IN THE INVESTIGATORY POWERS TRIBUNAL

BETWEEN:

PRIVACY INTERNATIONAL

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

WITNESS STATEMENT OF IAN HOSEIN

I, IAN HOSEIN, EXECUTIVE DIRECTOR, PRIVACY INTERNATIONAL, 62 BRITTON STREET, LONDON EC1M 5UY SAY AS FOLLOWS:

INTRODUCTION

1. I am the Executive Director of Privacy International. I make this statement in support of Privacy International's claim. The contents of this statement are true to the best of my knowledge, information and belief. Where I rely on sources other than my personal knowledge, I have set out the source.

2. I hold a Bachelor of Mathematics from the University of Waterloo in Canada and a PhD from the University of London. I am an expert on privacy and technology policy, having worked at Privacy International for 16 years. I have given evidence to the British and European parliaments, acted as an external evaluator for the UN High Commissioner for Refugees, advised the UN Special Rapporteur on Terrorism and Human Rights, and advised a number of other international organisations. I have held visiting fellowships at Columbia University and the London School of

Economics and Political Science, and was previously a Visiting Scholar at the American Civil Liberties Union. I am also a Fellow of the Royal Society for the encouragement of Arts, Manufactures and Commerce (FRSA). The purpose of this witness statement is to set out the history of UK legislative proposals relating to communications data prior to and since the enactment of RIPA.

EARLY EFFORTS TO LEGISLATE BULK COLLECTION OF COMMUNICATION DATA 2000-2007

3. The first public indication that the UK Government was seeking to legislate for the bulk collection and retention of communications data was a report, circulated in August 2000 within the Home Office on behalf of the National Criminal Intelligence Service ("NCIS"), the Association of Chief Policy Officers ("ACPO"), Her Majesty's Revenue and Customs ("HMRC") and the Intelligence and Security Services, entitled "*Looking to the Future: Clarity on Communications Data Retention Law, a submission to the Home Office for Legislation on Data Retention.*"[1] At the time, the Regulation of Investigatory Powers Bill was being debated in Parliament, and did not include any reference to data retention. The agencies that authored the report, on the other hand, were calling for legislation requiring the mandatory retention of communication data for seven years.

4. In December 2001 the Anti-Terrorism Crime and Security Act was passed by Parliament, in response to the September 2001 terrorist attacks in the U.S. Under Part XI of the Act, a voluntary data retention regime was introduced. The Act empowered the Secretary of State to issue a voluntary code of practice relating to the retention of communications data by communications providers. However, the Act did not enable the Home Office to compel companies to collect or retain communications data. Accordingly, the Home Office instead pursued a mandatory data retention regime through Europe, resulting in the passage of the EU Directive on Data Retention of 2006, which required up to two-year retention periods for telephony and internet data collected by EU communications service providers. The UK Parliament introduced retention in 2007 for fixed line and mobile telephony, and then in 2009 for internet data. The EU Directive was declared invalid in April 2014 by the CJEU.

[1] "Looking to the Future: Clarity on Communications Data Retention Law, a submission to the Home Office for Legislation on Data Retention," 21 August 2000. http://cryptome.org/ncis-carnivore.htm

THE INTERCEPTION MODERNISATION PROGRAMME 2008-2010

5. Although the EU Directive compelled the retention of information held by communications service providers, thereby making available vast amounts of information for governments to access, it was limited only to the information already collected by those service providers for business and network purposes. A telephone company would only have communications data on the phone calls made and received by its customers and specific services provided by that company used by that individual. An internet access provider would only have information relating to their users, and perhaps the email activities if the service provider also offered such services. But these domestic providers would not have recorded, for business purposes, the activities of their users on other service providers. Sky Broadband would not collect information on the activities of their customers who use non-Sky email services, for instance. During parliamentary debates around the UK's adoption of the EU data retention directive in 2009, the Government was required to clarify that retention would not involve the monitoring of external communications services ("third-party services") such as Facebook and MySpace.[2] According to the then Parliamentary Under-Secretary (Security and Counter-Terrorism), Lord West of Spithead: "*The regulations only bring additions to communications data that relate to internet e-mail, internet telephony and log-on history. The EU directive excludes data that relate to third-party services. Internet-related data must relate to the services provided by the communications provider and no data revealing the content of the communication can be retained under these regulations.*"[3]

