ISC Call for Evidence – Privacy and Security

Submission from Dr Julian Huppert MP

Executive Summary

1. Parliament has three main functions: to scrutinise the work of government, to pass legislation, and to authorise the raising of taxes and monitor its expenditure. In relation to security, intelligence and surveillance, Parliament has singularly failed to discharge these functions. Parliament has failed to set and monitor clear standards for how surveillance should operate and be scrutinised, and so the relevant legislation is being used far beyond the scope that was originally intended. There is no transparency over budgets or the effectiveness of surveillance programmes. In this regard, we have failed both the public, whom we serve, and the intelligence and security services that protect us.
2. Whilst I welcome this call for evidence, it can only be viewed as a first step towards an ongoing process of proper Parliamentary scrutiny, restoring public trust, and effective legislative support for the intelligence and security services that they fully deserve.
3. To remedy these problems, there are some key steps that need to be taken:
    a. A full post-legislative review of the Regulation of Investigatory Powers Act 2000 ["**RIPA**"], the Telecommunications Act 1984, and the Intelligence Services Act 1994, conducted by a body with knowledge and expertise in this area, including outside experts.
    b. Alongside the ISC, a separate body should be established with similar objectives and make-up as the Privacy and Civil Liberties Oversight Board in the US to scrutinise new and existing legislation and make recommendations.
    c. The amalgamation of the Investigatory Powers Tribunal, the Intelligence Services Commissioner, the Office of Surveillance Commissioners and the Interception of Communications Commissioner into a unified body, with increased funding, access to technical expertise, and an emphasis on necessity and proportionality in the review or assessment of surveillance.
    d. Greater transparency through the annual release of Government Transparency Reports which publish, as a minimum, the annual number of user data requests made by law enforcement, the intelligence agencies, and other authorities, broken down by requesting authority, success rates, types of data requested and category of crime or event being investigated. Greater transparency with regards to surveillance costs through more detailed breakdown of figures.
    e. Improved oversight through a reformed ISC – placing it on par with other Parliamentary Select Committees, with improved funding, greater access to technical expertise, and a more open nomination and selection process (subject to a veto on security grounds by the Prime Minister).
4. Strict limitations on "information laundering", whereby national legislation is bypassed through the sharing of information or reciprocal surveillance programmes with the security and intelligence services of other nations. These reforms should bring the UK in line with international standards, in particular the International Principles on the Application of Human Rights to Communications Surveillance. The thirteen principles enunciated here are: legality,

legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, transparency, public oversight, integrity of communications, safeguards for international co-operation and safeguards against illegitimate access. This would bring the UK in line with the UN General Assembly's Resolution A/RES/68/167 on the right to privacy in the digital age. In short, we should focus our resources on suspicion-led surveillance based on necessity and proportionality, not the mass surveillance of innocent citizens.

What balance should be struck between the individual right to privacy and the collective right to security?

5. The right to respect of private life *and correspondence* is not the only fundamental right infringed by the systematic surveillance of communications; it infringes other freedoms, such as freedom of expression, of association, of conscience and of religion. All of these rights are essential in safeguarding the democratic principles of our society. To focus exclusively on privacy without considering these other rights, misses the larger question: what kind of society do we want to live in?

6. When creating such powerful systems, we must consider not just those who currently operate them, but those who may follow, how those systems could be – or are being – abused, and how mission creep could extend the scope, level and time-span of such intrusion. These systems need to be future-proofed against a less benevolent government.

7. When assessing what balance to strike between the need for security and our civil and political rights, we must consider all the data and evidence that is available. We must balance the cost of the operations against the value of the objectives being achieved. And within that assessment, we must look at the full cost, not just the expense to the Treasury. With limited knowledge of what is being done in our name, our job is made harder.

8. How effective are current surveillance practices, how many attacks have been prevented, how many lives saved, injuries averted, or property protected, and at what cost? What would be the likely benefits of investing the same amount of money in more traditional forms of policing or engagement programmes? Would that change in focus be more effective in protecting our collective security? If one of the objectives of our security and intelligence apparatus is to save lives and protect property, then a full cost-benefit analysis needs to be carried out, in the context of other means of utilising that budget which are more effective at securing our goals.

