PRIVACY – GETTING IT RIGHT

Privacy protection in the Internet age has become convoluted and contentious. As we read of Facebook's Cambridge Analytica scandal, and the European Union introduces its tough new General Data Protection Regulation (GDPR), New Zealand is working on its own privacy law reform. What does it mean for the public sector? KATHY OMBLER found out.

In March, after years of delay, a new Privacy Bill was introduced to Parliament. Privacy Commissioner John Edwards welcomes the progress, along with this government's pledge to prioritise privacy law reform. "The current Privacy Act is 25 years old. Given the growth of the digital economy and increased demands on personal information across the whole economy, in particular across government, there is a need to refresh our legislation."

John Edwards

But it needs more work, he says. "The Bill as it currently stands is based on the recommendations of a Law Commission review in 2011 and subsequent recommendations by the previous Minister (of Justice) in 2014.

"There have been a lot of changes in the environment meantime and I think we need to take this opportunity to get it a little more future-proofed."

New Zealand has also fallen behind other jurisdictions, he says. "Better privacy and data protection regulation is a growing trend in OECD countries. In Europe, the EU General Data Protection Regulation (GDPR), which took effect in May, sets a new international benchmark for regulation."

A key reform in our Bill, as it currently stands, is the introduction of mandatory reporting of harmful privacy breaches, an original Law Commission recommendation. Under current law, the Office of the Privacy Commissioner receives only voluntary breach notifications, or notifications in response to a complaint.

Edwards says mandatory data breach reporting is needed to bring New Zealand into line with international best practice, and is a necessary addition for consumer protection. "When an organisation to which we have entrusted our personal information is unable to keep it safe, and they lose control of it, we need to be able to protect ourselves."

Susan Bennett is director of Australia-based Sibenco Legal & Advisory. At the 2018 Privacy Forum, in Wellington in May, Bennett presented an international perspective on data breach legislation and its variances in different jurisdictions, along with a summary of recent data breaches around the world. Examples include an American credit bureau which breached the privacy of 144 million customer records (which cost $30 million of forensic and legal costs) because it failed to patch a known application, and a British communications company which failed to implement basic security measures leading to the theft - by teenage hackers - of personal data of 157,000 customers.

Bennett told the forum that Australia introduced mandatory data breach reporting in February and within one month, 63 data breaches had been reported (this compared with 114 for the whole of 2017).

"Of the 63 breaches, 51 percent were due to human error and 44 percent were malicious cyber-attack. Passwords and patches were not updated, or there were known problems with technical systems. The lessons learned are that most data breaches are preventable," said Bennett.

Spark NZ's Head of Digital Trust, Sarah Auva'a, told the forum how mandatory data breach reporting is a positive move.

"It helps us keep pace with global privacy standards. It's also the right thing to do. It provides opportunity to engage with customers about online safety practices and, overall, it provides transparency and trust."

Everybody's data breach is unique, she added. "What agencies need to do can differ enormously, so the shift to mandatory reporting can help us. Agencies should have an agreed plan, strategy and principles for managing data breaches before they happen. Every breach needs to be assessed on its facts and raises unique issues."

Mandatory data breach notification would unearth issues without otherwise waiting for a complaint, and give individuals the ability to protect themselves from harm, echoed Daimhin Warner, of Simply Privacy consultancy.

"One of the critical things is for agencies to train staff to recognise a privacy breach. When to notify is really difficult," he said. "You want to be there before the media – a data breach is like a shark attack to the media. You also need to take the time to have enough knowledge of the breach to properly inform the people who you are

Protecting privacy – what to do?

With the Privacy Bill yet a work in progress, what can the public sector be doing now, to ensure it is following best practice in privacy matters? Here are six practical suggestions:

- Have your staff engage in an online privacy course. The Office of the Privacy Commissioner offers free, e-learning training modules. www.privacy.org.nz/further-resources/online-privacy-training-free
- Be familiar with the Privacy Act information privacy principles. These 12 principles are the essence of the Privacy Act. www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles
- Incorporate Privacy by Design principles when creating or changing information management systems. Privacy by Design calls for privacy to be taken into account throughout the whole engineering process. en.wikipedia.org/wiki/Privacy_by_design
- Undertake Privacy Impact Assessments (PIAs) which can help agencies identify and assess the privacy risks arising from their collection, use and handling of personal information, and when making changes to any existing process. www.privacy.org.nz/further-resources/knowledge-base/view/197?t=95132_125339
- Prevent data breaches. Keep passwords and patches up to date, maintain technical systems, and keep open and clear communication, both internal and external.
- Have a Data Breach Response Plan. Ensure that your organisation has a plan should a data breach occur. Train staff responsible for handling personal information to recognise a privacy breach. Create a culture where people feel comfortable reporting problems.

notifying. It's about balance."