6. Perhaps to address this perceived limitation of its data retention capability, in that it did not provide access to third-party services, throughout this period the UK Government was developing the "Interception Modernisation Programme". Funding for the IMP was included in the bid to HM Treasury as part of the Government's Comprehensive Spending Review 2007.[4]

7. In July 2008, Lord West of Spithead stated that

> "*The objective of the interception modernisation programme (IMP) is to maintain the UK's lawful intercept and communications data capabilities in the changing*

[2] HC Deb, 19 March 2009, c315WH
[3] HL Deb, 24 March 2009, c633
[4] HC Deb, 19 November 2008, c593W

communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost. It was established in response to my right honourable friend the Prime Minister's national security remit in 2006."[5]

8. The Interception Modernisation Programme ("IMP") was concerned with the collection and retention of third-party data. As then President of the Council, Privy Council Office Baroness Ashton of Upholland explained in 2008,

> "*It is partly to do with a magical thing called internet protocols, which are about the new ways in which people communicate. Noble Lords will be aware of the whole of the internet, from Facebook onwards, but telephone conversations also are increasingly conducted over the internet. As with any other technological advance, it is important that we look at the implications for the services. The modernisation programme is being undertaken in part at least to try to anticipate the way in which those methods of communication could be used in the future.*"[6]

9. In October 2008 the details about the IMP were published by *The Sunday Times*. The article reported that the Government was considering spending up to £12 billion on a centralised database to "*to monitor and store the internet browsing habits, e-mail and telephone records of everyone in Britain*." The article stated: "*The Home Office stressed no formal decision had been taken but sources said officials had made clear that ministers had agreed "in principle" to the programme.*"[7]

10. In the resulting public debate, the Home Office minister Vernon Coaker stated that a public consultation would soon follow:

> "*Since 2006 there has been ongoing work with intelligence agencies, SOCA, police, HMRC and the telecommunications industry to analyse the size of the problem and to investigate possible solutions to help maintain this essential capability, including relevant safeguards. I recognise there is a difficult balance between public safety and public rights to privacy so I recently announced my intention to launch a public consultation on the Interception Modernisation Programme.*"[8]

---

[5] HL Response to Parliamentary Question HL4466, July 2008, Column WA76
[6] HL Deb, 6 February 2008, c1069
[7] David Leppard, "Government will spy on every call and e-mail", *The Sunday Times*, 4 October 2008. http://www.thesundaytimes.co.uk/sto/news/uk_news/article240225.ece
[8] HC Deb, 24 November 2008, c830W

11. Yet when asked about the creation of a national database of communications data,[9] the Government responded that it had "*not yet decided on a definitive proposal on how to modernise these capabilities. Consideration of options is under way. When the Government do bring forward policy proposals, they will be notified to Parliament in the proper way, with associated information on financial implications*."[10]

12. The Government acknowledged the significant pressure to consult on the development of the IMP. According to Lord West of Spithead:

> "*There has been a good deal of interest in this programme from those within this House. I know; I have given many briefings to noble Lords and I stand ready to give more if asked for. In addition, I have bent over backwards to ensure that the Opposition get briefings from Ministers and officials. There has been a great deal of media speculation about the Government's plans. There will shortly be a full consultation exercise on options relating to maintaining our communications data capability in the longer term as methods of transferring data change*."[11]

13. Although the consultation was originally planned to commence in January 2009,[12] it was not until April 2009 that the Government launched "*Protecting the Public in a Changing Communications Environment*".[13] As described by the Minister, "*This consultation relates to communications data (information about a communication but not its content) and is seeking the public's view on how to ensure that communications data continue to be retained in and made available lawfully, on a case by case basis, to public authorities*."[14] The proposals in the consultation paper departed significantly from the proposal leaked to the Sunday Times; while the focus on collection and retention of data from third-party services remained, the Government abandoned the centralised collection of data. The paper stated that although this was technically effective it would have privacy implications:

> "*The Government has no plans for a centralised database for storing all communications data. An approach of this kind would require communications service providers to collect all the data required by the public authorities, and not*

[9] Question from James Brokenshire, HC Deb, 8 October 2008, c667W
[10] HC Deb, 8 October 2008, c667W
[11] HL Deb, 24 March 2009, c620
[12] 24 November 2008, c830W
[13] The Home Office, "Protecting the Public in a Changing Communications Environment", April 2009. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228726/7586.pdf
[14] HC Deb, 19 May 2009, c1296W

only the data required for their business needs. All of this communications data would then be passed to, retained in, and retrieved from, a single data store. This could be the most effective technical solution to the challenges we face and would go furthest towards maintaining the current capability; but the Government recognises the privacy implications of a single store of communications data and does not, therefore, intend to pursue this approach."[15]

