www.jusletter-it.eu

Malcolm Crompton / Chong Shao

Reconciling Privacy and Security in the Age of Snowden: applying the 4A's Framework to an age-old challenge

Der Europäische Gerichtshof verfügte 2014, dass die EU-Richtlinie zur Vorratsspeicherung von Daten ungültig ist. Dies folgte den Enthüllungen von Edward Snowden im Jahr 2013 über die stark umstrittene und umfassende Überwachung all jener, deren digitaler Fingerabdruck in irgendeinem Kontakt mit den USA steht. Beide legen signifikante und vermeidbare Fehler in der Weiterentwicklung und Durchführung der Politik dar. Dennoch existiert ein Rahmen («Framework») zur Verwaltung und Vermeidung solcher Risiken, wenn Zwangs- und verdeckte Massnahmen für Rechtsdurchsetzung oder Nationale Sicherheitsbelange in Frage stehen. Es handelt sich um den «4As Framework», welcher vor Jahren vom Datenschutzbeauftragten Australiens entwickelt wurde. Der Artikel beschreibt diesen Rahmen. (ah)

Kategorie: Beiträge
Rechtsgebiete: Datenschutz; Datensicherheit
Region: Australien

Zitiervorschlag: Malcolm Crompton / Chong Shao, Reconciling Privacy and Security in the Age of Snowden: applying the 4A's Framework to an age-old challenge, in: Jusletter IT 15. Mai 2014

Inhaltsübersicht

[Rz 1] Undoubtedly one of the most important rulings on privacy by the European Court of Justice so far in 2014 was its decision[1] that the EU Data Retention Directive[2] was invalid.

[Rz 2] Equally, one of the biggest stories of 2013 was Edward Snowden's revelation of operational details of surveillance programs conducted by the United States of America and its international partners. The revelations have had a global and historical impact, even as the disclosures continue.

[Rz 3] The vocal responses from both sides of the privacy-security spectrum have been predictable and have generated more heat than light. We have been hearing the same arguments for the whole of the last century, but especially over the last decade they have become very tired – increased surveillance must be either an unbridled good or the harbinger of a totalitarian state.

[Rz 4] Those who argue against the enhancement of surveillance do so in the face of evidence to the contrary: *terrorism is a persistent threat*[3], *organised crime is more potent than ever*[4]. At the same time nation states have become *increasingly active players*[5] in cyberspace. Intelligence agencies could not have kept us safe, and will not be able to keep us safe, if their powers and capabilities are prevented from evolving in line with the threats that we face. A sensible debate must recognise this reality.

[Rz 5] At the same time, the proponents of expansive measures to address our security threats have been conspicuously quiet about how to make them safe and acceptable to the public. The common refrain, for example, that mass surveillance is OK because «it's just metadata» is ludicrous given *how sensitive and useful it can be*.[6] Assertions that NSA surveillance has been duly conducted in accordance with the law ring hollow in light of *emerging evidence of misconduct*[7] as well as *issues with the supervising authorities*.[8]

[Rz 6] The Snowden affair and the reasoning in the Court of Justice are the most visible examples of a more general challenge: how do we make sure that the people and institutions that have been granted coercive powers can exercise them safely and appropriately in a modern society? The challenge sharpens considerably when they are also covert. Even the most ardent critics of Snowden now agree on the importance of effective oversight and of clarifying the uncertainty surrounding the collection of metadata.

---

1 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf(all Internet sources last visited on 23 April 2014).

2 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

3 http://edition.cnn.com/2013/04/15/us/boston-marathon-explosions.

4 http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509.

5 http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all.

6 http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/.

7 http://www.theguardian.com/commentisfree/2013/dec/31/nsa-powers-have-been-abused.

8 https://mises.org/daily/6672/FISA-the-NSA-and-Americas-Secret-Court-System.

