After Snowden - the evolving landscape of privacy and technology

Robin Wilton
Technical Outreach Director - Trust and Identity
Internet Society

wilton@isoc.org

July 2017

This paper appears in the Journal of Information, Computers and Ethics in Society (JICES).
The final publication version can be accessed online, here:
http://www.emeraldinsight.com/loi/jices

I feel privileged to have been invited to contribute to this special edition of JICES, particularly as I can lay no claim to the kind of academic credentials which such a contribution would normally reflect. I come to the topic of ethics and online privacy from a background primarily in the IT industry, having spent 28 years as an IT specialist, consultant and industry analyst, and the last 4 years in the non-profit sector engaged in privacy advocacy. In that role, I find I am often translating between technologists and policy makers, trying to help them make sense of the effects technology is having on our individual and collective lives, and develop the appropriate technical and non-technical responses to those effects.

You will find this paper less studded with citations than the others in the special edition, and with a higher proportion of opinion - though my hope is that the opinions I express will (a) stand up to debate, and (b) spur some thoughts about possible avenues for proper academic research, by proper academics. I apologise in advance for a bias towards findings drawn from the UK and US: however, since Snowden's disclosures primarily concerned the activities of US intelligence agencies and their close allies in the "Five Eyes" group (Australia, Canada, New Zealand, UK and US), it is natural to look at the pre- and post-Snowden state of privacy in those countries, and particularly in the most active - the US and UK.

1 - The pre-Snowden context

As a privacy advocate, my pre-Snowden analysis was that the primary threat to individual privacy was seen as coming from commercial exploitation of data (online social fora, data mining, targeted/behavioural advertising), with data monetisation as a powerful motivating force.

Some did express concerns about government intrusions on citizen privacy, to be sure, both retrospectively (for instance, when anti-terrorism laws were found to be being used for trivial enforcement purposes entirely unrelated to terrorism), and prospectively (for instance, in warning that draft legislation was worded in ways that made privacy-eroding outcomes more likely).

Civil society organisations such as Privacy International, the Electronic Frontier Foundation, the American Civil Liberties Union, and the Open Rights Group, have, for years, been active in this regard. In the UK I am also aware of more narrowly-focused advocacy groups such as No2ID, and MedConfidential, who advocate in favour of better citizen protection in specific domains (government eID and healthcare data, respectively), and there are, doubtless, similar organisations and groups in other countries.

My assessment is that even those groups tended to focus (albeit not exclusively) on the "overt" public sector uses of data — the intelligence and law-enforcement uses being, for obvious reasons, less open to scrutiny and comment. Taking the UK as an example: even where there is a mechanism for public accountability (the Intelligence Services Commissioner's annual report) it is, for the most part, an entirely procedural report, and devoid of any hints at operational practice. Reports from 2001 to 2015 can be found on the ISC website [1]:

It is interesting to compare the 2012 report with that for 2013 (which had to address media

reports alleging unlawful conduct on the part of the intelligence services). The reports for both 2012 and 2013 both explicitly reflect the Commissioner's conclusion that the agencies were operating lawfully, and within the constraints imposed on them by the law.

For 2012, the main report fills some 20 pages, plus a further brief Annex describing the roles of the different security agencies inspected by the commissioner, and the kinds of warrant under which they exercise their powers. The report for 2013 is more than twice as long, at 49 pages, and has a further 10 pages of Annex. The body of the report is again mostly procedural, but the commissioner also addresses the topic of media reports concerning the Snowden disclosures. The Annex of the report for 2013 report describes the roles of the agencies, and the warrants under which they operate, but also has sections on the following topics:

- The European Convention on Human Rights (specifically, Article 8 - the right to respect for private and family life)
- The Application Process for Warrants
- Necessity and Proportionality

The significance of these additional sections in the Annex for 2013 is that they describe the legal obligations that safeguard citizens' privacy from undue intrusion. Governments that are signatories to the European Convention on Human Rights (ECHR) can only claim exemption from the requirements of Article 8 to the extent that privacy intrusions are lawful, in pursuit of a legitimate aim, and that they are necessary and proportionate in a democratic society. Two useful examinations of these principles have been written by Stephen Greer, for the Council of Europe [2], and Douwe Korff [3], of London Metropolitan University. So, as well as fulfilling the Commissioner's statutory function of reporting on the proper functioning of the intelligence services, the report for 2013 specifically aimed to support the contention that the intelligence services' actions to date were lawful, and were not in violation of Article 8.