14. Later in the paper, the Government described what a centralised solution would look like:

> "*This would require the collection and retention of both communications data relating to the services offered by UK communications service providers, and also the additional third party data from services that UK communications service providers do not offer but that are carried over their networks. This data would then be sent in near real time to a single location at which it would be stored. All this data would then be automatically arranged and organised, where appropriate, to enable subsequent lawful queries from public authorities to be answered quickly and effectively and in the timescales required, in accordance with the relevant safeguards*."[16]

15. The Government went on to recognise that such a system would require too significant a change from current retention practice:

> "*However, this approach would also represent the most significant shift from the current system. Today, communications data is collected and retained by different companies in separate locations. Under this approach, all the data would be held together in one place. The Government recognises the privacy implications in holding all communications data from the UK from a 12-month period in a single store. The Government therefore does not propose to pursue this approach.*"[17]

16. The alternative proposal advanced by the Government was to compel the collection and retention of third-party data by communications service providers. The Government proposed legislation that would "*ensure that the data required by public authorities to protect the public is collected and retained by the communications service*

[15] "Protecting the Public in a Changing Communications Environment", paragraph 16, p. 4.
[16] Ibid, p. 25.
[17] Ibid.

providers."[18] This would include both the data that UK communications service providers already collect for their own business purposes and some additional data, largely relating to communications services provided from overseas providers.

17. The response to the consultation was largely negative,[19] with almost half of respondents to the consultation (90 out of 221 respondents) objecting to the consultation paper overall, and 38 per cent of the remaining respondents opposing the Government's proposed approach. As a result, draft legislation was generated but not introduced.

THE COMMUNICATIONS CAPABILITIES DEVELOPMENT PROGRAMME 2010-2012

18. The May 2010 election resulted in a Coalition agreement that included measures "*to reverse the substantial erosion of civil liberties under the Labour government and roll back state intrusion*."[20] The Coalition pledged to "*end the storage of internet and email records without good reason*." [21]

19. Nevertheless, the July 2010 Home Office Draft Structural Reform Plan indicated its intention to "*[p]ublish proposals for the storage of internet and e-mail records, including introducing legislation if necessary*" by November 2010.[22]

20. The issue was revisited in the Strategic Defence and Security Review of October 2010.[23] The review stated that the Government would require "*investment in technologies to support the gathering of communications data vital for national security and law enforcement*."[24] It also identified how the intelligence community would need to "*continue to invest in a range of covert intelligence capabilities to enable us to identify, investigate and disrupt terrorist activity at the earliest possible stage […]* [with] *the*

[18] Ibid, p. 4.
[19] Home Office, "Protecting the Public in a Changing Communications Environment: Summary of Responses to the 2009 Consultation Paper", November 2009.
http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary
[20] HM Government, "The Coalition: Our Programme for Government", May 2010.
http//www.gov.uk/government/uploads/system/uploads/attachment_data/file/78977/coalition_programme_for_government.pdf
[21] Ibid.
[22] Home Office, "Draft Structural Reform Plan", July 2010, p. 9.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/98647/pdf-version.pdf
[23] HM Government, "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", October 2010.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf
[24] Ibid, p. 13.

Government Communications Headquarters (GCHQ) bringing its technical and analytical capabilities to bear."[25]

21. The Government would therefore

> "*introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communication data and to intercept communications within the appropriate legal framework. This programme is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. [...] We will legislate to put in place the necessary regulations and safeguards to ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties*."[26]

22. The IMP was replaced by the "Communications Capabilities Development Programme" ("CCDP") run by the Communications Capabilities Directorate. The CCDP was tasked with developing new legislation to regulate the ability of the security services and the police to access communications data and to conduct interception of communications. The Counter-Terrorism Strategy, published in July 2011, confirms the Government's intention:

> "*Communications data is an important tool for investigators and provides an invaluable means by which the police and law enforcement agencies can better safeguard the public. But our current capability was not designed to deal with the growth in the use of internet-based communications. The ability of the security, intelligence and law enforcement agencies to use internet-based communications data will decline unless action is taken. As we set out in the Strategic Defence and Security Review (SDSR) the Government will therefore introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communications data and also to intercept communications within the appropriate legal framework. Legislation will be brought forward to put in place the necessary regulations and safeguards to ensure that the response to this technology*

