer and a Google web server (as the intended recipient). The Google web server will search Google's index of web pages for search results, and in turn send a second communication — containing those results — back to the searcher's computer (as the intended recipient).
>
> 134. Google's data centres, containing its servers, are located around the world; but its largest centres are in the United States, and its largest European centres are outside the British Islands. So a Google search by an individual located in the UK may well involve a communication from the searcher's computer to a Google web server, which is received outside the British Islands; and a communication from Google to the searcher's computer, which is sent outside the British Islands. In such a case, the search would correspondingly involve two 'external communications' for the purposes of section 20 of RIPA and paragraph 5.1 of the Code.
>
> 135. Similarly, a computer user in the British Islands searching for a video posted on YouTube will in effect send a communication to YouTube's website to ask it to give him the results of a particular search; which means that he communicates with a YouTube web server; and the web server, in tum, communicates back to him the results of the

[8] This is available at <http://privacyinternational.org/sites/default/files/2018-03/2014.05.16%20Witness%20Statement%20of%20Charles%20Blandford%20Farr.pdf>.

search that he has made. Whether or not those communications are 'external' will depend upon where the web server used by You Tube is located. ...

137 Thus a user located in the British Islands posting a message on Facebook will communicate with a Facebook web server, located in a Facebook data centre. If the [F]acebook data centre is outside the British Islands, then the message will be an 'external communication'. ..."

61 This indicates that, under RIPA, the UK government's position was that a communication with an overseas server was, without more, an "external communication",[8] so bearers containing such communications could be intercepted. The equivalent concept in the IPA is "overseas-related communications" (in sections 136(3) and 176(2)) and "overseas-related information" and "overseas-related equipment data" (in section 176(2)–(3)).

62 Mr Dix's evidence, as set out above indicates, that the UK government takes the position that communications with an overseas server are not (without more) "overseas-related communications" under the IPA.

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

Signed: [redacted]

Date: 17 April 2019

Name: George Danezis

[8] The equivalent concept under RIPA was "external communications", which were defined in section 20 as "a communication sent or received outside the British Islands". Under section 8(4) of RIPA, the requirements in section 8(1)–(2) requiring one person or set of premises as the interception subject, and to schedule the factors to be used to identify the communications to be intercepted, did not apply if, amongst other things, the description of the communications to which the warrant related confined the authorised conduct to the interception of "external communications' and other conduct necessary to what the warrant authorised