Big Brother Watch: Intelligence and Security Committee submission

February 2014

Executive Summary

In a Democratic society, some secrecy is tolerated, as are some intrusions upon liberty and privacy, provided the legal framework is transparency, the oversight mechanisms robust and the overall sacrifices of liberty made with an appropriate level of understanding.

Recent revelations have made clear that the scale of intrusion on our privacy in the name of security, enabled by an explosion in digital communications and the computing resources available to the state.

Ministers have assured the public no central database of internet communications would be created. We now know it existed already. Parliament and the public were not informed by Ministers, the Intelligence and Security Committee or the Commissioners.

The legal framework has not kept pace with technology nor provided for robust oversight. Law has been interpreted to allow far more data to be collected than ever considered by Parliament, while the Commissioners, Investigatory Powers Tribunal and Intelligence and Security Committee have failed to inform the public or Parliament and offered ineffective means of redress. This entire system should be re-drawn, including Inspectors General, the ability to challenge surveillance in court and for far greater transparency about how powers are used, why, and by what organisation.

Equally, decisions were taken to weaken encryption and undermine cyber security to facilitate greater data gathering, while companies who complied with lawful requests were also targeted and their data flows hacked. Such offensive cyber action has taken place without a clear legal framework or debate.

We submit that the wider framework of authorisation and oversight of surveillance wholly fails to respect a separation of powers that is to be expected of a modern democracy. These questions are essential not only to reassure the British public but international users of the internet, many of whom are customers of British companies or are transmitting data through fibre optic cables that touch UK territory.

President Obama's NSA review panel recognised many of the issues involved in this arena and produced a thorough analysis of existing programmes, capabilities and concerns. This is a stark contrast to the convention of not discussing intelligence matters in the UK. This convention must be brought to an end, as it has now reached a farcical point where it prevents any meaningful debate in our outside of Parliament while also failing to provide any reassurance about legitimate surveillance activities.

Equally, the US continues to become more transparent, publishing its own figures and encouraging companies to do so. The Department of Justice has made clear that no surveillance power should be conducted without appropriate transparency to allow understanding of how powers are used. More than 40 legal opinions and rulings have now been published.

Secrecy not only undermines accountability, but also effectiveness. The National Audit Office previously concluded that secrecy was used to disguise incompetence in the projects to build the MI5 and MI6 buildings, rather than genuine national security interests. The same allegations have been made in the Special Immigration Appeals Court.

This contrast acutely highlights the failures in our system and places our digital economy at a disadvantage.

Finally, the Government should urgently address the question of whether it collects data in bulk on millions of British people.

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

1. Of course, it is the primary role of Government to protect its citizens. It is also equally obvious to state that Government should not be able to act without any limits, and it is part of the Government's role to ensure those acting on its authority do not exceed their legal authority.
2. As the Church Committee noted, *"Personal privacy is essential to liberty and the pursuit of happiness".* It is also essential to the functioning of a democracy – from a secret ballot to doctor-patient confidentiality, the ability of journalists to speak to sources and indeed constituents to speak to their elected representatives.
3. We would also highlight that the committee should not just be considering 'collective' security, but also individual security. Some actions may be considered for the benefit of the collective security but would compromise individual security, or the integrity of systems relied upon by society, like the internet or utility grids.
4. Revelations about GCHQ actively working to undermine encryption standards, along with the NSA's commercial partnerships to weaken security products, absolutely undermine individual security. They also make infrastructure and commercial systems like online banking more vulnerable. Equally, so too does offensive cyber action against companies who comply with lawful requests for data.
5. By weakening internet security, for example, the outcome may be the very opposite of that intended – that criminal or terrorist elements are able to access information that they would previously have been denied, and to use it for hostile purposes. The current situation seems to lack any systematic risk assessment or public debate.
6. Privacy is also a part of security, for example the concerns about a national ID card database becoming a 'honeypot' for hackers. If data is not collected, it cannot be lost, stolen or abused.
7. Indeed, writing in the foreword to a consultation on communications data legislation in September 2009, Jacqui Smith, then Home Secretary, wrote *"I also know that the balance between privacy and security is a delicate one, which is why this consultation explicitly rules out the option of setting up a single store of information for use in relation to communications data."*
8. Speaking to the Sun (article published April 2nd 2013) the Home Secretary Theresa May also recognised these concerns, saying *"There are no plans for any big government database."*
9. This raises a fundamental question. If people are to accept an intrusion on their personal privacy in the name of collective security, there is a balance to be struck. That balance, in a democratic society, should be through public debate, discussion and legislation. The public may not tolerate the intrusions those in power would wish to impose – whether 90 day detention without charge or ID cards – but that is the nature of democracy.
10. Therefore, it is essential that the committee addresses how, despite clear statements of intent of successive Governments that there would be no central database of communications data, let alone content, that under the Tempora programme such a database was created.