[25] Ibid, p. 42.
[26] Ibid, p. 44.

challenge is compatible with the Government's approach to information storage and civil liberties."[27]

THE DRAFT COMMUNICATIONS DATA BILL 2012-2014

23. The May 2012 Queen's speech announced the Government's intention to introduce the Draft Communications Data Bill. The draft Bill was released in June 2012, with a Forward by the Home Secretary stating:

> "*For many years our police and security and intelligence agencies have used communications data from landline telephones and mobiles to catch criminals and to protect the public. This information – which does not include the content of a phone call or email – has played a role in nearly every serious organised crime investigation and in all major Security Service counter-terrorism operations over the past decade and is fundamental to policing across the UK. But the ability of the police and others to use this vital tool is disappearing because communications data from new technologies is less available and often harder to access.*
>
> *The purpose of this Bill, therefore, is to protect the public and bring offenders to justice by ensuring that communications data is available to the police and security and intelligence agencies in future as it has been in the past. I recognise that these proposals raise important issues around personal privacy. This Government is committed to ensuring that here, as elsewhere, we strike the right balance between protecting the public and safeguarding civil liberties. I believe that there are compelling reasons for the provisions in this Bill and want to ensure that they are fully considered and understood before we commence the formal legislative process.*"[28]

24. The Home Office was adamant that the Bill did not envisage interception or mass surveillance:

> "*Nothing in these proposals will authorise the interception of the content of a communication. Nor will it require the collection of all internet data, which would be neither feasible, necessary nor proportionate. We will extend existing safeguards regarding data retention, access and oversight.*"[29]

[27] "CONTEST: The United Kingdom's Strategy for Countering Terrorism", Cm 8123, July 2011, p. 53.
[28] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf
[29] Ibid, p. 2.

25. In retrospect, it appears that the Draft Communications Data Bill was an attempt to place Tempora on a legislative footing, particularly with respect to the collection, analysis and processing of communications data. The Draft Bill first establishes the order making power of the Secretary of State (not necessarily limited to the Home Secretary) to "*ensure that communications data is available to be obtained from telecommunications operators by relevant public authorities*", or "*otherwise facilitate the availability of communications data to be so obtained from telecommunications operators*" (Part 1, Clause 1(1)). An order may provide for a number of mechanisms, including "*the entering into by such operators of arrangements with the Secretary of State or other persons under or by virtue of which the Secretary of State or other persons engage in activities on behalf of the operators on a commercial or other basis for the purpose of enabling the operators to comply with requirements*" (clause 1(2)(a)(iii)), and "*impose requirements or restrictions on telecommunications operators or other persons or provide for the imposition of such requirements or restrictions by notice of the Secretary of State*." (clause 1(2)(b)) These requirements may include requiring that communications data can be disclosed without undue delay, can require operators to comply with specified standards, acquire, use or maintain specified equipment or systems, or to use specified techniques. The requirements may include "*requirements which ... (ii) are in respect of communications data relating to the use of telecommunications services provided by another telecommunications operator in relation to the telecommunication system concerned*." (clause 1(3)(c)(ii))

26. This therefore permits the Secretary of State to require a service provider to use technical measures decided by the Government to collect metadata, including data generated by another service provider. This was a fundamental change in policy from, for instance, the Data Retention Directive, which only applied to data already collected by a service provider which related to its own service. Service providers could be required to install and use equipment to collect metadata about the use of third-party services. For example, if a person in the UK uses a US email provider (e.g. Gmail) at an internet café in London, the communications service provider for the internet café could be required to intercept the communication, use searching and filtering equipment to try and obtain the metadata, then store that information.

27. One confusing element is that the Bill then states that this power does not relate to "*any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system*" (clause 1(4)). In the debates

around the Bill this grew contentious because gathering the communications data of third-party services would necessarily entail interception and inspection of the content of packets over the network.