Assessing 'harm' and therefore recognising when a breach has occurred could be challenging for agencies, he added.

Edwards agrees. "The Office of the Privacy Commissioner has had 25 years' experience in identifying harm, so we are accustomed to the idea. However it is quite different showing harm that a person has actually suffered to predicting harm that might occur – and this is something we expect the Select Committee to focus on when it considers the Privacy Bill.

"The threshold should be; is it clear enough for agencies to understand whether an obligation to report harm has been met?"

Agencies should have an agreed plan, strategy and principles for managing data breaches before they happen.

The best thing to do is avoid breaches altogether, he adds, acknowledging there is already a trend within the public sector of improving maturity in privacy practice.

Lessons learned

Edwards discussed incidents where government agencies, rushing the development of new information-sharing products, have taken insufficient care to protect personal or agency information, leading to privacy breaches and closure of the new online portals. Lessons have been learned, he said.

"Having good practice in completing privacy impact assessments, and really testing the risks associated with new innovations, will continue what I think has been a very encouraging trend in the public sector, promoted by the Government Chief Privacy Officer, of learning from our experience and pausing and assessing the risks associated with new applications."

Two further reforms in the current Bill will strengthen and increase the role of the Privacy Commissioner.

The first, compliance notices, will empower the Privacy Commissioner to serve a notice on a non-compliant agency.

"At the moment, I have no ability to enforce compliance," says Edwards. "I can't force anybody to do anything except provide me with information from time to time. So the compliance notice gives me the ability to say: you are not complying with the Privacy Act, now go ahead and comply with the Privacy Act - and they would be obliged to do so."

The second proposed reform, access determinations, will empower the Privacy Commissioner to issue an access determination when a person has been refused access to their personal information.

Edwards says right of access to information has been core to the public sector since 1982. "If an organisation refuses a request for personal information, that person can ask the Privacy Commissioner to investigate. However the organisation currently doesn't have to comply with any recommendation from me, all I can do is bring proceedings to the Human Rights Review Tribunal and the case can take up to three years to be dealt with.

"The access determination would allow me to demand that the organisation release information, and that will be binding on them."

Despite these reforms, Edwards is seeking still more teeth, in what he describes as a 'once-in-a-generation' opportunity to modernise privacy legislation.

"I want the Privacy Commissioner to have the power for genuine sanction. I would like to be able to go to a court and say this organisation has repeatedly ignored its obligations under the Privacy Act and as a result there should be consequences and civil proceedings."

Basic things

Public submissions on the Privacy Bill closed on May 24 and the Bill will now go to the Select Committee. Meanwhile, Edwards offers some essential advice for the public sector, when it comes to managing privacy.

"The day to day things are important; being clear about respecting individuals' preferences, being careful about how information is moved around. Basic things like design are important. If you're being asked to use data in new ways, think about the implications. Ask yourself, are you designing a proportional response that public policies demand?

"Everyone needs to make sure that appropriate, sensible and well managed sharing is enabled. However we must ensure the information is only used for legitimate reasons, and we should not just share for sharing's sake," he adds.

Privacy legislation is actually a positive thing, Edwards says, recalling discussions from an international Data Sharing seminar, held in Melbourne last December.

"Speakers from other jurisdictions agreed that privacy or data protection rules are often wrongly identified as obstacles to information sharing. They reiterated that the keys to success are social license, and clarity and transparency about the objectives and methodologies of the information sharing."

Public sector agencies should see the Office of the Privacy Commissioner as enabling, he adds. "It helps them to achieve their objective. It helps them to maintain the trust and confidence of people across New Zealand. If they are doing things that are counter-intuitive or getting in the way of providing assistance to New Zealanders, then they probably need to check their assumptions and maybe talk to our office."