Defendant
G Biggar
GB-1
31 January 2018

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

CO/1052/2017

THE QUEEN on the application of

LIBERTY

Claimant

v.

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

Defendants

WITNESS STATEMENT OF GRAEME BIGGAR

I, Graeme Biggar, of the Home Office, 2 Marsham Street, London SW1P 4DF, will say as follows:

1. I am Director, National Security, within the Office for Security and Counter Terrorism in the Home Office. Policy and legislation concerning investigatory powers, including communications data, sit within my area of responsibility. I have held this position in the Home Office since July 2016 and have been a senior civil servant for 11 years.

2. I make this statement on behalf of the Defendants, the Secretaries of State for the Home Department and for the Foreign and Commonwealth Office. The purpose of the statement is to respond to certain matters raised in the witness statement of Corey Stoughton on behalf of the Claimant, and to support the Defendants' defence of the claim. This witness statement is supplemental to that of Andrew Scurry.

3. Save where otherwise stated, all facts and matters referred to in this statement are true and within my own knowledge or have come to my attention during the course of my work. Insofar as facts or matters are not directly within my knowledge they are true to the best of my knowledge and belief.

4. Documents to which I refer in this statement are exhibited in the bundle marked 'GB1'. Page references below are to that exhibit.

Communications data and content

5. Ms Stoughton concludes her statement by implying that the Government does not consider that the retention of and access to communications data is intrusive. This is not the Government's position. The Government acknowledges that any retention or acquisition of data relating to a person's communications involves some degree of interference with that individual's privacy. However, the specific level of intrusion will depend on what data is retained or acquired, and in what circumstances.

6. The suggestion in para 7 of Ms Stoughton's witness statement that communications data produces a deep and comprehensive understanding of a person's life would appear to be predicated on the basis of the entirety, or at least a significant proportion, of a person's communications data being acquired and examined over an extended period of time. Any form of personal data, if acquired over a significant period and examined in its entirety may enable similar conclusions to be drawn and communications data is not unique in that respect. I agree that examination of communications data on this scale would be significantly intrusive, but I also consider it highly unlikely, except in the most extreme circumstances, that the acquisition of such data from a service provider would be authorised, because it would not be considered necessary and proportionate.

7. Ms Stoughton goes on to say that communications data can be more revealing than content: but that is not a fair comparison. The content equivalent on a "like for like" basis to the acquisition of the volumes of communications data postulated by Ms Stoughton would be a public authority intercepting the entirety or significant proportion of a person's communications over an equivalent period of time and

examining everything that a person said in a phone call, email, letter, text and the content of every single web page that person viewed online during that period. I consider this would be much more intrusive.

8. In paragraph 8 of her statement Ms Stoughton explains how she considers that it is difficult to separate communications data from the content of communications. She rightly points out that the definition of content explicitly excludes inferred meaning. This, in my view, is entirely appropriate as the definition of the content should only include information which makes up the content of the communication itself.

9. To give an example, one could infer, from the fact that a person has telephoned their manager at work, that they are seeking to discuss work related issues. The inference may or may not be correct: the telephone call could equally concern discussion of a lunch engagement between two friends. The inference is a matter of speculation (whether accurate or inaccurate) from the fact of the communication itself, not something that derives from what was said on the telephone call. Put simply, the inference that could be drawn is not, and cannot reasonably be considered to be, the content of that communication and is therefore rightly excluded.

Web pages and internet connection records

10. Ms Stoughton's witness statement at paragraphs 10-13 misunderstands the effect of paragraphs 2.64-2.65 of the Draft Communications Data Code of Practice ("the Draft Code"). The Draft Code published in November 2017 is not intended to have a different effect to the version published in 2016: indeed, the definition of an internet connection record is set out in the Act and has not changed. The purpose of the code is to explain how this definition applies in practice. Communications data will still not include a list of all web pages visited.