[Rz 7] Fortunately, we have a well-established approach developed by the Office of the Australian Information Commissioner that has resolved such difficult issues in the past: the *4A's framework*.[9] Here's how we can do it again today.

1 Analysis

[Rz 8] The first thing we need to get right is *analysis*. This involves a series of steps:

- Define the problem – taking care to be calm, objective and framing it in the right way
- Be clear about the values that you would like to preserve and uphold – for example, respect for individuals, due process, etc.
- Choose the most suitable option with the least privacy impact on balance – for example, only confirming 18+ age (rather than collecting everything on the ID card), introducing a sunset clause to enabling legislation, establishing a reasonable cause requirement, etc.
- Ensure that you are conducting the analysis while keeping in mind the other A's as well.

2 Authority

[Rz 9] Next, we need the right *authority* for law enforcement and national security agencies to do their job properly. As with everything, there needs to be a careful balance. Where privacy is likely to be affected, the power should be granted expressly by legislation setting out in objective terms what kinds of information can be collected, for how long, in what circumstances and for what purposes. Independent judicial oversight is crucial for especially sensitive cases.

[Rz 10] As the Snowden affair demonstrates, a breakdown of the authority-granting process will undermine trust and credibility in the system as a whole.

3 Accountability

[Rz 11] The third thing we need to get right is *accountability*: making sure that power is, and is seen to be, exercised in the right way. For law enforcement and national security agencies, their power is frequently exercised in a corrosive environment, in difficult situations against vile people seeking to subvert or corrupt them. Misuse and abuse of power *can and does happen*[10] – no-one is infallible. Is it any surprise, then, that «trust us, we'll do the right thing» is met with cynicism and derision by the public?

[Rz 12] Again, we don't need to invent solutions from scratch. Many jurisdictions have laws and institutions that provide for accountability mechanisms such as access to information, prohibition on classifying or withholding information about violations of law, whistleblower protection, and monitoring and review of power-wielding agencies.

---

9 http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/law-enforcement/privacy-fact-sheet-3-4a-framework-a-tool-for-assessing-and-implementing-new-law-enforcement-and-national-security-powers.

10 http://www.heraldsun.com.au/news/law-order/hundreds-of-police-members-caught-abusing-confidential-information-on-operational-intelligence-database/story-fnat79vb-1226637132957.

[Rz 13] The real challenge is to ensure that in practice, our accountability bodies are able to function effectively now and in the future. This means firstly that they have the necessary scope to operate, enshrined in legislation. No agency or activity should escape scrutiny, and there should be strong powers of evidence-gathering. Secondly, they must be allowed to operate without undue political or outside influence. Thirdly, we must provide them with sufficient resources in order for them to do their job effectively. Having the entire legal mandate in the world is useless without the money and personnel to carry it out.

4 Appraisal

[Rz 14] Finally, as we see in the current debate, nothing stands still. Technology changes, the threat landscape changes, corruption rears its ugly head and more. Hence the last of the 4A's: *appraisal*. We need to monitor the new measures and evaluate whether they are working as expected. We need to ask whether the circumstances have changed, which circles back to an analysis of what needs to be done about it.

5 Conclusion

[Rz 15] Give me privacy, or give me security? Let's move beyond this false dichotomy and have a conversation based on facts, sound judgment, and an appreciation of our past successes.

Malcolm Crompton, BSc (Hons), BEc, FAICD, CIPP is Managing Director of Information Integrity Solutions Pty Ltd, a global privacy strategy provider based in Australia. He served as Privacy Commissioner of Australia from 1999 to 2004. Malcolm's global reputation and expertise in privacy was recognised when he was honoured in Washington DC with the IAPP 2012 Privacy Leadership Award.
Chong Shao, BA, LLB (Hons) is a Consultant at Information Integrity Solutions Pty Ltd.
The authors may be contacted at mcrompton@iispartners.com and cshao@iispartners.com.
An earlier version of the article was published in World Data Protection Report (WDPR), Vol 14 Issue 4 of April 2014.