Privacy and different types of information

11. To compare CCTV and internet communications fundamentally fails to understand the nature of digital communications. CCTV images are difficult to index, sort and search. Digital communications are intended to be indexed and searched, allowing rapid identification and analysis. The only inhibition is the processing power required and as computer capabilities follow Moore's law and doubles roughly every two years, the price of huge processing power continues to fall.
12. We would also note the increasing doubt as to separations of content and non-content data. President Obama's NSA review panel noted that *"In a world of ever more complex technology, it is increasingly unclear whether the distinction between metadata ['communications data' in UK law] and other information carries much weight"*[1] while Bruce Schneier put it more succinctly; *"metadata equals surveillance."*[2]

Existing legal framework / specific legal changes:

13. *"The accumulation of all powers, legislative, executive, and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self-appointed, or elective, may justly be pronounced the very definition of tyranny."* James Madison, the Federalist Papers, Federalist No. 47, January 30, 1788.
14. This goes to the heart of the fundamental weakness of the current legal framework in Britain. Judicial oversight is entirely absent, save for local authority surveillance post Protection of Freedoms Act 2012, with the executive branch responsible for nominating members of the ISC and authorising surveillance warrants.
15. The various Commissioners are appointed by and report to the Prime Minister, not Parliament. Secretaries of State retain a veto on what material the ISC can see and its business is determined by a memorandum of understanding with the Prime Minister. Its reports are subject to redaction by the Prime Minister.
16. As former Court of Appeal judge Sir Stephen Sedley noted recently, we have 'a statutory surveillance scheme shrouded in secrecy, part of a growing constitutional model that raises the question as to whether the tripartite separation of powers, legislature, judicial and executive still holds good.' We do not consider it any longer in doubt.
17. Equally, there are many non-legal issues that are not should be reformed. For instance, the convention that Ministers do not comment on intelligence matters is increasingly absurd. For example:

    Mr David Davis: *To ask the Secretary of State for the Home Department whether she has given directions under Section 94 of the Telecommunications Act 1984 to the providers of telecommunications services for the acquisition of data in bulk relating to (a) thousands and (b) millions of people. [186135]*

    James Brokenshire*[holding answer 4 February 2014]:Section 94 of the Telecommunications Act 1984 states that the Secretary of State may issue directions in the interests of national security and, as with the practice of previous Governments, we do not comment on security matters.*

[1] NSA Review, page 120
[2] https://www.schneier.com/blog/archives/2013/09/metadata_equals.html

18. Either the Government is collecting data in bulk, or it is not. To confirm it is would not endanger national security, as the US Government has disclosed both the statutory provisions and the legal basis for its use of bulk data collection. Similar answers have been provided when Ministers have been asked for the specific legal authorities underpinning programmes in the public domain.

REGULATION:

19. The existing legal framework within the Regulation of Investigatory Powers Act has not kept pace with changes in technology. Definitions of data types, as well as broader considerations of intrusiveness and the potential for large-scale 'big data' type analysis, let alone the emergence of routine 'external' internet traffic, were not part of Parliament's deliberations.
20. There should be an explicit statutory bar on the acquisition of 'bulk' data relating to thousands or millions of British people, save for a situation reasonably considered an emergency. Such collection should be disclosed in a specific report by the relevant commissioner. Aggregating such data is a high risk strategy and yet there appears to have been no independent or democratic risk assessment of the invasive surveillance regime that has been adopted. We can only assume given the lack of any explicit denial that the British Government is operating similar bulk-collection schemes as the US Government, of the sort conducted under Section 215 of the PATRIOT Act.
21. Section 94 of the Telecommunications Act 1984 should be repealed – given it has not been cited by Ministers with relation to current activities of the intelligence services we must deduce it is out of date and not being used. If it is being used then the question must be asked how, and why it has not been referred to by Ministers when citing the Intelligence Services Act, Human Rights act and Regulation of Investigatory Powers Act.
22. Definitions in RIPA should be redrawn, including a specific definition of geolocation data. The definition of content should be revised to provide appropriate protection for private but not person-to-person communications (ie a Facebook status update).
23. Provisions for the interception of external communications s8(4) RIPA should be repealed and replaced with a narrow power to intercept communications where lawful co-operation agreements are not in place. A requirement of 'reasonable in focus, scope and breadth' test would be appropriate here and such orders should only be made where there is no other reasonable avenue of investigation available.
24. Protections for legally privileged or otherwise sensitive information should be introduced, for example patient-doctor confidentiality, investigative journalism and constituent to MP communications.
25. Definitions should be revised to expressly prohibit the designation of a telecommunications system, switch, router or other such technical intermediary as a 'premises' for the purpose of RIPA.
26. A statutory bar should be introduced to prohibit collection of information from a foreign intelligence agency if that information could be obtained from a lawful request to a commercial service provider.