However, in February 2015, the UK's Investigatory Powers Tribunal (IPT) ruled that - at the time of the 2013 report - the intelligence services' actions had been unlawful from 2007, when its systems of bulk interception (specifically, the PRISM and UPSTREAM programs) were started, until December 2014. The grounds for the ruling rested on Articles 8 (privacy) and 10 (freedom of expression) of the ECHR. The IPT ruled that the legal basis for these interceptions was not sufficiently accessible and foreseeable to those potentially affected. In other words, citizens were not adequately informed about the kinds of behaviour to which the law could give rise [4].

The challenge in the UK was successful not because the court found there was anything unlawful about the activity itself, nor even because the court found fault with the governance regime, but because the basic operating principle of the governance regime was not public. Once that information became public (which happened only as an incidental effect of the court record), full compliance with the ECHR was held to have been achieved.

Before Snowden, then, we had a starting set of assumptions, along these lines:

- The principal threat to individual privacy is from commercial companies;

- The threat from law enforcement and intelligence services is limited, targeted, and subject to some kind of appropriate - albeit opaque - governance;
- Ultimately, there are legal protections that guarantee respect for citizens' privacy rights.

Snowden's disclosures undermined those assumptions, particularly for citizens of the "Five Eyes" nations (Australia, Canada, New Zealand, USA, and UK), and, as noted in the survey findings, Spain. The threat to privacy from commercial monetisation of personal data persists, and remains one of the most powerful motivating forces in the Internet economy, but our awareness of the scale and potential intrusiveness of government surveillance activities was abruptly raised. Those activities give rise to significant concerns, not least because of the imbalance of power between the individual and the state, and in particular, the enforcement mechanisms available to the latter.

Snowden revealed that law enforcement and intelligence access to data (in motion and at rest) had been taking place on a mass scale, often indiscriminately and with no requirement for warrants. Where intelligence and national security are the motivating factor one must expect a certain opacity in the exercise of lawful powers, but as the IPT ruling makes clear, citizens are still entitled to expect that those powers are subject to effective oversight. In the absence of effective oversight, the risk is that government agencies fail to demonstrate democratic necessity, and fail to show that there is adequate protection against abuse of the powers.

2 - Inferences and reactions

If one thinks of Snowden's actions as a catalyst provoking a chemical reaction, there is much to be inferred from looking at the reaction itself, not just the actions that set it off. I want to consider four topics in particular:

- The legislative reaction to findings of illegal surveillance
- Changes in the public understanding of surveillance and its effects
- Cross-border implications
- The roles of the public and private sectors

The legislative reaction

In cases where Snowden's disclosures led to a ruling that intelligence and security services had been acting illegally, the government response was often to change the law to legalise the behaviour, rather than to change the behaviour [5]. The research report from New Zealand provides an example of a similar approach in New Zealand, where intelligence and law enforcement agencies were found to have acted unlawfully in the "Kim Dotcom" case and the 2007 terrorism case.

Changes in public understanding

We have also had to become more nuanced in the way we think of the collection of surveillance data. One justification offered for indiscriminate data collection is that "collecting the data is not, *per se*, surveillance. It's not surveillance until someone looks at it". This line of argument has led

to a more public dialogue about the so-called "chilling effect" of pervasive monitoring; that is, the constraining effect on civil liberties, if citizens are aware that their every action *could* be arbitrarily surveilled. This hypothesis should not come as news to us: it is, after all, exactly the principle on which Bentham based the panoptical prison: the inmates' behaviour is most effectively constrained if they know that they *might* be under surveillance at any time, but can never tell whether they *are* being surveilled at a given moment. Interestingly, Bentham saw the Panopticon as what we would now think of as a public-private partnership: it would be operated by a commercial contractor, who would be motivated by financial penalties for deaths in custody, escapes, recidivism and so on [6]. This mixing of commercial and public sector roles is a topic to which I shall return below, under **Public and private sector roles**.

Cross-border implications

A strong theme across the research findings is that of cultural context. Respondents' expectations regarding the relationship between the individual and the state are strongly influenced by historical experience in their country or jurisdiction. For example, as the research report on Spain describes, that country's experience of totalitarian government under Franco had a profound effect on citizens' expectations of how a government would behave once a liberal democracy had been established. The report on the PRC and Taiwan paints a more complex picture, in which public attitudes are influenced not just by domestic politics, but also by the interplay of political relations between Taiwan, the PRC and the United States.

