Submission to the Justice Committee on the Privacy Bill 2018 (34-1)

Catalyst IT

May 2018

catalyst
open source technologists

Level 6, Catalyst House, 150 Willis Street, Wellington 6011
PO Box 11053, Manners Street, Wellington 6142, New Zealand
+64 4 499 2267 // enquiries@catalyst.net.nz // www.catalyst.net.nz

1 Introduction

1.1 Catalyst IT was founded in 1997 in Wellington, with a vision to deliver effective and efficient technology solutions using open source software. We are now the largest New Zealand-owned company specialising in free and open source technologies and services.

1.2 Based in Wellington with approximately 270 staff spread across our offices in Wellington, Auckland, Christchurch, Australia and the United Kingdom, we have established an impressive track record for successfully delivering, hosting and maintaining many large-scale systems for a wide range of clients, including clients at all levels of the New Zealand government.

1.3 We believe that the need to ensure the security and privacy of personal information and other data is critical. This is especially so in the context of information technology where a vast amount of personal information of all kinds is being collected, stored, processed, used, sold and shared, all in real time. New Zealand's privacy laws should be robust enough to ensure that New Zealanders' personal information is treated consistently with their rights and freedoms as data subjects, as well as their increasingly high expectations around privacy. It is crucial that the law contains incentives that are adequate to ensure that personal information is treated with the appropriate level of care.

1.4 We support the Bill. However, we believe that the changes in the Bill do not go far enough. We support the additional changes proposed by the Privacy Commissioner in his 2016 report.[1] We also propose a number of other changes designed to align the Bill more closely with the General Data Protection Regulation (GDPR), about to come into force in the European Union.

1.5 We believe that the Bill represents a good opportunity for New Zealand to position itself as a privacy-affirming jurisdiction. By enacting privacy regulation that is comprehensive, emphasises the rights of data subjects and is easily enforceable, New Zealand can present itself as a jurisdiction where privacy and data protection matter. The ability to trade on an internationally-recognised high standard of legislative protection would represent a significant competitive advantage to New Zealand companies, especially in the information technology sector.

1 Privacy Commissioner *Report to the Minister of Justice under Section 26 of the Privacy Act: Six Recommendations for Privacy Act Reform* (2016), https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf.

2 The Bill and the Privacy Commissioner's Recommendations

2.1 We agree with the Privacy Commissioner and others in their assessment of the Bill that it will move New Zealand towards the standards of privacy and data protection that apply in other key OECD countries, by:[2]

(a) empowering the Commissioner's office to issue compliance notices;

(b) empowering the Commissioner's office to issue a determination where a person has requested access to personal information and has been refused;

(c) introducing new offences;

(d) introducing mandatory reporting of harmful privacy breaches; and

(e) strengthening protections in relation to cross-border data transfers.

2.2 We also agree with the recommendations made by the Commissioner in his 2016 report that the Privacy Bill should introduce, in particular:

(a) data portability as a consumer right;

(b) controls on the risk that individuals could be re-identified from anonymised data;

(c) increased civil penalties for non-compliance with the Act; and

(d) a power of the commissioner to require agencies to demonstrate compliance with the Act.

2.3 Being specialists in open source software, we have always be advocates for the rights of technology users to sovereignty over their own data and to freedom from the "lock-in" business models inherent in many proprietary technologies. Users should be free to move their data from one system to another without being beholden any given provider. Data portability has been explicitly recognised as a right in privacy-focussed jurisdictions, including the European Union.[3] The right not to be identified from anonymised data has been similarly recognised, and such re-identification is set to become a criminal office in the United Kingdom.[4]

2.4 It is critical that the rights and duties contained in the Privacy Act are regarded as serious and legally binding. In order to achieve this, there must be real and significant incentives for compliance with the Act. The idea that privacy regulation must have teeth is clearly recognised in (among other places):

2 John Edwards *Welcoming the Privacy Bill* (2018), https://www.privacy.org.nz/blog/welcoming-the-privacy-bill/.

3 GDPR article 20.

4 See: Rebecca Hill and John Leyden *Re-Identifying Folks from Anonymised Data Will Be A Crime in the UK* (2017), https://www.theregister.co.uk/2017/08/07/data_protection_bill_draft/.

(a) Australia, where organisations found to be in breach of the Privacy Act 1988 can be fined over $2,000,000 as of May 2018;[5]

(b) the United Kingdom and the rest of the European Union, where (once the GDPR comes into force in May 2018) organisations can be fined up to €20,000,000, or 4% of their annual global turnover, whichever is the higher;[6]

(c) Canada, where organisations found to be in breach of the Personal Information Protection and Electronic Documents Act can be fined up to $100,000;[7] and

(d) the United States, where organisations found to be in breach of the various federal and state privacy laws have been subject to significant financial penalties, including a $4,300,000 penalty for violating the Privacy Rule of the Health Insurance Portability and Accountability Act.[8] In addition, there is currently a bill before the United States Senate under which fines of up to $5,000,000 could be imposed for failures to maintain adequate information security or to make the required notifications in the event of a privacy breach.[9]

2.5 Our view is that the current penalties under the Privacy Act 1993 and proposed Bill for certain kinds of non-compliance (up to a maximum of $10,000) do not create the necessary incentives for organisations to conduct the lengthy and expensive undertaking of implementing and maintaining adequate privacy and data security processes and safeguards. We support the Privacy Commissioner's call for fines of up to $100,000 for an individual and $1,000,000 for an organisation to be imposable in cases where personal information has been mishandled.