9. This underlines our first problem: the lack of public information. When I sat on the Joint Committee on the draft Communications Data Bill ("**the Joint Committee**"), we requested information on how Communications Data was being used, but the Home Office did not have the fairly basic data requested. When we asked for figures on the financial benefits of accessing additional data, the figures provided to us were described as "simply fanciful and misleading" (at para 267 of the Report).

10. But we must also factor in the social, political and economic cost of the current mass-surveillance model. How many people are having their rights infringed, and to what extent? How many peaceful activists have had their rights curtailed? How many individuals have been put under surveillance for trying to effect peaceful change? If the UK could not avoid liability by using 'national security' exemptions under the Data Protection Act 2000, what would be the net value of damages that would be payable to our citizens? Whilst we have no current models for quantifying this damage, this is something that the proposed post-legislative review should properly consider.

11. Furthermore, the use of mass-surveillance and attempts to break standard encryption technology creates a strong risk to the digital economy which has led the fragile economic recovery, and represents £110bn of the UK's GDP. It is a dynamic market – and it can move. People who are concerned about privacy can move their businesses and infrastructure to places like Germany which are protecting it better. Aside from the potential Balkanisation of the internet, undermining privacy and the digital economy is contrary to the UK's economic interest.

12. If the reports of attempts by our intelligence services to undermine standard encryption methods is true – and I suspect that it is – then we are creating a very real risk of fatally undermining the internet and the whole of our digital economy. I have serious concerns about the potentially catastrophic consequences that would follow if our online banking encryption or similarly vital encryption is broken as a result of the work of our intelligence services. A weakness or backdoor created by our intelligence services would be open to abuse by antagonistic states and criminal gangs; to assume otherwise is naïve in the extreme.

13. Those of us making submissions are being asked to balance competing interests in the absence of the majority of the evidence that is needed to give an informed opinion. Discussing principles is all very well, but it needs to be done in a real-world context and with the facts laid bare. Nobody is suggesting that sensitive operational details should be made public; but percentages, statistics, and performance figures should all be released in quarterly or annual transparency reports. Without this information, Parliament cannot conduct proper scrutiny.

14. That being said, the evidence we have so far is not reassuring. None of the witnesses to the Joint Committee "could provide specific evidence of significant numbers of lives saved to date" (at para 268 of the Report). The US Privacy and Civil Liberties Oversight Board ("**PCLOB**") reached the same conclusion: it could not find "a single instance" in which the NSA's mass phone surveillance program "made a concrete difference in the outcome of a terrorism investigation". "Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack." Thus the only evidence available to us as to the effectiveness of the UK's and US' mass-surveillance is that such surveillance is largely ineffective. Given that two of the main functions of Parliament are to scrutinise the work of the Government and to oversee the raising and expenditure of taxes, two reforms are essential. First, there must be independent and effective oversight in Parliament and through an amalgamated and improved Surveillance Commissioner system as set out in the Executive Summary above. And secondly, there must be greater transparency in terms of financial, economic and social costs and the effectiveness of our surveillance programmes.

15. For many people our privacy *is* our security. So much of our important information is stored online that losing control of it places us in real danger; from our login details to our address to our current location. Therefore, the starting point for balancing privacy and security must be that *surveillance should be based on suspicion*. And in the 21st Century, we must ensure that our digital communication and behaviour is given the same level of protection as our offline behaviour.

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?

16. "Internet communications" is vastly more complex than that phrase suggests. Internet communications include emails, websites visited, social networks, and with the rise of VOIP-

based apps, it also includes what we would traditionally consider to be texts and phonecalls. It is unrealistic and unreasonable to suggest that our online communication and behaviour should be treated any differently than our offline communication and behaviour.