AUTHORISATION

27. High level judicial authorisation should be introduced for authorisation of:
    a. Interception warrants

b. Directed surveillance warrants
c. The use of Covert Human Intelligence Sources (with regard to undercover operatives)
d. Intrusive surveillance
e. Certificated warrants not relating to an individual

28. Low level judicial authorisation should be introduced for the acquisition of communications data and restrictions on which type of organisation able to access it removed. We would note that technical expertise may not be suitably found in the Magistrates system and as we called for in our evidence to the Joint Committee on the Draft Communications Data Bill a new, central, national judicial authority should be established for this purpose to allow fast and efficient resolution of requests.

OVERSIGHT

The Intelligence and Security Committee

29. Calls for reform are not new. In 2004 the Foreign Affairs Select Committee called for the ISC to become a full Parliamentary committee, something backed by former Director of Public Prosecutions Lord MacDonald and many more. The question goes to the heart of the constitutional issue of oversight.
30. Assertions that the ISC is now free to conduct its business in entirely an unrestrained manner are false. At present the ISC is subject to significant restraint from the Prime Minister. These restraints include the Committee's work being restrained within a private Memorandum of Understanding with the Prime Minister and Secretaries of State being able to veto the information requests of the Committee.
31. We note the state of affairs that arose in 2000, when the Government of the day initially claimed publishing National Audit Office report into the significant overspend in constructing the MI5 and MI6 buildings would prejudice national security.
32. We also note the remarks in the 2007 Green Paper *'The Governance of Britain'* and the Justice and Security Green Paper (JSPG). Both included provisions to restore confidence in the ISC and highlighted several areas where improvements could be made. We remain concerned these proposals have not been taken forward in full.
33. For example, the Governance of Britain Green Paper included consideration that *"House of Commons debates on the Committee's reports, to be led by the Chair of the Committee rather than by a Government Minister, with reports also debated in the House of Lords"*
34. Furthermore the JSGP noted that *"The approach preferred by the ISC is that Parliament and not the Prime Minister should, in future, make the final decision on membership and the Chair of the ISC."* It goes on to discuss the Wright Committee proposals: "*ISC membership nominees be elected by secret ballot from within party groups, that the Chairman should be held by convention by a member of the majority party and should be elected by a secret ballot of the whole House of Commons with a process for the Prime Minister to pre-approve any individuals wishing to stand."*[3]
35. We fully support such a reform to the appointment process to the committee.

[3] Justice and Security Green Paper para 3.28 pp 43

36. We would also note that the ISC's increased budget of £1.3m represents roughly 0.07% of the Single Intelligence Account Budget and that even with increased staffing, it is unclear how the ISC is capable of performing an investigative role. We would highlight this should be considered alongside reform of the Commissioners and IPT and with the introduction of an Inspector General the ISC would not be doing investigative work and could focus on policy questions and specific lines of inquiry.
37. We also note and agree with the view expressed in 2011 by the Joint Committee on Human Rights that allegations of complicity in torture *"should be a wake up call to Ministers that the current arrangements [of review by the ISC] are not satisfactory".*
38. Those who have previously served as ministers with access to and a working relationship with the agencies should not be allowed to sit on the committee until two parliaments have elapsed from no longer holding such an office. The chair should be a member of the opposition.

Justice and Security Act 2013 (JSA)

39. Section 2 JSA should be repealed – the ISC should be free to determine its own investigations free from restraint from the Prime Minister or Secretaries of State
40. Section 3(3) and consequential provisions should be repealed – the Prime Minister should not have the ability to redact the committee's reports
41. Section 4 of Schedule 1 should be repealed and the committee given the power to request any information from any person as is required – Secretaries of State should not retain a veto without external, independent oversight
42. Section 7 of Schedule 1 should be repealed – if information of a criminal act is revealed to the committee, appropriate action should not be precluded. Separate provisions for whistle-blowers should be introduced.
43. Committee members should also be able to hire their own staff to work on their behalf within the committee. This 'designee' system is currently in place on the Senate Intelligence Committee of the US Congress, for example.

