Claimant
C Stoughton
First
CLS-1
15 January 2018

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

Claim No: CO/1052/2017

B E T W E E N:

THE QUEEN
on the application of
LIBERTY

Claimant

- and -

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

Defendants

FIRST WITNESS STATEMENT OF COREY LYNN STOUGHTON

I, COREY LYNN STOUGHTON, of 26-30 STRUTTON GROUND, LONDON SW1P 2HR, will say as follows:

1. I am the Advocacy Director at Liberty. I supervise Liberty's legal and policy work on a range of issues, including technology and surveillance. I am authorised by Liberty to make this statement in support of its application for judicial review of certain provisions of the Investigatory Powers Act 2016 ("**IPA**").

2. Liberty is a cross-party, non-party membership organisation founded in 1934. Liberty engages in campaigning, public education, lobbying and litigation in order to promote civil liberties and human rights in the UK, including the right to privacy and appropriate limits on government power. Further background on Liberty's work can be found in the First Witness Statement of Silkie Jo Ellen Carlo dated 28 February 2017 ("**Carlo**

Statement") in paragraphs 8–15. I agree with but do not repeat what Ms Carlo says in the Carlo Statement.

3. I hold a Juris Doctorate from Harvard Law School and Bachelors of Arts in both Political Science and History from the University of Michigan. I have worked for Liberty since June 2017. Prior to that, I was appointed by President Barack Obama as senior counsel in the United States Department of Justice, Civil Rights Division, under Attorney General Loretta Lynch, which position I held until from October 2015 to 19 January 2017. I have worked on issues of privacy, technology, surveillance and civil liberties since 2004, when I was employed by the American Civil Liberties Union and handled a range of policy research and litigation projects addressing the balance between rights and state power in the post-9/11 era, including challenges to the legality of the National Security Agency's warrantless surveillance program.

4. The contents of this statement are based upon my own knowledge, except where I indicate otherwise, and are true. Where they are not based upon my own knowledge, the contents of this statement are true to the best of my knowledge and belief and I have identified the sources of that knowledge and belief, including government publications and other publicly available sources.

5. I now produce marked **CLS-1** a paginated bundle containing a true copy of the non-public document referred to in this witness statement. I refer to it in the form "CLS/1/x where "*x*" is the page number of the exhibit . Where I refer to publicly available documents, I do not exhibit them.

6. This statement provides additional evidence to that in the Carlo Statement. Specifically, it addresses the following matters, in response to the Defendants' Detailed Grounds of Resistance and the statement of Mr Andrew Scurry (which is not dated) ("**Scurry 1**") and, in particular, various suggestions made that appear to try to downplay the seriousness of the interference with privacy and freedom of expression caused by retention of communications data). Those matters are:

   (1) the intrusiveness into privacy of the collection and analysis of communication data;

   (2) the difference between "events data" and "entity data" and how the collection and analysis of both types of data can affect privacy;

(3) the regime Mr Scurry describes for issuing retention notices, in particular the risk that they could be used to support a system of indiscriminate surveillance and the chilling effect that risk has on the activity of organisations like Liberty and its members and clients; and

(4) the related issues of why post-hoc notification of the use of intrusive investigative power to collect communications data is essential to the work of organisations like Liberty and why the availability of review by the Investigatory Powers Tribunal is insufficient to allay the significant concerns about our privacy and the privacy of our members and clients.

THE INTRUSIVENESS OF RETAINING COMMUNICATIONS DATA

7. The intrusiveness of the retention of communications data with an individual's privacy is explained in paragraphs 19–29 of the Carlo Statement. Ms Carlo also discusses the particular threat to the work of organisations like Liberty at paragraphs 30–44. As Ms Carlo notes in paragraphs 29–35, revealing the "simple fact of a single communication and the identities of the parties involved" can be a significant invasion of privacy and seriously interfere with the work of human rights organisations, journalists, lawyers and political actors, and can deter whistleblowing that is critical to uncovering corruption and misconduct in a democratic system. Security professionals have described communications data as often more revealing of people's lives than the content of communications, as explained in paragraphs 27–29 of the Carlo Statement. Communications data produces a deep and comprehensive understanding of a person's private life, revealing aspects of her interests, identity, relationships, movements and activities.