17. Whilst CCTV carries with it certain benefits, particularly in relation to a reduction in car crime, it is conducted in a public place, whereas internet communications are far more intimate, often carried out in the home or in private, and any such surveillance is far more intrusive. Furthermore, there is public resistance to the current over-use of CCTV: the UK has some 5million such CCTV cameras, a substantial proportion of all those in the world. With the potential to use facial recognition software will this also be used for tracking? Or is this already happening? This underlines a fundamental concern with the development of new technologies and surveillance: there is little public debate and almost no Parliamentary approval for their use. A good principle was outlined by Sir David Omand, former head of GCHQ:

> *"Democratic legitimacy demands that, where new methods of intelligence gathering and use are to be introduced, they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved".*

How does the intrusion differ between data (the fact that a call took place between two numbers) as opposed to content (what was said in the call)?

18. With reams of metadata available about all of us, processing such data can be as revealing as accessing content; in my view, it should be considered quasi-content. The terminology of RIPA gives equivalence between what is available on the outside of an envelope to what is available from metadata, and as noted by the Joint Committee such equivalence is woefully out of date (at para 304). Whilst Royal Mail delivers 22 billion letters each year, this number is nothing compared to the 1 billion tweets, 23 billion Google searches, 70 billion Facebook views, 145 billion text messages, 160 billion instant messages, and the 2.4 trillion emails sent in UK each year. Our laws and our policies must reflect this monumental change.

19. As such, it is the *nature of the information* that is disclosed that should be given proper protection, not just the format in which it is stored or the method by which it is collected. The information that can be gained from metadata can be as revealing and intrusive as full surveillance; it contains a wealth of detail about an individual's familial, political, professional, religious, and sexual associations. As noted by US District Judge Leon when deciding that the use of such metadata was a breach of the 4th Amendment of the US Constitution:

> *'Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life'*

20. That view of metadata was reflected in the Report of the Joint Committee, at paragraphs 304-306, a view which is all the more relevant today:

> "304. The **language of RIPA is out of date**…[it requires] new definitions of communications data. The challenge will lie in creating definitions that will stand the test of time. There should be an urgent consultation with industry on changing the definitions and making them relevant…
>
> 305. **The definitions of use, subscriber and traffic data are particularly problematic. Subscriber data should not be a catch-all for data that does not meet the other definitions.** Currently the definition of subscriber data could be read to cover all sorts of data that social networks and other services keep on their customers which can be highly personal and is not traditionally thought of as communications data. A new

definition of subscriber data is needed that simply covers the basic subscriber checks that are the most commonly used…

306. **A new hierarchy of data types needs to be developed. Data should be divided into categories that reflect how intrusive each type of data is."**

21. If follows that where data is considered intrusive, it should be accorded the same statutory protections as intrusive surveillance under RIPA. There is an urgent need for a review of the definitions used in RIPA, and for the inclusion of a new hierarchy of data types based on how intrusive each type of data is; that hierarchy can then be given corresponding protection.

To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security?

22. Again, this all depends on the effectiveness of such monitoring. At present, the best available evidence from the Joint Committee and PCLOB (both quoted above) indicates that mass-surveillance is wholly ineffective at either unveiling previously unknown threats, saving lives, or making a "concrete difference in the outcome of a terrorism investigation." If such mass-surveillance is as ineffective as the evidence suggests, then there can be no necessity or proportionality in sacrificing our citizen's civil rights. It goes against our strong liberal tradition of no surveillance without suspicion. It is expensive, ineffective, intrusive, and in breach of our obligations under the Human Rights Act – obligations that are not undertaken for the benefit of a distant judiciary, but for the benefit of our fellow citizens and the foundations of our society.

Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted.

23. For all the reasons set out above, the answer is no; the legal framework is not remotely 'fit for purpose'. It was predominantly created before the advent of mass internet communications. The proportion of UK adults who regularly use the internet rose from 27% in 2000 to 84% in 2012[1]. Christopher Graham, Information Commissioner, said of RIPA that it was "drafted for the wiretap age"[2], an age that has long since passed. There are 130 mobile phone contracts per 100 people and 52% of mobile phone users have a smartphone, which aren't just phones. They are computers, GPS trackers, diaries, email devices, web browsers, cameras, and social networking devices. This has created an entirely new landscape for our intelligence and security agencies, a landscape with an outdated legislative map and no clear public policy direction.

