Intelligence and Security Committee
Privacy and Security Inquiry

Executive Summary

1. The challenges facing the intelligence agencies in an era of big data are on public record and have been the subject of discussion over the past decade. The conversation has largely taken place behind closed doors between democratically elected officials and special interest groups: this might now change and for the better.

2. We live in a surveillance society. But Government no longer has the monopoly on surveillance. The private sector mines and trades our personal data everyday without our knowledge, while the ubiquitous smartphone has given citizens the means to record, relay and relish their most private moments in public.

3. The era of big data is also profoundly changing the way the public and private sectors think about information - none more so than Internet companies:

    - Google produces more than 24 petabytes of data per day; (a volume that is thousands of times the quantity of all printed material in the US Library of Congress);
    - Facebook gets more than 10 million new photos uploaded every hour;
    - 800 million monthly users of Google's You Tube service upload over an hour of video every second: and,
    - In 2012 Twitter saw 400 million tweets a day.[1]

4. The Intelligence and Security Committee's inquiry into privacy and security was triggered by the Snowden revelations – but it is only the latest inquiry in a long line of reports, reviews, and debates on the subject. As long as technology continues to evolve, it will not be the last. As technology and cultures change so will our understanding of privacy and the priorities we value in the name of national security.

5. The evolution in technology and communications is reshaping our intelligence agencies for an age of information. In 2013 1.004 billion smartphones were shipped across the globe marking a 38.4% increase from the previous year. Not surprisingly intelligence agencies are keen to understand how this surge in demand for smartphones will impact on their roles and capabilities. GCHQ slides[2] leaked by Edward Snowden suggest GCHQ is to develop its capabilities in order to meet the scale of the challenge facing it.

6. The revelations by Edward Snowden, an American NSA contractor, have severely jeopardized UK intelligence. If Snowden had taken a select number of 'files' to demonstrate that NSA was collecting the telephone records of tens of millions of Americans and had presented this to the Permanent Select Committee on Intelligence in the US Congress and/or a US newspaper he may well have been heralded as a savior of American's privacy - but he didn't.

7. According to media reporting Snowden used Web crawler, a cheap software package designed to index and back up websites, to scour the NSA's data and return a trove of confidential documents.[3] We think Snowden accessed roughly 1.7 million files including 58,000 highly classified UK intelligence documents. Snowden demonstrated the very same traits as the organisation he was so keen to hold to account when he began collecting highly classified files in an indiscriminate and bulk fashion.

8. A key issue raised by Snowden's revelations in relation to the surge in smartphone use and the impact on intelligence agencies is whether it ought to be public knowledge that GCHQ were considering the development of two specific capabilities under their Mobile Applications Project? Arguably not. But are we confident that the ISC has oversight of GCHQ's capabilities and future ambitions in this space?

---

[1] Viktor Mayer-Schonberger and Kenneth Cukier, Big Data, John Murray publishers, 2013
[2] Mobile Theme Briefing http://cryptome.org/2014/01/gchq-mobile-theme.pdf, 28 May 2010
[3] Snowden used cheap software to plunder NSA data,9th February 2014,
http://swampland.time.com/2014/02/09/snowden-nsa-cheap-software/

9. The 2011-2012 Annual Report suggests some understanding that ICT was (and remains) a major priority for GCHQ and that according to a member of GCHQ "it's also about new accesses, new tradecraft, new techniques and new tools … the challenge is for us to make the most of that technology lead that we've got to compensate for some of these small reductions in effort."[4]

10. This short submission is divided into three sections; the first section sketches out the current level of surveillance and 'sousveillance' in the UK today; the second section provides a brief analysis of why the Snowden revelations have not had the kind of impact in the UK they have in the US; the third section describes what privacy means today.

A) The Surveillance Society

11. We live in a surveillance society. While some commentators have argued that successive British governments have made the UK the world capital of privacy intrusion[5], governments do not have a monopoly on surveillance. The private sector mines and trades our personal data everyday without our knowledge, while the ubiquitous smartphone has given citizens the means to record, relay and relish their most private moments in public.

12. The British Security Industry Authority (BSIA) estimate there are up to 5.9 million closed-circuit television cameras in the country, including 750,000 in "sensitive locations" such as schools, hospitals and care homes. The survey's maximum estimate works out at one [camera] for every 11 people in the UK.[6] According to one report 'virtually every single Local Authority system and number of cameras in the systems has grown as a result of public request and pressure to extend or develop the system.'[7]

13. It is not just about people watching us. Every day we leave a 'footprint' of personal information for others to see. Our digital exhaust includes how long we view content online, how often we visit different sites and what we seek. The majority of consumers in the UK allow retailers to use some of their personal data in order to present personalized and targeted products, services, recommendations and offers. In one survey, consumers were asked to choose between personalized shopping experiences based on their past consumer behavior, or non-personalized experiences in exchange for having retailers not track their data, 64 percent of respondents said they'd prefer the personalized experience.[8] We are keen to reap the benefits this accessibility and openness affords.