28. Due to political resistance to the Bill, another consultation ensued, with a Joint Committee constituted to review the draft Bill. I twice gave evidence before the Committee, and raised the serious concerns I had with the Bill, including that it would sanction the mass surveillance of communications at a scale previously only seen in undemocratic and authoritarian states.[30]

29. In the Joint Committee hearings, the Home Office was directly asked about third party collection and the use of national probes, and Mr Farr, the official who is also giving evidence in these proceedings, gave evidence of the government's desire to legislate for the implementation of automated data collection facilities on UK networks:

> "***Lord Faulks**: Do you envisage actually using powers to capture the data from the major overseas company, or is it envisaged that it is going to be restricted to the smaller fry?*
> ***Charles Farr**: I personally would not want to go down the route of collecting third-party data from a network here without the collaboration of the service provider. It is not in keeping with the relationship we have with the major service providers now and I really do not think it should come to that pass. I can understand, as the UK CSPs have said to us and said to you, that that would put them in a difficult position; and we want to avoid it.*
> ***Lord Faulks**: We need to see some informal reassurance from you. Can it be built into Bill in some way?*
> ***Charles Farr**: I said to them that it is an in extremis power. I would draw a distinction between our dealings with major US ACSPs[31] and our dealings with smaller niche companies from potentially hostile states. I can imagine that any government may wish to have in its back pocket a power to draw data off a UK network, where a CSP in a hostile state is unwilling to provide it and is not even interested in establishing a co-operative relationship. I think that it is in that sort of*

[30] House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, Session 2012-13, Oral Evidence, p. 48. http://www.parliament.uk/documents/joint-committees/communications-data/Oral%20Evidence%20Volume.pdf
[31] The term 'ACSP' is undefined, but in the evidence session appears to refer to 'American Communication Service Provider'.

context that we envisage probes (DPI), and certainly not, if we can possibly avoid it, in the context of the major ACSPs."[32]

30. In their written evidence to the Joint Committee, the Home Office also made reference to a number of suppliers who made technology to collect 'required' communications data (CD) from networks:

> "*110. Where practical, CSPs may use their existing suppliers and solutions to collect required CD from their networks. A number of UK and international suppliers provide specialist DPI*[33] *equipment. We are confident that CSPs and industry can provide a CD collection capability, and will work with them to procure a sustainable network collection capability. Manufacturers who provide DPI equipment to the global telecommunications sector include: Acme Packet Inc; AdaptiveMobile Ltd; Advanced IO Systems; Alcatel- Lucent; Arbor Networks Inc.; BAE Systems Detica; Bivio Networks Inc.; Bridgewater Systems Corp.; Cisco; Cloudshield Technologies; Endace; Huawei; IP Fabrics; Ipoque; Juniper; Niksun; Procera Networks; Radware; Roke Manor; Solera Networks; Symantec; Tilera; Unipier; TRL; and Verint*."[34]

31. The Government tried to differentiate these practices from the previous centralised database. In their written evidence, the Home Office also stated:

> "*30. The Government has also considered alternative technical solutions. An approach considered by the previous Government would have involved the wider deployment across UK networks of technical probe equipment (as referred to in paragraph 20) to collect large volumes of data about services transiting the network (such as webmail or social media). Although we do not rule out the use of probes where necessary, this Government has reviewed this option and sees no benefit in pursing it.*" [35]

32. The Draft Bill sees this processing of communications data as consisting of "*reading, organisation, analysis, copying, correction, adaptation or retrieval and its integration with other data*," (Clause 1(1)(5)). This data must then be retained for twelve months.

---

[32] Ibid, p. 353
[33] 'Deep Packet Inspection'
[34] House of Lords, House of Commons, Joint Committee on Draft Communications Data Bill, Session 2012–13, Written Evidence, p. 247. http://www.parliament.uk/documents/joint-committees/communications-data/written%20evidence%20Volume.pdf
[35] Ibid, p. 236.

33. Part 2 of the Draft Bill established a regime for obtaining the data. This power, as under RIPA, is self-authorised by 'a designated senior officer'. The purposes include a wider variety of interests, much broader than under the Intelligence Services Act (clause 9(6)). Though judicial authorisation was introduced in this draft bill (clause 11), it was only for certain authorisations not relevant to this discussion as it excludes the primary relevant public authority of the draft bill, being the police, SOCA, HMRC, and "any of the intelligence services".

34. A core new component of the Draft Bill that had been missing from the IMP proposals was the inclusion of a "filter" (Part 2, clauses 14-16). Rather than have a centralised database, as proposed under IMP, the draft bill introduced filtering arrangements. The "filter" as envisaged by the Government was a massive data mining operation that would take all of the decentralized data stores and search all the information in them with selectors and build social network graphs and pattern of life analyses. The potential privacy consequences of such data mining software has been well described by others and I do not repeat those concerns here.