24. This raises particular concerns in respect of s.94 of the Telecommunications Act 1984, which allows secret directions "of a general character" that are "in the interests of national security or relations with the government of a country or territory outside the United Kingdom." Given the complete transformation of the character, usage and capabilities of smartphones, s.94 has clearly been drawn far too broadly. Information on the use of s.94 does not have to be provided to Parliament, and it gags whoever the directions are served on. When the Joint Committee looked at this, we were unable to find any information about how the power was being used. There was no ability to have any oversight. This is a significant flaw which must be remedied with some urgency, and is certainly an issue which should be considered by the proposed review.

[2] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/907/11042602.htm

[2] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/907/11042602.htm

Deleted: ¶

25. The fact that our legislative framework is not fit for purpose is evidenced by the European Commission referring the UK government to the Court of Justice of the EU in September 2010 due to – among other things – its continuing failure to provide full statutory oversight for interception of communications. This is symptomatic of how low our standards have fallen compared to our European partners.[3]

26. Whilst the Coalition has amended RIPA so as to require local authorities to seek approval from a magistrates for surveillance and only to use such surveillance for serious crimes, such judicial approval is not required for the police, the security and intelligence services, and many other public authorities. We predominantly follow a process of self-authorisation or Executive authorization, which does not address the need for independent assessment of necessity and proportionality. While there are perhaps instances where Executive authorization is necessary, the preferred approach should be one of judicial authorisation of surveillance.

27. It is now time for a full post-legislative review of RIPA, the Intelligence Services Act 1994, and the Telecommunications Act 1984. And it is time for a full review of the policies, technology, structures, and oversight of Privacy and Security issues.

28. Such a review could lead to a Regulation of Surveillance Act as proposed by Justice in their 2011 report *'Freedom from Suspicion'.* Such an Act should be:

> "clear, coherent and no more complex than it needs to be; an Act that ensures that decisions about surveillance are made by independent judges rather than politicians; an Act that provides effective oversight rather than the seemingly endless proliferation of part-time commissioners; an Act that promotes accountability and public trust rather than corrodes it; and an Act that is principled, proportionate and effective."[4]

29. It has been repeatedly argued by a succession of Prime Ministers and Home Secretaries that the actions of the security and intelligence services are within the law. I do not doubt that the intention of the agencies is to remain within the law. But that simply demonstrates that the law itself is cast too widely, particularly given recent technological advances.

30. One of the failings of the draft Communications Data Bill was an absence of background information which would have enabled Parliamentarians to assess the case for new powers. The committee unanimously rejected the idea of simply accepting the word of the Home Office and the agencies for the need for new powers. If new powers are genuinely required, it is clear that the law must be reformed, and information provided sufficient for Parliamentarians to assess the necessity.

Independent Oversight – The Investigatory Powers Tribunal and the Commissioners

31. The Investigatory Powers Tribunal (IPT) is a perfect example of inadequate oversight. By 2011 it had only upheld 10 complaints of 1,100. The IPT was set up by RIPA in 2000, but it was not until 2003 that it even agreed to hold public hearings to determine legal issues in public, a cornerstone of our legal system. I agree with Chief Constable Nick Gargan, the former lead on surveillance for the Association of Chief Police Officers, when he described the IPT as a missed opportunity.[5]

32. Moreover, a fractured and patchy commissioner system does nothing to remedy the problem of ineffective oversight. Part 4 of RIPA provides for after-the-fact oversight by three different

[3] www.europa.eu/rapid/press-release_IP-10-1215_en.pdf
[4] p.16 Justice report: *Freedom from Suspicion* (2011)
[5] http://www.theguardian.com/commentisfree/libertycentral/2010/aug/02/surveillance-investigatory-powers-tribunal

bodies: the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Office of Surveillance Commissioners. Different activities are governed by different Commissioners, all of whom appear to be underfunded and resourced. Most recently the Chief Surveillance Commissioner, introducing his 2013 annual report, stressed that "the capability of [his] office has been reduced to a point where regular and frequent publication of guidance [was] not possible."[6]

33. Speaking to the Home Affairs Select Committee in 2011, it was made clear that the Commissioners, despite their overlapping roles, underpinned by the same principles and laws, had failed to create a unified strategy or even meet in the same room to discuss priorities, etc. Clearly we need a more unified system, a pooling of resources, increased funding, and improved access to technical expertise. The proposed review should consider replacing the IPT and the three Commissioners with a unified Surveillance Commission.