8. Communications data cannot be neatly separated from "content" of communications. This is illustrated not only by the examples in the Carlo Statement but also by:

(1) the IPA itself (which in section 261(6) excludes from the definition of "content", and thereby includes in communications data, "any meaning arising from the fact of the communication or from any data relating to the transmission of the communication"); and

(2) the Home Office's draft Communications Data Code of Practice, which expressly contemplates deriving the "inferred meaning" of communications from communications data: Home Office, *Communications Data: Draft Code of Practice* (November 2017) paragraphs 2.19, 2.56.

9. Below I explain two kinds of communications data that illustrate the potential intrusiveness of communications data:

(1) Internet connection records ("ICRs"); and

(2) Cell site location data.

(a) Internet Connection Records

10. Internet connection records ("**ICRs**") provide an example of the intrusiveness of the retention of communications data. Access to ICRs enables public authorities to retain, access, and mine private and potentially sensitive information based on people's internet activities. ICRs can reveal which newspapers you read online, where you shop online, what interest-based forums you join, and whether you access pornography (even, to the extent that some pornography sites have descriptive names, what kind of pornography you access). They reveal whether you have visited the site for a charity that provides support for people with mental health problems or learning disabilities or HIV, or for people considering abortion.[1]

11. I understand that, under section 21(6) of the Regulation of Investigatory Powers Act 2000,[2] communications data did not include anything beyond the domain name (for example, "www.nytimes.com", but not the underlined text in "www.nytimes.com/newsgraphics/2016/news-tips/"[3]) in an ICR. The Government's Autumn 2016 Draft Communications Data Code of Practice made clear that the underlined text in the example above (unless it contained usernames and authorisations or a port) were excluded from communications data.[4] However, the

---

1 More detailed information on the IPA's provisions on ICRs is included in Liberty's Briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords (October 2016) (available at https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20briefing%20on%20ICRs%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf).

2 Section 21(6) provided: "that expression ["communications data"] includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored".

3 A web page headed "*Got a confidential news tip?*"

4 Home Office, *DRAFT Communications Data Code of Practice* (Autumn 2016) paras 2.54–2.55. Paragraph 2.55 stated: "With the exception of the port, and in certain circumstances the userinfo, these elements of a URL, where present, will not constitute communications data." "[T]hese elements" were explained in paragraph 2.54 included "path and optional parameters,

government's current Draft Communications Data Code of Practice (November 2017) does not contain this exclusion and makes clear that, at least in some circumstances, communications data may include a full web address.[5] This is possible under the IPA because there is no equivalent provision in the IPA to section 21(6).

12. It is not difficult to imagine the chilling effect the power to retain ICRs has on individuals' privacy and freedom of expression. Adolescents who might visit certain websites as they question their sexuality or gender identity; people with specific legal problems who might seek online legal guidance or advice from speciality law firms; people with medical conditions trying to make sense of their doctors' latest advice; people using dating websites (or websites for those wishing to conduct an affair); people expressing their political views on online forums; people gambling online; and people seeking to view legal pornography in the privacy of their own homes — all of these people must now consider, under the IPA, that the Government has (and exercises) the power to demand that their internet service provider keep, log, and on request share with Government a list of the websites and, potentially, the particular pages that they have visited.[6]

13. I consider that the IPA's expansion of the power to require retention of ICRs significantly increases the intrusiveness into an individual's privacy and freedom of expression of that retention. Telecommunications operators would not retain these records (or retain them to the same extent or for the same period) absent Government interference, as Mr Scurry says (see, for example, paragraph 32 of his statement).

