Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament

Caspar Bowden is an independent advocate for information privacy rights, and public understanding of privacy research in computer science. He is a specialist in EU Data Protection, European and US surveillance law, PET research, identity management, and information ethics. He is author of 2013 EU Parliament inquiry briefing[1] on the US FISA law, and co-authored the 2012 Note on privacy and Cloud computing[2] (which anticipated the infringements to EU data sovereignty disclosed by Edward Snowden). For nine years he was Chief Privacy Adviser for Microsoft for forty countries, and previously co-founded and was first director of the Foundation for Information Policy Research (www.fipr.org). He was an expert adviser for UK Parliamentary legislation, author of the RIP Act Information Centre (www.fipr.org/rip/), and co-organized six public conferences on encryption, data retention, and interception policy. He has previous careers in financial engineering and risk management, and software engineering (systems, 3D games, applied cryptography), including work with Goldman Sachs, Microsoft Consulting Services, Acorn, Research Machines, and IBM. He founded the Award for Outstanding Research in Privacy Enhancing Technologies, is a fellow of the British Computer Society, and a member of the advisory bodies of several civil society associations.

There is no Executive Summary

The ISC would welcome written evidence on the following issues:

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

1. Balance is a misleading metaphor. It tends to connote an unstable equilibrium with a single balance point on a linear scale. The policy options may include combinations resulting in different equilibria which are metastable, stable or unstable in the context of post-Snowden policy on surveillance.
2. For example, one reaction to Snowden might be to intensify surveillance and provide GCHQ with authority[3] to monitor every

1 *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, 16-09-2013, Caspar Bowden, intr. Didier Bigo http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

2 *Fighting Cyber Crime and Protecting Privacy in the Cloud*, 15-10-2012, Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, Amandine Scherrer http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf

3 This might even be possible today depending on nice interpretations of the interactions of the Intelligence Services Act and RIPA

webcam in every laptop in the UK. If done overtly, this would likely produce a cowed population living under a sense of oppression, but amenable to further intensification of surveillance down a slippery slope. If done covertly, it raises the question why is that intuitively unacceptable (assuming it is), yet qualitatively similar surveillance of private life through metadata analysis (see below) seems more politically palatable? Does this merely reflect public and legislative (lack of) comprehension or technical imagination?

3. Another option would be to end blanket collection of metadata, and switch to a regime of targeted preservation of metadata about defined suspect groups on a lawful basis. This might assuage public concerns, and leave a bright and comprehensible line for public understanding of the permitted limits of mass-collection.

4. Therefore a key factor in deciding "balance" is the long-term effect on political and democratic culture, and maximising short-term public consent to the demands of a security apparatus is not necessarily the wisest course, given that we are in uncharted waters.

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

5. The Internet is not a public space, it is composed of many layers of private, social and public realms. CCTV surveillance is both overt and confined to public space, or private and social spaces lawfully subject to another's control. In contrast, the controversial aspects of state mass-surveillance are that it is covert and conducted over wholly or partially private spaces of data and communications.

6. I draw ISC's attention to my 2002 paper on ATCSA data retention[4], which is based on the metaphor that retention is like having a CCTV camera installed "inside your head" i.e. that it invades the subjective interior space of our thoughts and intentions, because these can be inferred from Internet and other metadata.

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?

---

4 Caspar Bowden, *CCTV for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*, 1 Duke Law & Technology Review 1-7 (2002) http://scholarship.law.duke.edu/dltr/vol1/iss1/47

7. It is incompatible with human rights in a democracy to collect all communications or metadata all the time indiscriminately. The essence of the freedom conferred by the right to private life is that infringements must be justified and exceptional. As the Romanian constitutional court[5] expressed it, the continuous limitation of the right to privacy [implied by mass-collection of metadata] empties the principle, by making the exception into the rule.

8. This principle against blanket data collection might be suspended in time of war or concrete imminent threat (as found by the German Constitutional Court in their *Rasterfahndung* decision[6]) but it cannot be the normal mode of surveillance in a democracy.

9. It is a strange fact that the obvious alternative policy to blanket **retention** has never been explored or publicly developed by the Home Office in 15 years, that of targeted and selective **preservation** of metadata about a defined (but dynamic) list of suspects. In fact this legal capability is provided in Pt.1 Ch.2 of RIPA, and is necessary to give effect to obligations under the Council of Europe Cybercrime Treaty. However these powers are generally only used in particular investigations, because of course UK policy developed to ensure such data was retained about the entire population.

10. However to assess whether blanket data retention is proportionate in the sense of the Human Rights Act requires a comparison to a hypothetical alternate regime in which preservation powers are exercised systematically over a target list that can be rationally justified by criminological research. For example, for offences for which recidivism is commonplace, it could be proportionate to release offenders on license under the condition of metadata preservation (with deterrent penalties for evasion).

11. If it is argued that such targeted preservation could stigmatize certain groups or that data about innocent persons would be caught, it must be pointed out that is much better than the current situation in which everybody's data is collected indiscriminately all of the time for no particular reason whatsoever.