The Commissioners:

44. A short-term fix would be that Commissioners should report to Parliament, not the Prime Minister, and be free to direct their affairs as appropriate.
45. Equally, there are loopholes in the existing system. For example, the Interception of Communications Commissioner is intended to have oversight of the acquisition of communications data, however only has a statutory remit to monitor the acquisition of CD under the Regulation of Investigatory Powers Act. There are a number of other authorities used to acquire CD beyond RIPA.
46. However, we do not feel that the current Commissioner system commands public confidence. We note that in the Justice and Security Green Paper, proposals to extend the ISC's remit and authority should lead to reform of the Commissioner model. It stated: *"if a decision was made to have a parliamentary committee with significantly enhanced powers of oversight, particularly with regard to operational activity, then it would be inappropriate also to create a powerful Inspector-General."*[4]

[4] JSGP Para 3.51 pp 47

47. We believe that the Commissioner system should be wholly reformed and that an Inspector General model should be pursued. This should be taken alongside wholesale reform of the Investigatory Powers Tribunal.

Transparency:

Please find attached a fuller transparency paper in an appendix.

48. We agree with President Obama's review panel finding that *"there is a compelling need today for a serious and comprehensive re-examination of the balance between secrecy and transparency"*[5] which was reflected in recommendation ten of their report.
49. Legislation should be introduced to provide for the presentation of full and comprehensive statistics about the use of surveillance powers, and to allow consideration of their effectiveness.
50. Where data is not currently available, there should be a proactive duty on the individual agencies or organisations to record the information required. Similar obligations are already placed upon law enforcement and intelligence agencies as well as companies abroad, for example the German Telecommunications Act 1996, s 88(5) and 18 U.S.C. § 2516.
51. Data should be published on an annual basis and broken down by:
    f. The individual organisations
    g. What legal authority is being used
    h. What purpose the surveillance was undertaken or data accessed
52. Where CHIS, directed, intrusive or intercept powers were used, for what offence and whether the investigation resulted in a prosecution or conviction. This should follow the model already in place for wiretap statistics by the US Department of Justice. *(See appendix)*
53. Where certificates are signed, how much data was collected under them and how many citizens were affected
54. The US Government has committed to publishing the number of individuals affected by these requests and we believe the UK Government should also do so
55. The US Government has committed to allow companies to report on the data requests they receive – and how many are contested – and the UK should do the same
56. The total financial amounts paid under cost recovery mechanisms (as an annual, aggregate figure) broken down by capital expenditure, staffing costs and data access requests.
57. The issue of non-RIPA avenues being used to acquire data should be included until they are repealed by Parliament

Auditing

58. All public bodies carrying out surveillance functions should be required to conduct systematic audits on the use of their powers and publish the number of infringements and disciplinary procedures conducted.

Cyber Security and risk

59. All British agencies should be under a statutory duty to not act in a manner that would undermine the cyber security of British businesses or citizens. There should also be a statutory duty to notify the commercial manufacturers of software used by British citizens and businesses to notify those companies when vulnerabilities are discovered in a timely manner. It is unclear

[5] Page 125

who is responsible for assessing the risk to cyber security – in a wide sense – of offensive actions by GCHQ or other agencies. This would also include considerations of the data being held by agencies and the risks of it being compromised – for example, by a 29 year old US Government contractor in Hawaii.

60. British agencies should also be prohibited from taking steps to acquire information from companies who do co-operate with lawful requests for information, without the knowledge of those companies, unless there is an imminent threat to life or doing so would jeopardise an on-going investigation. In the latter scenario judicial authorisation should be sought.

REDRESS

61. The Investigatory Powers Tribunal should be abolished. Cases should be brought in open court subject to a closed material procedure or public interest immunity framework. Costs should be available to those who successfully challenge the surveillance directed at them. Public determinations on the facts of the case, subject to necessary technical redactions, should be available in every case.
62. Individuals who are subject to surveillance under RIPA should be legally notified when there is no risk to jeopardising an on-going investigation. This should ordinarily happen within 12 months of the conclusion of the investigation and allow for judicial extension in 6 month increments. The Committee must consider how citizens are able to seek redress if they have no means to find out if they have been subjected to surveillance.
63. Such provisions are in use in other countries without detriment to national security. The German Constitutional Court's decision in the *Grosser Lauschangriff* case, rightly emphasised the fundamental nature of the right of an individual to be informed that she had been placed under surveillance.
64. MPs should be empowered to receive whistle-blower complaints and the national security exemption in the Public Interests Disclosure Act should be abolished.
65. Legal advice on the validity of any programme that allows data to be collected without suspicion, subject to essential redactions, should be published. We note the US Government has now declassified more than 40 such legal opinions and judgements.