11. The Draft Code explains that those parts of a web address (otherwise known as a "uniform resource locator", or URL) which are used to route a communication to the intended recipient are "communications data". Other parts of the web address, not necessary to route the communication, are not communications data. The Draft Code indicates at paragraphs 2.64 and 2.65 that the parts of the web address which are not

necessary to route the information include the *"path and optional parameters, which are similar to a file path on a computer. For example, in "socialmedia.com/profile/home", the path is "profile/home"*. In other words, in this particular example, the fact that a person had visited (say) Facebook would be communications data; but the identity of the person whose profile they had visited, and the pages they had visited within that profile, would not be communications data. That is because, in this example, the "profile/home" elements of the web address would not have been used to route the communication concerned.

12. Any amendments to the internet connection record provisions in the code of practice published for consultation on 30 November 2017 were for clarity, rather than representing any change in the Home Office's position as set out in the previous Draft Code from November 2016.

13. The Government's Operational Case for the retention of internet connection records, published in 2015 and revised in 2016[1], sets out in more detail an explanation of what an internet connection record is: see GB1/1. It is consistent with the position I have set out above. For instance, it explains at page 7 that an internet connection record will only identify the service that a customer has been using: it is not intended to show what a customer has been doing on that service.

14. Ms Stoughton refers at paragraph 14 to David Anderson QC's position on internet connection records in June 2015. However, the way she describes his position is misleading. In his report *"A Question of Trust"* he said that the Government should not proceed with the policy until an operational case has been made. He did not say that no such case existed.

15. Following the publication of his report, the Government published the Operational Case for internet connection records in 2015 (the 2016 version of which is exhibited to this statement). David Anderson subsequently said to the Joint Committee on the Draft Investigatory Powers Bill (see GB1/2 at page 36):

[1]The Government accepted the recommendations of the Joint Committee on the Draft Investigatory Powers Bill as to the retention of internet connection records, and revised the Operational Case accordingly.

David Anderson: *"The Government have produced a 24-page operational case, as I recommended they should. I did not recommend 24 pages, but they have produced an operational case. They made out their case for three reasons why the police and others might want that information. That is now free for committees to interrogate, and no doubt you have started that process already"*.

16. The Joint Committee concluded that: *'We consider that, on balance, there is a case for Internet Connection Records as an important tool for law enforcement.'* (See GB1/3 at page 39). They also concluded that the purposes for which internet connection records can be acquired should be extended beyond the three that were originally set out in the Operational Case, as published in 2015:

> *'We agree that all of the proposed purposes for which access to ICRs could be sought are appropriate. Furthermore, we recommend that the purposes for which law enforcement may seek to access ICRs should be expanded to include information about websites that have been accessed that are not related to communications services nor contain illegal material, provided that this is necessary and proportionate for a specific investigation.'*

17. The Government accepted this recommendation.[2]

Events data and entity data

18. At paragraphs 29 to 31 of her statement, Ms Stoughton asserts that data concerning all mobile phone applications, or "apps," that an internet service subscriber has installed on their phone will constitute entity data in relation to that subscriber. That assertion is wrong. More specifically, it is made in reliance on an incomplete quotation from the Draft Code of November 2017, which gives a misleading impression. Ms Stoughton says that information about apps on mobile phones is "entity data" for the purposes of the Draft Code, because such data includes *"the services...to which the owner of the devices subscribes"*. The full quotation from the Draft Code (see para 2.24) is: *"An entity (see below for further details) can also include devices so this data would cover information*

[2] The Government then published a revised Operational Case for the retention of internet connection records in 2016 that covered the extended purpose: see fn 1 above.

about the devices owned by a customer as well as the services provided by the telecommunications operator to which the owner of the devices subscribes" (emphasis added).

19. The apps on any one device are likely to be provided by multiple companies. There is no reason why the telecommunications operator to which the owner of the device subscribes would have any list of those apps. For instance, a mobile network operator would have no reason to know that a subscriber had apps on their device provided by MailOnline, or the Guardian, or NatWest (to use Ms Stoughton's examples), or a host of other possible app providers, other than the operator themselves; and information about such apps would not be "entity data". Those apps would not concern services provided by the telecommunications operator, but services provided by MailOnline, the Guardian, or NatWest, as the case may be. Nor, indeed, would entity data include data concerning a communications app not provided by the telecommunications operator themselves (for example, WhatsApp, which is owned by Facebook).