14. Our information is increasingly relied upon by the public and private sector to make important judgments about people. There is now more opportunity than ever for those decisions to be made without our consent or involvement. Those decisions will ultimately influence our futures in fundamental ways, from the kinds of services we are offered or are entitled to, or our desire for a realm of privacy, through to our ability to secure credit. [9]

15. The issue of consent will only become more of a problem as we begin to understand the implications of big data. According to Viktor Mayer-Shonberger and Kenneth Cukier, the three strategies long used to ensure privacy – individual notice and consent, opting out and anonymisation, have lost

[4] Para 65, ISC Annual Report, 2011-2012, July 2012, Cm 8403
[5] At least according to Simon Jenkins: 'Here's proof: The Innocents do have something to fear' http://www.theguardian.com/commentisfree/2009/apr/01/jacqui-smith-expenses 1st April 2009
[6] David Barrett, One surveillance camera for every 11 people in Britain, says CCTV survey, 10 Jul 2013 http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html
[7] Indpendent public opinion report conducted by TNS Research International for the CCTV User Group, 2010 https://www.cctvusergroup.com/downloads/file/An%20Independent%20Public%20Opinion%20Survey%20in%20Public%20attitudes%20to%20Public%20Space%20CCTV%20Final%20Version.pdf ,
[8] Why Consumers are increasingly willing to trade data for personalisation http://www.digitaltrends.com/social-media/why-consumers-are-increasingly-willing-to-trade-data-for-personalization/ 10 December 2012
[9] Peter Bradwell & Niamh Gallagher, FYI: The new politics of personal information, Demos July 2007 http://www.demos.co.uk/publications/fyi

much of their effectiveness, not least because big data analysis involves finding correlations and patterns that might otherwise not be observable. It almost necessarily involves uses of data that were not anticipated at the time the data were collected.[10]

16. As Jamie Bartlett and others have suggested what may seem innocuous, even worthless information — shopping, musical preferences, holiday destinations — is seized on by the digital scavengers who sift through cyberspace looking for information they can sell: a mobile phone number, a private email address.[11]

17. This industry is legal and lucrative. Data is the currency of the information age. As *The Economist* recently put it: 'abolishing privacy is the next big trend in American shopping. Store bosses dream of identifying shoppers by their smartphones or with cameras and facial-recognition software.'[12] Piecing together the fragments of individual lives bit by byte has allowed companies to create pictures of us that they can repackage and sell to the highest bidder. For example a GPS service designed to help drivers find quick routes was also selling the information to the Dutch police, who could use it to work out who was breaking local speed limits. Each year, the Little Brothers get cleverer.[13]

18. Surveillance has changed in the era of big data. "In the spirit of Google or Facebook, the new thinking is that people are the sum of their social relationships, online interactions and connections with content. In order to fully investigate an individual, analysts need to look at the widest possible penumbra of data that surrounds the person – not just whom they know, but whom those people know too… this was technically difficult in the past when investigators attached alligator clips to phone wires – today its relatively easy.[14]

19. The fact that the intelligence agencies have been investing in capabilities to respond to the data deluge was the subject of a Congressional Research Service report in January 2001 titled *NSA: Issues for Congress*. The report said:

> NSA's efforts are being challenged by the multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states... In some cases, NSA must resort to analyses of traffic patterns–who is communicating with whom, when, and how often–to provide information that may not be obtainable through breaking of codes and reading of plaintext.

B) The Snowden Revelations

20. In a White House conference with reporters in August 2013 President Obama suggested that given the history of abuse by government it was right to ask questions about surveillance - particularly as technology is reshaping citizen's lives. Are we in the same situation in the UK?

21. One way to navigate this debate is to ask ourselves the degree to which we, as citizens, have confidence in our government institutions to operate effectively. Do we trust the British system of oversight of our intelligence agencies, and the government departments who are responsible for them?