14. Despite their intrusiveness, independent experts have questioned the rationale for retaining such data. The Independent Reviewer of Terrorism Legislation noted in June 2015 that it had not been demonstrated that "access to weblogs is essential for a wide

---

which are analogous to a file path on a computer. In the example of socialmedia.com/profile/homethe /profile/home is the path" and "[t]he optional query parameters and fragments. These query parameters (identified by a '?' in the URL) contain data that doesn't fit within a hierarchical path structure and can locate certain content".

5 Home Office, *Communications Data: Draft Code of Practice* (November 2017) paras 2.64–2.65.

6 I understand, too, that telecommunications companies do currently log for their own business purposes the full web addresses which their subscribers access. For example, I understand that some mobile telecommunications companies do so and then label the content (for example, "news", "fashion", etc), tag it with a geolocation and anonymise it, and then sell that data (for example, to advertisers or content generators). Open Rights Group, Cashing in On Your Mobile? How Phone Companies Are Exploiting Their Customers' Data (2016) at 16 (available at https://www.openrightsgroup.org/assets/files/pdfs/reports/mobile-report-2016.pdf).

range of investigations" and that, even within the law enforcement community, "it is widely accepted ... that the compulsory retention of web logs would be potentially intrusive."[7] He observed that no other European or Commonwealth country appears to compel the retention of such data and that Canadian and American law enforcement represented "that there would be constitutional difficulties in such a proposal."[8] He concluded that while "retained records of user interaction with the internet (whether or not via web logs) would be useful ... that is not enough on its own to justify the introduction of a new obligation on CSPs, particularly one which could be portrayed as potentially very intrusive on their customers' activities."[9] Nonetheless, as I have explained above, this appears to have occurred under the IPA and proposed Code of Conduct.

(b) The Example of Cell Site Location Data

15. As the Carlo Statement notes in paragraph 41, communications data has the potential to "constantly record our locations, and the [IPA] provides for the possibility that this will be indiscriminately retained for the State". This is an important example of the way in which the retention of communications data poses a significant threat to privacy and freedom of expression.

16. As well as ICRs, communications data includes, for example, "locational communications data" or "cell-site data". This is data recorded and maintained by mobile phone service providers based on the frequent connections to mobile communications infrastructure that modern mobile phones make. Where a person carries their mobile phone, cell-site data makes it possible to reconstruct in detail everywhere that person has been over hours, days, weeks or even months. The volume and precision of that data is likely to grow steadily in coming years, generating ever more granular locational information and thereby increasing the intrusiveness of its retention.

---

7 David Anderson QC, Independent Reviewer of Terrorism Legislation: A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraphs 9.60–9.61. In paragraphs 9.53–9.54 of that report, Mr Anderson defines "web log" to "include websites visited up to the first '/' of its [URL], but not a detailed record of all web pages that a user has accessed".

8 David Anderson QC, Independent Reviewer of Terrorism Legislation, A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraph. 9.55.

9 David Anderson QC, Independent Reviewer of Terrorism Legislation, A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraph 14.33.

17. In order to access a network, mobile phones connect to nearby cell sites (or "masts"), each of which has a unique identifier. These connections are logged, which creates a record of the phone's location.[10] This occurs many times per day, on a typical smartphone. The precision of a mobile phone user's location data depends on the size of the cell site "sectors" in the area. The coverage area of each cell site sector is smaller in areas with greater density of cell sites, such that urban areas with greater density have the smallest coverage areas. For example, according to the website www.mastdata.com, a resource page created for telecommunications professionals to identify available cell masts, there are more than forty cell sites (including small cells, discussed below) in a less than 250-meter radius of the Royal Courts of Justice (postcode WC2A 2LL).

18. The density of cell sites continues to increase as data usage from smartphones rises — a result of growing use and volume of text messages, emails, web browsing, streaming video, news and other smartphone apps and other complex uses of smartphones that involve the transmission of data. Because each cell site carries a limited volume of data, as data usage increases, carriers erect additional cell sites, each covering smaller geographic areas.[11] This is why, as I have mentioned, the accuracy of the location that is recorded continues and will continue to increase.