In other words, the cultural context that forms people's attitude to government surveillance is not a single-country matter. Nor, of course, are the legislative factors: the US-EU Privacy Shield legislation was struck down because the US governance regime applied to personal data could not afford it equivalent levels of protection to those (supposedly) in force in the EU. The surveillance data from many of the programs Snowden revealed was destined for consumption by agencies of the Five Eyes nations, begging the question of whether or not the governance regimes in those countries are equivalent, compatible, or robust in their protection of citizens' rights.

Public and private sector roles

The Snowden disclosures threw a probably unwelcome light on the extent to which commercial product and service providers were complicit in the pervasive monitoring of citizens' data. Data might be intercepted on communications links, retrieved wholesale from intermediary mail/messaging servers, and even decrypted thanks to the inclusion of weaker default settings in commercial encryption products. Anecdotally, in the wake of these specific revelations, there was a flight from US IT product and service providers, costing them billions of dollars in lost business.[7] We can probably attribute some changes in the mainstream market to that effect.

First, there are now more commercial offerings of end-to-end encrypted messaging and secure email, though it is less clear whether consumers truly understand the trust models underlying such products and services. For instance:

• Who assesses the robustness/reliability of the security mechanisms on which such offerings are

based - particularly for proprietary, closed-source implementations?
- What would be the vendor's response if served with a warrant for access to a consumer's device or data?
- In terms of lawful interception, what is the status of a secure communication once decrypted by the recipient?
- For webmail services transmitted over HTTPS, how is traffic protected once it emerges from the encrypted transport-layer session?

Second, it is also possible that more consumers are developing a more nuanced understanding of the relative merits of, say, browsing over HTTPS, using a VPN, and/or using an obfuscation tool such as Tor. However, I think it is open to question whether consumer demand for such options is so widespread or so loud as to reshape the IT product landscape in its own right, and whether that consumer demand is driven by concern over government interception or the commercially-instigated threats to privacy.

In addition to any commercially-driven changes, the Internet Engineering Task Force (IETF), a technical standards body for the Internet, responded to Snowden's revelations by declaring that "pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible".[8]

A further aspect to the public-private sector relationship, which emerged in 2015, deserves its own detailed examination.

The relationship between law enforcement and technology vendors was tested, and is likely to undergo further transformation, in the wake of the San Bernardino shootings of December 2015. In the course of investigating this attack, law enforcement authorities were initially frustrated in their attempts to access data on an iPhone used by one of the attackers. They turned to Apple, the vendor, which responded by saying that it did not have the means to override the security code set on the device by its user. This provoked a debate (still unresolved) about the legitimate obligations of vendors of products with security mechanisms that are ultimately controlled by the consumer.

The law enforcement argument, as expressed, for example, by David Bitkower of the US Department of Justice [9], takes two lines of attack.

The first is along these lines: "it is not acceptable for an individual to be able to put data beyond the reach of a duly-authorised warrant. Where technology allows a user to secure data, it must remain possible for a warrant to be executed and for the secured data to be accessed by law enforcement, independent of any consent, co-operation or awareness on the part of the user. The technology provider is therefore under an obligation to ensure that law enforcement access is possible, regardless of any settings/keys the user has applied".

The research that forms the basis for this special edition should, I believe, lead us to identify a number of problems if this position is put into practice. Technology, data, and online services are

poor respecters of geographic or jurisdictional boundaries. The Internet is, axiomatically, a frontierless environment. We therefore have to consider the instances in which secure technologies end up being used in jurisdictions other than those in which their vendor is located.

Suppose, therefore, that a law enforcement official from the autocratic regime of Oppressia serves a warrant at Apple's local registered office, demanding that (as provided for under Oppressian law) Apple grant access to the data held on the phones of a number of journalists who have been critical of the regime. The warrant might be repugnant to the US authorities who called for warrant-proof data to be eliminated, but that is not the concern of the Oppressian authorities: as far as they are concerned, the conditions for invoking the technical capability have been duly met. There is no practical way to avoid this kind of outcome, if technical back doors are made mandatory.