The ISC and Select Committees

34. With regards to scrutiny, oversight and accountability within Parliament, one of the biggest problems brought to light by the Snowden revelations is the lack of expertise and lack of information available to the Intelligence and Security Committee. It appears that the ISC was kept in the dark about several significant programmes, such as Tempora and Dishfire, by the very bodies they were set up to scrutinize.

35. The ISC's reports are redacted by the security services and the Prime Minister, with no indication as to whether it is done in the interests of genuine national security or just to avoid embarrassment for the Government. I agree with Sir Francis Richards, a former senior intelligence official, who said that it is "not a very good idea" for an ex-Minister to head the ISC. There is the problem of people being asked to scrutinise the consequences of decisions that they have made, and that makes it hard to develop the right sort of relationship.

36. Like the Surveillance Commissioners, the ISC is seriously under-resourced, and lacks the technical expertise necessary to carry out its functions. It is also not a proper Select Committee of Parliament. It generally sits in private and is shrouded by secrecy, which further undermines public confidence and public knowledge about the extent of the surveillance powers being used by the security and intelligence services. Of course, there will be times when private sessions will be necessary, but this should be the exception rather than the rule.

37. Lord Macdonald, the former DPP, recently gave a speech entitled *'Secrecy in Justice – Can it Ever be Fair?'* In it he called for radical reform of the ISC. His suggestions that it be a Joint Parliamentary Select Committee, with specific powers to obtain evidence including the power to obtain information, by summons, from outside parties, lay experts, ministers, civil servants and security chiefs, whilst being served by an independent secretariat with independent legal advice, and with the Chair coming from the Opposition Party, are all recommendations that I support.

38. Other select committees should also be involved in the scrutiny process. Sitting on the Home Affairs Select Committee ("**HASC**") I have shared the frustration of my colleagues firsthand when we haven't been able to get the information we need to properly hold the Government to account. There is a legitimate interest for other select committees to hear such evidence in order to fully carry out their functions, particularly where such issues cut across the remits of various Select Committees. The current HASC counter-terrorism inquiry is severly hampered by

[6] http://www.official-documents.gov.uk/document/hc1314/hc05/0577/0577.asp

the Home Secretary preventing the head of MI5 from giving evidence to us. It is not unusual for Ministers to give evidence to Select Committees other than their 'home' committee, and there is no reason why the same should not be true for agency heads, given appropriate safeguards.

Information Laundering

39. There needs to be strict controls on the use of "information laundering", that is the process by which national legislation is bypassed by means of the sharing of information or reciprocal surveillance programmes with the security and intelligence services of other nations. Given the minimal protections for citizens under the current legislative framework, it is essential that such information laundering is halted immediately, and that this issue is fully considered by the proposed review body so that recommendations and strict legislative controls can be put in place to prevent such information laundering occurring in future.

40. One of the biggest problems that we face is that the internet knows no boundaries, and cares little for jurisdiction. Thus the current legislative distinction between internal and external communications, when many servers are based overseas, makes a mockery of the limited protections in place for our citizens. Communication between two British Citizens inside Britain ought to be treated as internal communications, even if the routing goes overseas. This is why the emphasis of our legislation needs to move away from the method of collection of the information and towards how sensitive that information can be, with corresponding judicial or other controls on accessing such sensitive or intrusive information. At present the vagueness of the letter of the law is allowed to defeat the spirit of the law.

Dr. Julian Huppert
Member of Parliament for Cambridge
7 February 2014