19. Service providers retain location information for the start and end of incoming and outgoing calls as well as information related to the transmission of text messages and routine internet connections — which smartphones make constantly to check for new emails, social media messages, news alerts, weather updates, and other functions.

---

10 Vodaphone, 'How the technology works' (available at http://www.vodafone.com/content/index/about/sustainability/mmh/how-the-technology-works.html#).

11 According to Ofcom, in the UK average mobile data volume per head increased by 40% in 2016 alone. Ofcom, International Communications Market Report 2017 at 81 (available at https://www.ofcom.org.uk/__data/assets/pdf_file/0032/108896/icmr-2017.pdf). As a result of the Government's mandate to develop a new 5G network to carry more mobile data at faster speeds, experts have estimated the UK will need several hundred thousand additional masts across the country. Sarah Knapton, '400,000 Extra Phone Masts Needed', Telegraph, Mar. 30, 2017 (available at http://www.telegraph.co.uk/science/2017/03/30/400000-extra-phone-masts-needed-bring-5g-network-rural-britain/).

The information recorded can include not only cell site and sector, but also estimated distance of the phone from the nearest cell site.[12]

20. The precision of the location recorded in communications data is also increasing as service providers deploy more and more "small cells", sometimes called "microcells", "picocells", or "femtocells", which provide service to much smaller areas than traditional cell sites, such as a floor of a large building or a single home.[13] The Government acknowledges that, with communications data from these smaller devices, the location of a person in a particular building can be pinpointed.[14]

21. The London Underground provides one example of the current high precision of location tracking services linked to mobile devices (albeit using wifi signals rather than cellular networks). In London — as is increasingly the case in cities around the world — nearly every Underground station is wifi-enabled. Unless their wifi capability is disabled, all passengers carrying a smartphone or any other wifi-enabled device, such as a laptop or tablet, automatically exchange data with Transport for London's ("**TfL**") wifi system. This is the case even if the passenger does not use TfL's wifi during his or her travels or does not log into TfL's system when prompted to do so.

22. During a trial period, TfL constantly tracked the movements of Underground passengers carrying wifi-enabled devices. During that trial, TfL logged more than 500 million wifi connection requests from around 5.6 million devices in a single month. The arrangement of TfL's wifi access points enabled TfL to construct minute-by-minute accounts of the locations and movement patterns of passengers, including specific routes taken between stations — even walking patterns within particular stations.[15] TfL stated the data was collected anonymously, but TfL refused to release the dataset in

---

12 See Craig Silliman, Executive Vice President, Pub. Policy & General Counsel, Verizon, Technology and Shifting Privacy Expectations, Bloomberg Law, Oct. 7, 2016 (available at https://bol.bna.com/technology).

13 Brian X. Chen, With AT&T Femtocell, Your Coverage Troubles Could Be Over, Wired (Mar. 24, 2010) (available at https://www.wired.com/2010/03/att-microcell/); Sacha Kavanagh, Guide to Small Cells (available at https://5g.co.uk/guides/small-cells-hetnets-5g/).

14 UK Forensic Science Regulator, Codes of Practice and Conduct, Appendix: Digital Forensics – Cell Site Analysis at 11.1.5 (9 June 2016) (available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/528197/FSR-C-135_Cell_Site_Analysis_Issue_1.pdf

15 TfL, Review of the TfL Wifi Pilot (August 2017) at 8, 20, 38-43 (available at https://tfl.gov.uk/corporate/publications-and-reports/wifi-data-collection).

response to a Freedom of Information Act request, on the grounds that the data "relate to a living individual who can be identified from the data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller".[16] The pilot demonstrates the potential for communications data to track a large number of people's locations and movements with extraordinary precision as technology develops and proliferates.