There is a further issue to be addressed, which can be illustrated by two examples. First, it would seem odd to claim that the builder of a house, having designed it to be secure against burglary, has a responsibility to facilitate law enforcement access to the house in the event that the householder has locked the doors and windows. Second, it is quite possible for an individual to put data beyond the reach of a duly-served warrant with no recourse to technology at all. For instance, I have noted some password reminders on paper, which would be indecipherable to a third party. We are therefore expecting more of technology and technology vendors than would be reasonable in non-digital domains of life. Intuitively, that more extreme set of requirements ought to be justified on the basis of something more than convenience to the law enforcement and security authorities.

One might conclude that it is unsafe, particularly in the cross-border context, to proceed on the assumption that a government, or a law enforcement agency with a duly-served warrant, cannot be a "bad actor", at least in terms of the culture and intent of the legislating jurisdiction.

The question of legal constraints on individuals' ability to preserve their own privacy and security continues to evolve rapidly. For example, as of early February 2017, it appears that US President Donald Trump is considering an executive order requiring visitors to the US to disclose the user IDs *and passwords* for social media accounts they hold [10]. This raises serious questions about whether it can be appropriate for law enforcement agencies of one country to be able to authenticate as (i.e. impersonate) individual citizens of another, particularly in the absence of any suspicion of wrong-doing on the part of the individual.

The US Department of Justice's second line of argument, as expressed by David Bitkower at the 2016 Privacy and Security Forum in Washington DC, runs roughly as follows: "it is inappropriate for a technology vendor to be making unilateral (policy) decisions about whether or not law enforcement agencies are able to access encrypted data". One resulting implication is that it is for a national government to make those decisions, and for that nation's technologists to embody the required level of accessibility in their products. As we saw from the Oppressia analogy above, once the technology makes back-door access possible, that access is also open to uses which do not serve the purpose envisaged by the originating nation. In any other technical domain, where different nations express different requirements, the usual solution would be to try and agree a mutually acceptable international standard. However, the idea that a critical mass

of nations could agree an international standard for law enforcement circumvention of encryption seems optimistic, to put it mildly.

This tension between legitimate law enforcement objectives and the technical privacy protections available to citizens will be hard to resolve at the national level, let alone internationally.

Conclusions

Post Snowden, the general perception of threats to online privacy has shifted from a predominant focus on commercial threats to a recognition that government activities, in the sphere of intelligence and national security, also give rise to significant privacy risk.

Snowden's disclosures have challenged many of our assumptions about effective oversight of interception capabilities.

Our expectations concerning both privacy and the legitimacy of law enforcement actions are contingent, and depend at least partly on cultural norms; expectations about the role of the state also depend on national experience. But it is unwise to assume that the relationship between the individual and the state is a static thing. It is mutable, and can change surprisingly fast in reponse to shifts in the political climate, as the historical analyses of the surveyed countries illustrate, and as we continue to see in emerging national responses to security threats and technical innovation.

The tension between legitimate law enforcement access and personal privacy remains challenging to resolve, and the pace of technical innovation is likely to mean that legislative measures struggle to keep pace as an effective solution.

[1] Annual reports of the Intelligence Services Commissioner: http://intelligencecommissioner.com/content.asp?id=19
[2] Greer S, The Exceptions to Articles 8 and 11 of the ECHR: http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf
[3] Korff D, The Standard Approach to case assessment under Articles 8-11 and Article 2 ECHR: http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf
[4] UK-US surveillance regime was “unlawful for seven years” - Guardian, 6th Feb 2015 https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa
[5] Bowcott G, cited in the Spanish research report for this issue.
[6] "The more strictly we are watched, the better we behave” - (The Bentham Project, University College London): http://www.ucl.ac.uk/Bentham-Project/documents/leaflets/benthampanopticon.pdf
[7] Newsweek article on a report by the Information Technology and Innovation Foundation, June 2015: http://europe.newsweek.com/nsa-surveillance-may-cost-us-tech-companies-more-35-billion-328482

[8] RFC7258, Internet Engineering Task Force, May 2014: https://tools.ietf.org/html/rfc7258
[9] David Bitkower, US Department of Justice, April 2016: https://phys.org/news/2016-04-encryption-row-spotlights-privacy.html
[10] John Kelly, US Secretary of State for Homeland Security, February 2017: http://www.nbcnews.com/news/us-news/amp/us-visitors-may-have-hand-over-social-media-passwords-kelly-n718216