---

5 E Kosta, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, (2013) 10:3 SCRIPTed 339 http://script-ed.org/?p=1163

6 BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. (1 - 184), http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html

12. Suppose that 95% of the effectiveness of the data retention regime could be achieved by intelligently targeting 1% of the population? It would be very hard to argue that increasing the amount of data one hundred times to achieve an extra 5% effect, was justifiably proportionate

13. The residuum of 5% would include "hard cases" of opportunistic crime and terrorism that might have been prevented, but in a more limited sense than usually understood. Access to the "time machine" provided by blanket retention can only help investigate terror networks and the causes of terrorist crimes. They cannot prevent acts of terrorism infallibly merely because data about everyone is being collected.

14. This then is the true balance: the breaching of the principle against blanket collection which voids the essence of the right to private life, or a lawful regime of targeted and proportionate preservation, which nevertheless might result in a residuum of crimes that might have been prevented or detected under a blanket retention regime.

15. Law enforcement agencies' appraisal of necessity cannot be taken at face value. In evidence to the Joint Committee on the Communications Data Bill, the Interception Commissioner pre-emptively distanced himself from "case studies" included in his annual report which he said were provided by the Home Office. In my evidence submission[7] I demonstrated how five out of six studies obviously failed to demonstrate necessity (the other was inconclusive), and that another anecdote offered by police in oral evidence was diametrically misleading.

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

16. The distinction is not a simple one and cannot be made by assigning a sensitivity level to data types in isolation.

17. The pattern of association between individuals and websites and geographic locations reveal a map[8] of private life which includes intimate and personal contacts, political activities, and business

7 Caspar Bowden , 23rd August 2012, *Submission to the Joint Committee on the draft Communications Data Bill* http://www.parliament.uk/documents/joint-committees/communications-data/written%20evidence%20Volume.pdf

8 CCTV inside head ibid.

and professional relationships[9].

18. Global-scale databases of such relationships have been assembled on non-US citizens[10] by the NSA since at least 9/11, and the power to analyse and exploit such information automatically for foreign policy and political[11] purposes has been demonstrated in Snowden material

19. In contrast, speech-recognition of continuous voice streams (without training for particular speakers and at telephone quality bandwidths) remains a very hard problem in computer science[12]. However in the popular culture and early para-politics of the surveillance state, the main threat was portrayed as coming from computers which could scan and transcribe human speech. This image of the surveillance threat turned out to be a dead-end, but still colours public discourse .

20. It is harder to conceive of the surveillance power of traffic (metadata) analysis because of its scale and abstraction. Data-mining systems for national security use are designed to link any common identifying numbers of any kind, and look for correlations, geographical intersections of location data[13], and patterns in online social relationships. Unless special precautions are taken, few personal secrets of everyday life would withstand close analysis of metadata.

21. Critics of state mass-surveillance made these arguments[14] before

---

9 Evidence of Prof. Ed Felten to Senate Judiciary Committee hearing on *Continued Oversight of the Foreign Intelligence Surveillance Act*, October 2, 2013 www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf

10 *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, by James Risen and Laura Poitras, New York Times September 28, 2013 http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=2&_r=0&smid=tw-bna&pagewanted=all

11 *Snowden Docs: British Spies Used Sex and 'Dirty Tricks'*, NBC News Feb 7th 2014, by Matthew Cole, Richard Esposito, Mark Schone and Glenn Greenwald http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

12 As opposed to speaker identification via a voiceprint, which has been feasible and deployed since 1980s.

13 *NSA tracking cellphone locations worldwide, Snowden documents show* (CO-TRAVELER) Washington Post 4th Dec 2013, by Barton Gellman and Ashkan Soltani http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

14 *Unprecedented Safeguards For Unprecedented Capabilities* - Caspar Bowden, remarks for Hoover Institution National Security Forum Conference, 7th Dec 1999 http://www.fipr.org/publications/hoover.html

the emergence of online social networks and smart-phones (and post-9/11 stimulus to the surveillance-industrial complex) but in 2000 legislators seemed content that RIPA did not mandate blanket data retention, and Labour Minsters made three promises they would not do so[15].

22. The Labour administration broke these pre-election promises after 9/11, and debate on the mandatory data-retention provisions in Ch.11 ATCSA (the "UK PATRIOT Act") resulted in the longest game of Parliamentary ping-pong between Lords and Commons in 2001, ending in the passage of a mangled version of an amendment devised by the author. The intention was to restrict data retention to that which was necessary for national security, leaving open the interpretation of how broadly or selectively this might be done, but with the tacit implication that blanket retention was unlawful.

23. In 2002 the Information Commissioner obtained an Opinion from Ben Emmerson QC which essentially approved that the (mangled wording of the) national security purpose in ATCSA could necessitate blanket collection, and decided not to get involved. This was a momentous point in UK data retention policy, but the reasoning has only been publicly available[16] following a recent FOI request to the ICO.

b) 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.