23. Thus, details about the location of a mobile phone can provide an intimate picture of a person's daily life, such as whether she is in the car or on public transportation, when she is shopping or eating, and when she is visiting the doctor, a lawyer, a journalist, a political associate, a spouse or partner, a human rights organisation, or a friend.

24. Cell-site data reveals not just where a person was at discrete moments, but where she was going. For example, in one legal case currently pending before the United States Supreme Court, the government presented testimony explaining that cell site data points revealed a man's trajectories, placing him at certain businesses at the relevant times.[17] In that case, cell-site data also allowed the government to learn with whom a person associated and when, by matching the location information of two or more individuals.[18] Although this example involves the use of communications data to facilitate a criminal prosecution, which might be appropriate if obtained through a targeted request meeting appropriate legal standards, the point is that these examples reveal the potential of *generalised* data retention (whereby the State routinely mandates the retention of such data about innocent persons) to enable interference with privacy, without restrictions and safeguards to ensure it is only retained when necessary to facilitate fighting crime.

25. Historical cell-site data can reveal not just where people go but intimate details about people's lives, easily deduced by knowing which doctors have been visited and how often, which religious services attended, which stores frequented, which group meetings attended, which houses or buildings visited. Cell site location information can

---

16 Natasha Lomas, *How 'Anonymous' Wifi Data Can Still Be a Privacy Risk*, TechCrunch (Oct. 7, 2017) (available at https://techcrunch.com/2017/10/07/how-anonymous-wifi-data-can-still-be-a-privacy-risk/).

17 *Carpenter v United States*, Brief for Petitioner, at 25–26 (citing Joint Appendix 59, 61-62, 66-67) (available at http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-ts.pdf).

18 *Carpenter v United States*, Brief for Petitioner, at 25–26 (citing Joint Appendix at 133).

identify various patterns of life and identify important places in people's lives such as their home and work.

26. Cell-site data is but one example of how a single category of communications data has extraordinary power to reveal private details about a person. As technology develops, the power of communications data to paint pictures of our private lives will only grow. For example, with the rapid proliferation of the so-called "internet of things", virtually any appliance or personal item can now be connected to the internet and programmed to transmit information about a person's home, body, or movements to a third-party company's cloud-based server.[19]

27. Communications data from specific appliances or applications (not content, but the mere time, place or manner of a communication between a personal device and a particular third-party server) can reveal details about "exercise, moods, sleep patterns, and food intake," medical conditions and body functions, reproductive health, and sexual activity.[20]

"EVENTS DATA" AND "ENTITY DATA"

28. The IPA draws a distinction between what it labels "events data" and "entity data" in section 261(3)–(4) of the IPA. The government suggests that "[i]n certain public authorities entity data may be authorised at a lower level than events data" because "the set of events data as a whole contains the more intrusive communications data,

---

19 Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, 104 Cal. L. Rev. 805 (2016) (available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=4326&context=californialawreview).

20 Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, 104 Cal. L. Rev. 805, 818 (2016); Eric J. Topol, The Future of Medicine Is in Your Smartphone, Wall St. J., Jan. 9, 2015 (available at https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632); Moira Weigel, Fitbit for Your Period: The Rise of Fertility Tracking, Guardian, Mar. 23, 2016 (available at https://www.theguardian.com/technology/2016/mar/23/fitbit-for-your-period-the-rise-of-fertility-tracking); Kashmir Hill, This Sex Toy Tells the Manufacturer Every Time You Use It, Fusion, Aug. 9, 2016 (available at https://web.archive.org/web/20170507193448/https://fusion.kinja.com/this-sex-toy-tells-the-manufacturer-every-time-you-use-1793861000).

including information on who has been in communication with whom, a person's location, and, potentially, internet connection record."[21]

29. To the extent the Government means to suggest that the retention of "entity data" is not intrusive, I disagree. For example, it is my understanding that "entity data", by its plain language, include information about all applications ("apps") mobile phone or internet service subscribers have installed on their phone or as an add-on to their primary service. This information would be "entity data" because "entity data" includes "the services ... to which the owner of the devices subscribes."[22]