35. Should information derived by the filter reveal information relevant to the intelligence or police agencies, then data would be handed over. The "filter" was presented in the Explanatory Notes as a key safeguard for privacy, operated by the Secretary of State or a "designated public authority".[36] The Government's stated purpose for the filter was to limit the information disclosed to a requesting agency and thereby to limit collateral intrusion,[37] and generate information for the Interception Commissioner to keep under review. Yet the filter would have access to vast amounts of data in order to conduct its processing to respond to queries about the communications data. My assessment of the reality is that the "filter" in fact had the potential greatly to increase the intrusion on privacy involved in the collection and processing of communications data.

36. The order-making power of Part I and the "filter" under Part 2 were the most contentious aspects of the Bill. The Parliamentary committees were both concerned about the breadth of the order-making power, making links with other such order-making powers. When asked particularly about third-party data collection, one

[36] Ibid, pp. 30-31.
[37] Question from James Brokenshire, HC Deb, 8 October 2008, c667W

member of the Joint Committee asked the Home Office about the existing power under the Telecommunications Act.

> "*Q932* ***Dr Huppert****: This issue about collecting third party transient data is a very sensitive one. You raised the cases for educators, where you might have a very unfriendly Government, and so forth. Section 94 of the Telecommunications Act 1984 gives the power for extremely broad directions in the interests of national security to be placed on Ofcom and any provider of public electronic communications networks. Would that give you the cover that you need for national security cases?*
> ***Charles Farr****: Well, possibly, but it is not a particularly transparent bit of legislation.*
> ***Dr Huppert****: You think that we should repeal it as well?*
> ***Charles Farr****: I did not say that. Of course, you come onto the critical point of whether the information that you are looking for constitutes a threat to national security, or whether it is organised crime, which is not always a threat to national security. So, possibly – but I do not think it is a very appropriate vehicle, and it suffers from the threshold problem."* [38]

37. After a four-month consultation process, the Joint Committee produced a report that was highly critical of the draft Bill.[39] The Joint Committee expressed concern with the order-making power for the Secretary of State:

> "*This is commonly referred to as the third party provision. A simple illustration is that using the third party provision it would be possible to ask a United Kingdom broadband provider to collect data on e-mails crossing its network when those e-mails were sent using one overseas based e-mail provider to another overseas based e-mail provider.*"[40]

38. This raised concerns over security. According to Simon Milner, the Director of Policy for UK and Ireland of Facebook, who was quoted in the report:

> "*The security of our networks and the security of how we store and look after customer data are fundamental to our businesses. Therefore, when we are concerned*

[38] Joint Committee on Draft Communications Data Bill, Session 2012–13, Oral Evidence, p. 354.
[39] House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, Session 2012-13 Report, together with appendices and formal minutes.
http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf
[40] Ibid, para. 89.

that someone else might be trying to intercept our data, we will move heaven and earth to ensure the security of our network. It is a grave concern to us that it might well be part of the new framework that UK CSPs might be required to retain these data. One would expect there to be not only implications for relationships in the internet value chain but changes in behaviour by users. Facebook users already have the ability to encrypt their traffic, and we would expect many more UK users to choose to do so were that kind of measure to be introduced."[41]

39. In this regard, the Joint Committee was able to elicit assurances from the Government "*that the Home Secretary will invoke the third party provisions only after the original data holder has been approached and all other avenues have been exhausted*."[42] That is, if a third-party provider in another jurisdiction complied with lawful requests, then its data would not be collected *en masse*. The Joint Committee demanded that this be given statutory force rather than a loose commitment.

40. The Joint Committee concluded that:

> "*[…]there is a case for legislation which will provide the law enforcement authorities with some further access to communications data, but that the current draft Bill is too sweeping, and goes further than it need or should. We believe that, with the benefit of fuller consultation with CSPs than has so far taken place, the Government will be able to devise a more proportionate measure than the present draft Bill, which would achieve most of what they really need, would encroach less upon privacy, would be more acceptable to the CSPs, and would cost the taxpayer less. We make detailed recommendations accordingly on the content of a revised Bill*."[43]

41. The Joint Committee was particularly concerned about the lack of foreseeability in the application of the proposed law:

> "*We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft Bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data. Clause 1 would give the Secretary of State sweeping powers to issue secret notices to communications service providers*

[41] Ibid, para 96.
[42] Ibid, p. 34.
[43] Ibid, p. 74.