2.6 These figures are still conservative when compared with Australia, the United Kingdom (along with the rest of Europe) and the United States. We are conscious, however, that the smaller size of the New Zealand economy warrants a more conservative approach to maximum penalties. We believe that the Commissioner's proposed figures represent an appropriate balance between the need to incentivise compliance with good privacy procedures and the need to avoid over burdening New Zealand companies (and in particular small businesses) with potential liability.

5 Privacy Act 1988 (Cth) s 13G, and Crimes Act 1914 s 4AA for the value of a "penalty unit".

6 GDPR article 83.

7 Personal Information Protection and Electronic Documents Act ss 46 and 28.

8 Office for Civil Rights *Civil Money Penalty: Cignet Health Fined a $4.3M Civil Money Penality for HIPAA Privacy Rule Violations* (2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/index.html.

9 S.2179 – Data Security and Breach Notification Act (115th Congress (2017-2018)). See also: Rahul Mukhi and Britta Redwood *2018 Brings Continued Calls for a Federal Data Protection and Breach Statute* (2018), https://www.clearycyberwatch.com/2018/01/2018-brings-continued-calls-federal-data-protection-breach-statute/.

3 We Propose Additional Changes

3.1 As the Committee will be aware, the European Union's GDPR comes into force in May 2018 and applies to any organisation which processes the data of residents of the Union, regardless of the location of the processing organisation. In our preparation for compliance we have come to believe that the GDPR embodies global best practice when it comes to the protection of personal information. In a world where national borders are increasingly fluid – especially so in the information technology context – the idea of consistency in data protection regulation is attractive. We therefore support the idea of aligning New Zealand's privacy laws with the GDPR to the maximum extent possible. The Bill presents a good opportunity do this.

3.2 Fortunately, there is already significant overlap. Moreover, New Zealand was recognised by the European Commission as a jurisdiction with "adequate" data protection standards in 2012.[10] This represents a significant competitive advantage for New Zealand companies over companies based in non-adequate jurisdictions (like Australia) that are operating in the European Union. We propose that two key elements of the GDPR be incorporated into the Bill:

(a) a requirement for agencies to adopt the principle of privacy by design; and

(b) the recognition of the right of data subjects to be forgotten.

3.3 Privacy by design refers to the adoption of technical and organisational methods designed to integrate data protection safeguards into the collection and processing of personal information, at the outset of any such endeavour.[11] The principle aims to ensure that privacy is regarded as a primary consideration in the planning and implementation of any activity that engages privacy obligations. A privacy by design requirement means that privacy issues cannot be relegated to consideration as an after-thought or ignored altogether. The benefits of requiring agencies to act in accordance with the principle would include include:[12]

(a) increased awareness of, and focus on, privacy and data protection across organisations and industries;

(b) increased likelihood of agencies meeting their privacy obligations;

(c) reduced likelihood of agencies' activities being privacy intrusive and having a negative impact on individuals; and

10 European Commission *EU Approves New Zealand's Data Protection Standards in Step to Boost Trade* (2012), http://europa.eu/rapid/press-release_IP-12-1403_en.htm.

11 See: GDPR article 25.

12 See: Information Commissioner's Office *Privacy By Design* (accessed 2018), https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/. For more information see also: Information and Privacy Commissioner of Ontario *Privacy by Design* (2013), https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

(d) the fact that privacy problems are more likely to be identified in the early stages of an activity (which means that addressing them will often be simpler and less costly).

3.4 The right to be forgotten, and the related right to withdraw consent for the processing of personal information entitles individuals to the erasure of their data held by a given organisation upon request (subject to legal grounds or requirements for retention).[13] The right to be forgotten is firmly grounded in the idea that data subjects should, as far as is reasonably possible, retain sovereignty over their personal information. As vast amounts of information are amassed in databases and on the Internet, it is increasingly important that individuals have some control over what kind of information about them is available. This is especially so in relation to sensitive information (like demographic information and medical records). Key examples of why the right to be forgotten is critical can be found in the contexts of historical convictions, insolvency and other undesirable historical events: there are situations where this kind of information is obtainable on the Internet long after the relevant clean slate or insolvency period has expired.[14] This can have serious implications on individuals' ability to secure employment, housing and credit.

4 Conclusion

4.1 The Privacy Bill represents an important opportunity for Parliament to reform New Zealand's now-outdated privacy regime. It has come at a particularly opportune time in that privacy and data security and topical issues that are presently in the forefront of many New Zealand organisations' collective consciousnesses as they prepare for compliance with the GDPR.

4.2 We urge the Justice Committee to seize this opportunity and embrace the changes recommended above in order to demonstrate that New Zealand is a jurisdiction which takes privacy seriously. We believe that New Zealand should be a leader in championing the rights of data subjects. Enacting a comprehensive privacy and data security regime would go a long way towards establishing a reputation for New Zealand as a key privacy-friendly jurisdiction, which would incentivise organisations across the world to store their data here and would create a significant competitive advantage for New Zealand companies, especially in the information technology sector.

4.3 The Bill, as currently worded, is a good start. However, without some significant changes along the lines of those proposed in this submission, it would amount to a relatively insignificant reform falling well short of the standards of privacy protection that exist in jurisdictions comparable to ours. We strongly support the idea that the Privacy Bill should bring New Zealand closer to the

13 See: GDPR article 17.

14 See: Joseph Steinberg *Right to Be Forgotten* (2018), https://www.inc.com/joseph-steinberg/why-americans-need-deserve-right-to-be-forgotten.html.

position adopted in the GDPR, which we believe represents global best practice and will influence the privacy laws of countries across the world.