30. From data about which apps a person has subscribed to or has downloaded, one could identify what bank a person uses and where her investments reside (by banking or investment services apps such as NatWest, etc), what newspapers they read (by MailOnline or Guardian apps), whether they have children (by apps designed to educate or entertain small children or support parents of young children), a person's sexuality (by subscription to gay dating apps such as Grindr). There are even apps subscription to which would reveal that a person is having, or is interested in having, an affair.[23]

31. Academic studies have shown that analysis of a person's mobile phone apps correctly reveals a person's gender over 70% of the time, and is also effective in revealing the languages a person speaks and their relationship status.[24]

32. Entity data also includes user passwords that are retained by telecommunications operators.[25] Passwords are extremely sensitive, private information. This is especially the case as common experience is that many people re-use passwords across several

---

21 Scurry 1 para 13.

22 Home Office, *Communications Data: Draft Code of Practice* (November 2017) para 2.24

23 For example, the "Ashley Madison" application: see https://itunes.apple.com/us/app/ashley-madison/id359478823?mt=8.

24 S. Seneviratne, A. Seneviratne, P. Mohapatra, and A. Mahanti, Your Installed Apps Reveal Your Gender and More, 18 ACM SIGMOBILE Computing and Communications Review 3 (2015) (available at http://www.privmetrics.org/wp-content/uploads/2015/02/mc2r_spme2014.pdf); S. Seneviratne, A. Seneviratne, P. Mohapatra, and A. Mahanti, Predicting user traits from a snapshot of apps installed on a smartphone, 18 ACM SIGMOBILE Mobile Computing and Communications Review 2 (2014) (available at http://www.privmetrics.org/wp-content/uploads/2015/02/MC2R_paper_1569898227.pdf).

25 Home Office, *Communications Data: Draft Code of Practice* (November 2017) para 2.41.

accounts, such that disclosure of a user password jeopardises the privacy of not only the content of the account subject to a retention notice, but also, potentially, many other accounts containing additional private information. To the extent, therefore, that telecommunications providers retain plaintext user passwords, such information could be subject to a retention notice for "entity data".

THE IMPACT OF THE POWER TO ISSUE INDISCRIMINATE RETENTION NOTICES

33. As noted in paragraphs 18, 30–44, and 56–68 of the Carlo Statement, the possibility of indiscriminate retention of communications data: incites fears of being monitored or tracked that impact free movement, association, expression and thought; restrict the ability of Liberty and other human rights organisations and lawyers to protect their clients and contacts, including those who reveal serious misconduct in public institutions; and hamper the ability of journalists to carry out reporting that relies on confidence in the confidentiality of communications with sources.

34. Reassurances from the Government that, in practice, they will "consider" narrowing retention notices, including "whether [a retention notice] should apply to all customers of a particular service" (Scurry 1 paragraph 66, emphasis added; Detailed Grounds of Resistance paragraph 102), and that notices "may" be narrowed in a variety of ways (Detailed Grounds of Resistance para 112), do very little to assuage Liberty's concerns (or to indicate whether this *in fact* occurs). As long as the IPA's grant of authority to Government to undertake indiscriminate retention of communications data remains law, the existence of that power raises the concern that Liberty's data will inevitably be collected and retained over some period of time — and, once this has happened, obtained by the State whether or not with the intention to target Liberty in particular. That concern creates the chilling effect on rights and on the important legal, advocacy and journalistic endeavours described in the Carlo Statement.

35. Indeed, the fact that Mr Scurry is able to give only two examples where retention notices contained any such discretionary limitation other than variations on the 12-month time limit (Scurry 1 paragraph 67) underscores the fact that, as the Government acknowledges, in almost every case retention notices mostly sweep up the communications data of wholly innocent people or organisations solely because they are customers of a company served a notice. This new information greatly exacerbates Liberty's concerns.