(CSPs) requiring them to retain and disclose potentially limitless categories of data. We have been told that she has no intention of using the powers in this way. Our main recommendation is therefore that her powers should be limited to those categories of data for which a case can now be made. If in future a case can be made for the power to be increased, this should not be done without effective Parliamentary scrutiny. We recommend the procedure for this."[44]

42. The Intelligence and Security Committee ("ISC") also reviewed the draft bill. The ISC focused their analysis on how it related to the UK's intelligence and security agencies. In February 2013 the ISC released its own report on the draft Bill, reaching similar conclusions on the order-making power:

> *"We strongly recommend that more thought is given to the level of detail that is included in the Bill, in particular in relation to the order-making power. Whilst the Bill does need to be future-proofed to a certain extent, and we accept that it must not reveal operational capability, serious consideration must be given as to whether there is any room for manoeuvre on this point: Parliament and the public will require more information if they are to be convinced."*[45]

43. The ISC also stated:

> *"We have similar concerns regarding the background information accompanying the draft Bill. Whilst we recognise the need to take action quickly, the current proposals require further work. In particular, there seems to have been insufficient consultation with the Communications Service Providers on practical implementation, as well as a lack of coherent communication about the way in which communications data is used and the safeguards that will be in place. These points must be addressed in advance of the Bill being introduced."*[46]

[44] Ibid, p. 3.
[45] Intelligence and Security Committee, "Access to communications data by the intelligence and security Agencies", February 2013, para 79.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf, para. 79.
[46] Ibid, para. 80.

44. Both committees were also concerned about the filter. In the evidence sessions even the Chair of the Joint Committee began referring to the filter less as a safeguard and more as a "search engine".[47]

45. In their written evidence, the Home Office described the filter in terms remarkably similar to those used to describe Tempora:

> "*68. The purpose of the Request Filter is to automatically obtain, process and analyse communications data needed to answer more complex data requests where data from different communications services providers might be required. The Request Filter will ensure that, after processing, only the key communications data is passed to a public authority and data irrelevant to the investigation is destroyed. By using the Request Filter to automate the analysis, the amount of data passed to public authorities will be minimised, reducing the levels of intrusion and protecting privacy. Without these filtering arrangements, public authorities are likely to need to make many more requests to CSPs in future and would need to piece the communications data together in-house, with implications for personal privacy and data protection.*"[48]
>
> *118. The Request Filter will not separate content from CD. It will only filter CD that has already been retained by CSPs. Nor is it a central database. The legislation makes clear that the Filter can only acquire and process communications data to answer a specific public authority request. Once that request has been answered the Filter will permanently delete all the communications data it acquired.* "[49]

46. One example given by the Home Office on the power of the 'filter' would be to search vast stores of data to bring out selected information.

> "***Peter Hill**: I think you used the word "databases". Just to be clear, the filter only relates to accessing communications data. So a request will be made, for example, to know who the subscriber to an e-mail was, or "This phone was in these locations", and it will take that communications data. First of all, it will tell the person asking how much data is likely to be necessary to answer that query, so it will help them make the judgment about necessity and proportionality. If they go ahead, it will then*

[47] House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, Session 2012-13, Oral Evidence, Q310.
[48] Joint Committee on the Draft Communications Data Bill, Session 2012-13, Written Evidence, p. 242.
[49] Ibid, p. 248.

sift out the irrelevant data and give them the relevant data, not the data they do not need. I entirely take the point that it is a tool that can do a lot of things, but the point that this is a safeguard to try to focus the data that is being asked for is an important one. Rather than getting all the data and then sorting it within a police authority in order to get the bits you need, having a process which does that without human involvement should reduce the data that is being disclosed, not increase it.
***Stephen Mosley**: So, effectively, it will interrogate the communications data that is held by the third parties and bring the results to one place.*
***Richard Alcock**: Yes, on a request-by-request basis.*"[50]

47. The Joint Committee did not appear to be convinced. In the final report, the Joint Committee referred to the filter as a 'data mining device' and not substantively different from the centralised database that had been abandoned as a proper proposal by HM Government on privacy grounds:

> "*113. It is however important to consider how different the proposals for the Request Filter really are from the previous Government's proposals for a central database. A central database would have been one repository of communications data provided by the CSPs but stored on a Government owned and operated database. The Request Filter is a Government owned and operated data mining device which, to work efficiently, requires each CSP to maintain its own database of all its communications data in a common format. Each CSP database will be able to be accessed at any time by the Request Filter. So the same data is being stored about the same people and it is being stored in databases which are accessible to public authorities given powers under the Bill. The difference is that instead of one database there are many and they are privately owned. Although they are privately owned the Government can stipulate what should be held on them, for how long, and in what format it should be supplied. The differences therefore are not as great as the Home Office suggests; the Request Filter can be equated to a federated database.*"[51]

48. The Joint Committee was concerned with the scope of the Filter and who would run the Filter:

[50] House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, Session 2012-13, Oral Evidence, Q94.
[51] Joint Committee on the Draft Communications Data Bill, Session 2012-13, Report, together with appendices and formal minutes, pp. 34-35.