---

[10] Thomas M. Lenard and Paul H. Rubin, The Big Data Revolution: Privacy Considerations, December 2013 https://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf

[11] Jamie Bartlett, iSPY: How the internet buys and sells your secrets, The Telegraph, December 2013, http://www.spectator.co.uk/features/9093961/little-brothers-are-watching-you/

[12] Snooper blooper, Lexington, The Economist, http://www.economist.com/news/united-states/21592654-revelations-about-cyber-espionage-dismay-barack-obamas-most-loyal-fans-snooper-blooper

[13] Jamie Bartlett, iSPY: How the internet buys and sells your secrets, The Telegraph, December 2013, http://www.spectator.co.uk/features/9093961/little-brothers-are-watching-you/

[14] Viktor Mayer-Schonberger and Kenneth Cukier, Big Data, John Murray publishers, 2013

22. Trust in government ebbs and flows. According to a recent survey the majority of the British public is largely supportive of the current situation [regarding surveillance measures] with only 19% of the public believing that the British security services should cut back their surveillance powers.[15] 43% of the British public believes the leaks by Edward Snowden were a bad thing.[16]

23. This may go some way to explaining why the debate in the UK has been fairly mute – to the bafflement of some newspaper editors. Insofar as the initial news story was framed as a US problem, with the focus on the NSA collection of telephone records of tens of millions of Americans, the public backlash and the White House review on intelligence and communications technology, this is perhaps not surprising. Moreover, save for a possible review of the D-Notice system in the future, the subsequent news stories in the UK has largely focused on the impact of the revelations on other European governments, Russia, Brazil and further afield. One reason for this is provided by Gideon Rachman in the *Financial Times*:

> "Most British citizens accept and, indeed, celebrate the role of the state in keeping the country free and independent – and the role of the intelligence services has historically been integral to that task. The threat from terrorism, as witnessed in the London bombings of 2005, has only increased the awareness of the need for good intelligence. Everybody knows that there is no military solution to the "war on terror."[17]

24. There is another reason why the debate on Snowden's revelations in the UK is more muted. The Snowden saga is also a story about an American contractor who stole American and British secrets. Among the 1.7 million documents Snowden downloaded (the vast majority of which have not yet been, and maybe never will be, made public) many are highly sensitive, specific intelligence reports, as well as current and historic requirements the White House has given the agency to guide its collection activities.[18] A large majority are likely to be about sensitive military mission overseas carried out under the auspices of Joint Special Operations Command. Other documents that Snowden leaked which have no impact on the privacy of citizens (in the US and UK) include:

    - The classified portions of the U.S. intelligence budget, detailing how much the US Government spend and where on efforts to spy on terror groups and foreign states.
    - US cyber-warfare capabilities and targets and the revelation that the U.S. launched 231 cyber-attacks against "top-priority targets, which former officials say include adversaries such as Iran, Russia, China and North Korea.
    - The extent and methods of US spying on China.
    - Revealing NSA intercepts and CIA stations in Latin America.
    - Revealing a U.K. secret internet-monitoring station in the Middle East.
    - What the US Government knows about al-Qaeda efforts to hack US drones.
    - The NSA's ability to intercept the e-mail of al-Qaeda operative Hassan Ghul.
    - NSA's collecting data on the pornography habits of Muslim extremist leaders in order to discredit them.[19]

25. Snowden unveiled the intimate architecture and entrenched networks of the most secretive postwar institution, the "Five Eyes" intelligence alliance binding the US with the UK, Canada, Australia and New Zealand. Snowden's documents have disclosed so much about its operations, from the national leaders bugged to the mind-boggling masses of data trawled in search of terror targets, that the extraordinary new material still pouring out is losing its ability to shock.[20]

---

[15] Little appetite for scaling back surveillance, YouGov Survey, October 13, 2013, http://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/
[16] Ibid
[17] Gideon Rachman, Why the British like their spies, Financial Times, 10 November, 2013
[18] Walter Pincus, Snowden still holding keys to the kingdom, Washington Post, 19 December 2013 http://www.washingtonpost.com/world/national-security/snowden-still-holding-keys-to-the-kingdom/2013/12/18/b91d29a2-6761-11e3-8b5b-a77187b716a3_story.html
[19] The Extent of the Snowden Disclosures, Lawfare Blog, 6 January 2014, http://www.lawfareblog.com/2014/01/the-extent-of-the-snowden-disclosures/#.UvuHdLQfHKA
[20] The Snowden Files', by Luke Harding reviewed by Richard McGregor, Financial Times, 5th February 2014

26. A critical issue that the Snowden revelations have raised from a UK perspective is that of the current oversight mechanisms of the Intelligence Agencies. With the evolution of technology and big data much more could *and should* have been done to understand the work of GCHQ in this domain. This is not necessarily because the government and wider public believe what is happening is fundamentally wrong or disproportionate. Instead it because we feel that we must ensure that what is being done in our name can be accounted for, is proportionate to the requirements that have been identified and, in these austere times, is financially sustainable. This is particularly the case when it comes to large data mining programmes where the rationale and indeed benefits have not been made publicly clear – even in sanitized form.

27. The Snowden revelations have raised questions about the balance between national security and personal privacy which the next section discusses. However it is important to note that the terms of the debate have been widely misunderstood.