36. Even accounting for the Government's proposed amendments to the draft regulations — which require rather than merely permit the Secretary of State to consider whether she feels it appropriate to restrict a notice by geography or to exclude certain groups of customers from the scope of a retention notice — the IPA still permits Government to issue a retention notice relating to all communications data held by a telecommunications operator, resulting in the retention of innocent people's data where the Secretary of State is doing so for the purpose of preventing and detection a broad range of crimes (see section 87(2)(b) of the IPA). None of the proposed amendments protect the communications data of Liberty or any similarly situated organisation or individual who is engaged in no wrongdoing nor even suspected of wrongdoing.

THE IMPORTANCE OF NOTIFICATION AND THE INADEQUACY OF IPT REVIEW

37. As a practical matter, absent a notification requirement, it is extremely difficult for people who wish to protect the privacy of their data or who wish simply to ensure that any retention of and access to their data is lawful to obtain evidence sufficient to meet the threshold for seeking review in the IPT. The IPA prohibits telecommunications operators from informing customers that a retention notice has been issued or that retained data has been accessed, and the Government has provided evidence in this case stating that it will refuse to confirm or deny whether such activity has taken place (see, for example, Scurry 1 paragraphs 79–84).

38. As the structure of the IPA and the draft Communications Code of Practice make clear, the retention process is a transaction between the State and the telecommunications companies, which leaves the person whose data is used and whose privacy is interfered with completely in the dark.

39. Provisions in the IPA scheme for disclosure of "serious errors" do not constitute sufficient notice to provide redress for the concerns Liberty raises about unlawful retention (and subsequent acquisition) of communications data.

40. First, the practical reality is that individuals do not have the opportunity to scrutinise, let alone challenge, the State's determination about what constitutes a "serious error". That term that is not defined in the IPA, but requires at least "serious prejudice or harm" to the person concerned (see section 231(2)). The statute additionally requires that the "serious" error be a "relevant error" (see sections 231(1), (9)). These

subjective standards create a barrier to disclosure and risk depriving the "serious error" disclosure mechanism of any meaning whatsoever.

41. Second, "serious error" disclosure not only requires the error to be deemed "serious", but that the Investigatory Powers Commissioner be satisfied that it is in the public interest for the individual to receive notice. The fact that the individual's fundamental rights have been breached is expressly made not of itself enough under section 231(3) of the IPA.

42. Under the current scheme, the only people who are sure to receive notice that their data has been obtained by the Government are people charged with criminal offences where the prosecution relies on communications data. This is no recourse whatsoever for the many tens of millions of innocent people and institutions whose data is susceptible of being retained or obtained by the State under the IPA. This includes, for example, people whose data were included in a sweeping request relating to a large public place that police believe to be somehow connected to a crime; a victim or witness whose data has been accessed by police in a case that police decide not to prosecute; or people who happened to have used a particular telecommunications service in a general time frame or in a similar manner as a person associated with alleged criminal activity.

43. Even if the absence of notification were not a barrier to meaningful review, I consider that flaws in the IPT process render such review an insufficient safeguard of privacy. The IPT operates as a secretive court outside the regular framework of British justice. Multiple independent reviewers have called for significant reform.[26]

44. Liberty's concerns about the IPT are set out in its Observations in the *10 Human Rights Organisations v United Kingdom* claim, currently awaiting judgment in the European Court of Human Rights, which are exhibited as CLS/1/1-.

CONCLUSION

45. Liberty disagrees with any suggestion in Scurry 1 (or made by the Government more generally) that retention of, and access to, communications data does not constitute a serious interference with privacy, personal data and freedom of expression.

---

[26] A Question of Trust: Report of the Investigatory Powers Review (June 2015), paras. 14.103-08; RUSI Report, Recommendations 11-16.

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

Signed: [redacted]

Name: Corey Lynn Stoughton

Date: 15 January 2018