20. Services to which the owner of a relevant device subscribes would amount to entity data where, for example, the customer of a mobile network operator also subscribes to home broadband and fixed line telephony with the same operator.

21. Similarly, at paragraph 32 of Ms Stoughton's statement she addresses passwords retained by telecommunications operators. Paragraphs 2.41-2.42 of the Draft Code set out specific restrictions on when passwords can be obtained. Furthermore, the retention of passwords by telecommunications operators is very rare, and best practice guidance issued by the Information Commissioner's Office is that passwords should not be stored at all by telecommunications operators. Accordingly the purpose of the Draft Code in this respect is to make clear that in the rare circumstances where such data might be available from an operator, additional protections apply.

Retention notices

22. As Mr Scurry has explained, only a very limited number of providers are subject to data retention notices and only in respect of certain services. Ms Stoughton's witness statement appears to suggest that the Government start from a position that all data must be retained by the provider concerned, and then only put limited restrictions on

retention in restricted circumstances. I can say from my direct knowledge that this is certainly not the case. Personnel in my team are responsible for providing advice to the Secretary of State on whether, and in what form, to give data retention notices. We need a compelling evidence base before we would consider recommending a retention notice at all, and always focus on ensuring that the notice is circumscribed to the maximum extent consistent with achieving its intended aim. In practice, retention notices simply do not operate in the way Ms Stoughton suggests. For example, when we are proposing the retention of a new type of data by a provider we will start by recommending retention of only a limited amount of data to determine the level of value it provides to law enforcement; and will recommend extension of the scope of retained data only if necessary and proportionate to do so. Equally, we will revoke the requirements where they are not providing value, and are accordingly not necessary and proportionate.

Error reporting

23. Ms Stoughton addresses error reporting at paragraphs 39-42 of her statement. The provisions of the Act concerning error reporting need to strike a balance between the private interest of the affected individual and the public interest of maintaining national security. They seek to do so by ensuring that an individual is only informed when they have suffered as a result of the error and so could potentially be entitled to a remedy for the harm that they have endured.

24. Ms Stoughton complains at paragraph 40 of her witness statement that individuals do not have the opportunity to scrutinise, or challenge, *"the State's determination about what constitutes a "serious error""*. I should observe that under section 231 of the Act any decision as to whether an error is "serious", and whether it is in the public interest that the individual is informed of it, is to be taken by the independent Investigatory Powers Commissioner, not the Government. The Investigatory Powers Commissioner must be a person who holds or has held high judicial office within the meaning of Part 3 of the Constitutional Reform Act 2005: see section 227 of the Act.

25. The new serious error reporting regime is not expected substantially to alter the circumstances in which individuals are informed of errors. The last Interception of

Communications Commissioner, Sir Stanley Burnton, addressed the effect of the new error reporting regime in the Act at page 19 of his Annual Report for 2016 (under the section of his report headed "Serious Error Investigations"). He stated (see GB1/4 at page 44):

"Importantly, under the Investigative [sic] Powers Act 2016, there will be a change in the thresholds regarding when the Investigatory Powers Commissioner can inform an individual. Section 231 of the Act requires the Commissioner to inform a person of any relevant error where they consider it is serious and in the public interest for that person to be informed. The Commissioner is not permitted to determine that a matter is serious unless they conclude that the error has caused significant prejudice or harm to the person concerned.
Whether this will have an impact on the numbers of persons being informed of serious errors is difficult to judge. Under the existing regime, all occasions on which I have notified individuals of an error were cases in which they had suffered significant prejudice or harm (such as being arrested) and so would be covered under the new Act." (Emphasis in final paragraph added).

26. As to paragraph 44, the Government does not agree that Liberty's concerns about the IPT, as set out in its Observations in *10 Human Rights Organisations v United Kingdom*, have any substance. Rather than addressing those concerns in this statement, I annexe to this statement at GB1/5 a copy of relevant sections of the Government's Response in the *10 Human Rights* claim: the Response addresses the points made in Liberty's Observations at §§7.36-7.50 (at pages 69-75) in particular.

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

Signed: [redacted]

Dated: 31st January 2018