C) The end of privacy?

28. The Snowden revelations do not spell the end of privacy. Our perceptions of what constitutes privacy have already radically changed, and with it our sense of what privacy means in today's open society.[21] The evolution in technology and how we as citizens and consumers are challenging our views on privacy and a public discussion on the issues is sorely needed. But the evidence shows most of us are 'privacy pragmatists' – prepared to provide personal information for enhanced services or other benefits such as security.[22] What we, as citizens, want to ensure are that the safeguards in place to ensure our privacy and our personal information are not illegally sold for criminal enterprise, hacked, leaked or lost.

29. We rarely make an objective decision about how much of our privacy we are willing to trade for goods or services we receive in return. Privacy is thus often reduced to a mere procedural question in the commercial context – where it is up to us to pursue the details and 'opt out' if such an option is offered.[23] From a traditional sense of privacy such as freedom from intervention into one's personal space, we have reached a point where our privacy has become a commodity to be exchanged for goods or services.

30. Privacy should be understood as an elastic concept that acts as a gateway to a cluster of values such as dignity, trust, honesty, intimacy and anonymity. And herein lies the problem. We use outdated frames of reference that are no longer adequate to discuss the contemporary landscape of privacy concerns or re-frame complex issues about data protection and vulnerability in other terms.[24]

D) Conclusion

31. In conclusion it is worth reflecting on why security is often seen to be so powerful in relation to privacy. As Jennifer Chandler, an Associate Professor at the University of Ottawa explains: The reasons suggested for security's rhetorical power are:

    - Security in the sense of physical survival is a prerequisite for the enjoyment of other values such as privacy;
    - Human risk perception may be subject to cognitive biases than cause us to overestimate the risk of terrorism and to have difficulty perceiving the harm of reduced privacy;
    - We are apt to think that it is better to have more rather than less security, while this is not true for privacy;

[21] Edwards and Fieschi (Eds), UK Confidential, Demos, 2008
[22] Perri 6, The Future of Privacy, Private Life and Public Policy, Vol.1, Demos, 1998
[23] Edwards and Fieschi (Eds), UK Confidential, Demos, 2008
[24] Ibid

- To the extent that national security is obtained at the expense of the privacy of a minority, the majority is more likely not to perceive or care about the privacy costs and thus will regard the security measures as reasonable: and,
- Social-psychological reactions of solidarity following an external attack may cause people to be more willing to set aside individual rights claims such as privacy for a perceived collective benefit in terms of national security.[25]

32. Surveillance is a necessary activity in the fight against terrorism and serious crime and plays a vital part in our national security. But the legal framework in the UK has routinely struggled to keep pace[26], a fact recognized by the current government which, in the context of communications data, has argued that 'proportionality, a clear legal framework and rigorous scrutiny and oversight are at the heart of this.'[27]

33. Likewise the debate on privacy and security has not kept pace with the evolution in technology or indeed the changing threat picture in the UK. As such a more transparent and inclusive debate is long overdue. A more informed public – one that is empowered by information – is a valuable asset in a democracy.

34. To have a debate however we need to agree a starting point. Too often government, media and public have understood the tradeoff between security and privacy as a simple binary equation: more security equals less privacy and vice versa. This is never the case. Our perceptions of security and privacy will be very different today than 20 years ago and this must be taken into account.

35. The constant interaction between security and privacy reflects the changing threat picture, developments in technology and the public's response to these drivers. The fear then is in an era of big data and complex threats citizens are not being empowered with the information they require to understand the actions of government or indeed the intelligence agencies.

36. The nuances of trading security for privacy are rarely discussed. As one Minister recently put it: 'There is not always a direct trade-off between security and civil liberties. They are often mutually reinforcing: insecurity tends to erode civil liberties, and the denial of civil liberties often fuels insecurity.'[28] Just as there is no such thing as absolute security, most individuals want an 'intermediate level' of privacy, rather than complete exposure to or complete isolation from others.[29] And yet the individuals who debate the subject on behalf of us – come from each extreme – the moderate, nuanced, sophisticated discussion is left behind as the battle for domination continues.

Charlie Edwards
Director, National Security and Resilience Studies
Royal United Service Institute

[25] Jennifer Chandler, Privacy versus National Security: Clarifying the terms of the debate, Date unknown.
[26] Digital Surveillance, Open Rights Group, April 2013 https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/
[27] James Brokenshire, National Security and Civil Liberties – Getting the balance right, 3 July 2013, https://www.gov.uk/government/speeches/national-security-and-civil-liberties-getting-the-balance-right
[28] Ibid
[29] Allan Westin, Privacy and Freedom, New York: Atheneum, 1967