Access to telecommunications data in civil proceedings

Pirate Party Australia

By Simon Frew

Pirate Party Australia would like to take the opportunity to thank the Attorney-General's Department and the Department of Communications and the Arts for the chance to provide feedback on the access to telecommunications data in civil proceedings review. We are wholly opposed to expanding data retention to civil proceedings, and believe the current legislation already unduly affects the privacy of Australian citizens.

Privacy is a fundamental human right that has come under sustained attack in the last decade. Internet giants like Facebook and Google create detailed profiles of their customers so they can better target advertising, and other sites gather information on their users to sell. We carry tracking devices in our pockets and share our lives on social media. At the same time security and law enforcement agencies have campaigned for, and in many cases have been granted the ability and legal authority to monitor ordinary citizens with little to no legal oversight.

There have been countless articles declaring privacy dead[1], and perhaps from such a perspective, allowing data retained under the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 to be used in civil cases would be acceptable. However, such arguments overlook the reality of how we choose to reveal ourselves to the outside world and how we view privacy in the context of our own lives.

Privacy is a perceived state where we are free from unwanted observation or interference. It is the ability to control what we reveal of ourselves to the outside world. It exists as a risk calculus whenever we choose to reveal something about ourselves. We balance our ability to control our information against the perceived benefits and risks of exposure[2].

When opting to share information on the Internet, whether it be on social media or in exchange for services, we are doing this voluntarily. We choose what we are sharing, with whom, and have at least some understanding of the risks posed by data mining. The individual is still exercising control over how their life is revealed to the outside world.

Privacy is important for democracy itself. People need to be able to freely associate, debate, question and organise in support of their beliefs. Undue surveillance causes a 'chilling effect' on political speech as people self-censor to avoid scrutiny. Whilst privacy has a political aspect it should not be seen as separate from personal privacy. "Equal rights of personal choice, association and expression not only protect the political freedom and equality of individuals, but their personal freedom and equality too."[3]

---

[1] https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

[2] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart **Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts** in European Journal of Information Systems (2013) 22, 295–316 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.4790&rep=rep1&type=pdf

[3] Lever, Annabelle **Privacy Rights and Democracy: A Contradiction in Terms?** Contemporary Political Theory May 2006, Volume 5, Issue 2, pp 142–162

Mandatory data retention changes the privacy landscape. It makes using a computer or carrying around a mobile phone a public act. It shrinks the private space of citizens significantly.

To underline the importance of privacy to individuals, we do not have to look further than the current federal government. Illustrative examples are the appeals that both Attorney-General George Brandis[4] and Prime Minister Malcolm Turnbull[5] are fighting to avoid the release of their Ministerial diaries. There is a deep irony that the Minister who put forward the original data retention legislation and is further putting forward its proposed expansion to civil cases is fighting so hard to keep his own Ministerial business secret. Surely, if they can fight multiple appeals to defend their own privacy, they can understand the opposition to data retention and its expansion to civil cases?

The data retained under the Telecommunications (Interception and Access) legislation reveals detailed, private and personal information about everyone. Every time someone connects to the Internet, every time their phone pings a tower, every time they make a call they are creating personal data that can be used to reveal detailed personal information about their lives. It clearly states that data collected under the Act is considered to be personal information and is subject to the Australian Privacy Principles. From the legislation:

> (2) Information that is kept under this Part, or information that is in a document kept under this Part is taken, for the purposes of the *Privacy Act 1988* , to be personal information about an individual if the information relates to:
>
> (a) the individual; or
>
> (b) a communication to which the individual is a party.[6]

In order for data collected under the data retention regime to be made available to lawyers in civil cases, it is clear that an exception will be required thus reducing protections for citizens under the Privacy Act.

---

4 http://www.smh.com.au/federal-politics/political-news/george-brandis-loses-second-court-bid-to-keep-diaries-secret-from-labors-mark-dreyfus-20160906-gr9n72.html

5 http://www.theaustralian.com.au/news/nation/turnbull-appeals-ruling-opening-his-diary-to-public-view/news-story/63e9734a71ef9a30f70db96b096e2c29

6 http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s187la.html

One clear example of how data collected is private information is mobile phone location tracking data. It creates a detailed picture of your every movement day after day. This was demonstrated by a German Greens MP in 2009. When he requested six months of his phone data from Deutsche Telekom, he was able to generate a map of his every movement to demonstrate the privacy risks from data retention.[7] The information gave regular updates on his location for months on end, amounting to constant locational surveillance.

The risks posed by such data becoming available to lawyers are significant. Each time data is shared with an outside entity, it creates another location where the data must be protected from accidental or deliberate distribution. It is arguable that despite some significant leaks, including Victorian Police documents being uncovered in a Bikie club-house in 2013[8], law enforcement agencies have a higher standard of data protection than law firms. Law firms have been victims of hacking incidents in increasing numbers in recent years with the Law Council of Australia issuing a warning that more needs to be done to protect sensitive data held by lawyers in December last year[9].

The argument that warrantless mass surveillance is necessary for law enforcement agencies to catch criminals and terrorists is based on thin evidence[10][11] at best. There is at least some theoretical upside to come from the wholesale loss of privacy through data retention. With the proposal to expand access to the data collected for civil cases, there is no upside for ordinary citizens at all.

---

[7] http://www.zeit.de/datenschutz/malte-spitz-data-retention
[8] http://www.abc.net.au/news/2013-05-06/police-taskforce-on-substantial-information-leak/4671862
[9] http://www.abc.net.au/news/2016-12-14/law-firms-prime-target-for-cyber-attacks/8117598
[10] https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/
[11] http://theconversation.com/the-security-benefits-of-warrantless-surveillance-are-as-clear-as-mud-49278