24. The most glaring lacuna in the legal regime is any regulation of the modality of analysis of data in bulk. Data processing for national security purposes is exempted from almost all control under the Data Protection Act 1998[17]. The Interception Commissioner could in theory object that certain forms of data-mining were incompatible with the Human Rights Act, but there is no evidence he has done so, and this would require him to construct novel and complex theories of technology-dependent jurisprudence in isolation and in secret. Any complaint to the Investigatory Powers Tribunal is unlikely to reach these arcana, as the complainant (and the IPT) would have to know something about the complex systems involved to raise the issue.

25. In general, once data has been lawfully acquired for national

15 CCTV inside head 2001 ibid.

16 https://www.whatdotheyknow.com/request/qcs_opinion_on_data_retention_in

17 s.28 http://www.legislation.gov.uk/ukpga/1998/29/section/28

security processing there are no (publicly known) limitations on the nature of algorithms or their scale of application which are considered lawful or unlawful, other than the familiar ECHR rubrics of necessity and proportionality.

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

26. One of the least understood or examined parts of RIPA is s.16, which purportedly deals with "extra safeguards" in respect of mass-surveillance of "external" communications. The author wrote two[18] briefing papers as House of Lords Adviser to Opposition parties which resulted in substantial debate of this clause.

27. s.16 is drafted with fiendish complexity[19], but essentially creates a "third kind" of warrant apart from the ordinary "domestic" interception warrant for use inside the UK, and the GCHQ "trawling warrant" for external communications. The third kind of warrant authorizes GCHQ to scan all the nominally external communications it captures, to target a **person** known to be inside the UK. It was thus not a safeguard at all, but a hugely significant increase in powers beyond the popular conception that GCHQ was only involved in foreign and international surveillance. It is fair to say that almost no members of either House or the public or media appreciated this at the time of legislation (or subsequently). Despite attempts to explain to news media, it was apparently just too complicated to report.

28. As was already foreseen in the debates[20] in 2000, in practice external communications might contain a huge amount of data about persons and activities wholly within the UK, a situation much exacerbated since by the concentration of online services in a few big US-based companies.

29. The Interception Commissioner has never remarked or reported on the

---

18 http://www.fipr.org/rip/CertificatedAndOverlapping.htm and http://www.fipr.org/rip/OverRideCertificates.htm

19 A senior government official confirmed to me privately that it was intentionally drafted for maximum obscurity

20 *Lords Hansard 19 Jun 2000 : from Column 97* http://www.publications.parliament.uk/pa/ld199900/ldhansrd/vo000619/text/00619-20.htm and *Lords Hansard 12 Jul 2000 : from Column 318* http://www.publications.parliament.uk/pa/ld199900/ldhansrd/vo000712/text/00712-21.htm

use of s.16, nor has there been any other policy or legal commentary of significance since enactment. Yet it seems likely that the interpretation and use of s.16 is critical to understanding the impact of the reported TEMPORA system on the privacy of those within the UK

30. s.16 appears to have been designed to close a leap of logic by Lord Lloyd in the first[21] Interception Commissioner's report of 1986. Under the previous IOCA legislation's corresponding but more limiting section, such "internal targeting" by GCHQ was allowed **only for counter-terror** purposes. He therefore invented a non-statutory procedure to make this lawful for other purposes which he called an "overlapping warrant". This was a domestic warrant made out for the targeted person's (both internal and external) communications.

31. Intentionally or otherwise, in doing so Lord Lloyd elided the problem that GCHQ might only have discovered the identity of the person they wished to target inside the UK, through mass-surveillance of external communications by some other (non-personal) "factor". In this way a person inside the UK could fall under much more intensive surveillance through the fruit of the poisoned tree of GCHQ "external" mass-surveillance. To this problem, Lord Bassam replied[22] to questions in the RIPA debates that "*it would of course be unlawful to **seek** to catch internal communications in the absence of an overlapping warrant or a certificate complying with*" section 16. In this way, RIPA s.16 facially legitimated a huge (if little appreciated) extension of GCHQ's domestic surveillance power, beyond counter-terrorism, for the full range of interception purposes.

32. This example of s.16 is offered to illustrate how redrafting RIPA and closing the gap between the public understanding of surveillance powers and the reality is no simple matter, given a history of deceptive drafting and enactment with some degree of long-standing complicity by party leaderships not to delve into these matters in Parliament.

---

21 Paras 33-36, 1986/87 Cm 108 *Interception of Communications Act 1985. Chapter 56. Report of the commissioner for 1986* https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/iocc/IoCC%201986.pdf

22 Lord Bassam of Brighton to Lord Phillips of Sudbury, 4th July 2000, *re: RIP Bill Committee: Clause 15* http://www.fipr.org/rip/Bassam%20reply%20to%20Phillips%20on%20S.15.3.htm

33. Some proposals for specific reforms were included in my submission to the CDB Joint Committee in 2012[23]. Further suggestions may be offered in oral evidence to the ISC.

23 ibid.