> *"119. ... The scope of the Bill does not limit who the day to day operation can be transferred to, and some witnesses have expressed concern that it could be GCHQ which is not accountable to the public or to Parliament, although any transfer of functions would not affect the Secretary of State's responsibility for the exercise of the functions."*[52]

49. The Joint Committee therefore concluded:

> *"126. The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests."*[53]

50. The Intelligence and Security Committee reviewed the filter from the perspective of the intelligence and security agencies. Although they had concerns about the ability of the government to create such a complex system, their final report noted that "*both GCHQ and the Security Service use variations of such technology in their day-to-day business*." The ISC then quotes GCHQ stating: "*We already use in GCHQ similar sorts of technology that allow complex federated queries to be made from different data sources... so my sense is that it would be a challenge, but the underpinning technology is out there*."[54]

51. The ISC then concluded

> *"The technology seems to exist to provide this. It will be a significant challenge to integrate the numerous data sets from different Communications Service Providers to make the filter work, as well as manage the expectations of the various Departmental and Agency stakeholders. The record of government in managing such complex IT projects is mixed at best."*[55]

52. The ISC did not echo the Home Office's belief that there was an urgent need for policy action to address the capabilities of the intelligence and security services. The

[52] Ibid, p. 36.
[53] Ibid, p. 37.
[54] Intelligence and Security Committee, "Access to communications data by the intelligence and security Agencies", February 2013, p. 22.
[55] Ibid, p. 23.

ISC's report alluded to the far more extensive capabilities already possessed by such agencies:

> "*At present, the intelligence and security Agencies are able, to some extent, to work around the problem of declining communications data by obtaining intelligence using other national security capabilities which are not, in most cases, available to the police. This means that the Agencies are not facing as immediate a problem as that currently faced by the police and other authorities. Nevertheless, we believe that the decline of available communications data will begin shortly to have a serious impact on the intelligence and security Agencies.*"[56]

53. In any event, with the production of reports from two separate Committees articulating serious concerns about the draft Bill, in April 2013 the Deputy Prime Minister declared that the Draft Bill would not proceed. He conceded that "*the idea that the government will pass a law which means there will be a record kept of every website you visit, who you communicate with on social media sites, that's not going to happen.*"[57] In *The Daily Telegraph* he expressed his concern that the proposed legislation would involve keeping records on all innocent people, the legislation would be counter-productive, would raise complex jurisdictional issues, and set a worrying international precedent:

> "*We would be the first Western democracy to propose that our police and security services should be legally entitled to obtain data from servers in other countries. We would inhibit our ability to speak out as a leading voice for internet freedom.*"[58]

54. In what appears to be a reference to the Filter, the Deputy Prime Minister concluded his statement of concern with the following:

> "*No one denies the need for innovative solutions to meet the challenge of policing in the internet age. But the idea that we should store, en masse, the details of everyone's*

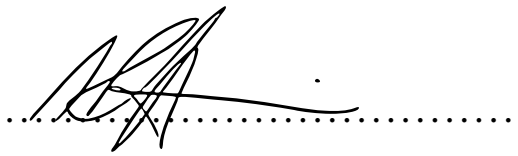
---

[56] Ibid, p. 13
[57] "Nick Clegg: No 'web snooping' bill while Lib Dems in government" BBC, 25 April 2013. http://www.bbc.co.uk/news/uk-politics-22292474
[58] Nick Clegg, "Nick Clegg: The 'snoopers' charter' cannot go ahead", *The Telegraph,* 25 April 2013. http://www.telegraph.co.uk/news/politics/nick-clegg/10019378/Nick-Clegg-The-snoopers-charter-cannot-go-ahead.html

web activity has not withstood scrutiny. Far better we focus our time and energy on the sensible and proportionate measures that help keep people safe."

Statement of Truth

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



Ian Hosein

8th **June 2014**