Presentation by Privacy Commissioner John Edwards to the Employers & Manufacturers Association (EMA) on 13 June 2018 in Auckland

The Privacy Bill

- The Privacy Bill is a reboot of the 25-year-old Privacy Act 1993
- The Bill had its first reading last month, and is currently before Justice and Electoral Select Committee
- Submissions on the Bill closed in late May
- The Bill's genesis is the Law Commission's report and recommendation in 2011
- There's been a long period of review and analysis with the Ministry of Justice
- Fundamental aspects of the Privacy Act remain the same
- The Bill introduces a number of key changes and some new enforcement powers for my office

Current Privacy Bill

What are the key changes in the Privacy Bill?

- Mandatory data breach notification – an agency must notify my office of privacy breaches (defined as unauthorised or accidental access to, or disclosure of, personal information) that pose a risk of harm to people, and to affected individuals.

- Compliance notices – I will be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with the law.

- New criminal offences – it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it. The penalty is a fine up to $10,000.

- Binding decisions on access requests – and I will be able to make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal.

Our submission

I recently made my submission on the Privacy Bill to the Justice and Electoral Select Committee. It recommended:

- Penalty Power - empowering the Commissioner to apply to the High Court for a civil fines to be imposed in cases of serious breaches (up to $100,000 for an individual and up to $1 million for a body corporate)

- Accountability - a power to require an agency to demonstrate its ongoing compliance with the Act
- Letting the Commissioner decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, instead of the Director of Human Rights Proceedings.
- In addition, I also recommended the introduction of these provisions:
    - Protection against the risk that individuals can be unexpectedly identified from data that had been purportedly anonymised
    - Portability - data portability as a consumer right.
    - Erasure, or the 'right to be forgotten' – a right to for individuals to erasure of personal information. This right is also included in legislation currently before the UK Parliament.
    - Algorithmic transparency and automated decision-making – addressing risks to personal privacy from the use of algorithms to make decisions about individuals.

GDPR

- This brings us to Europe, where the new General Data Protection Regulation (GDPR) has introduced much stronger privacy and personal data protections
- We've seen a lot of confusion about how New Zealand businesses will be affected as the build-up to the GDPR comes in
- I think partly the issue is that anxiety is being promoted by people who are talking up the extra territorial elements of the GDPR and the prospect of fines (up to €20 million or 4 percent of global annual turnover - whichever is higher)
- Laws have extra territorial effect only in quite limited circumstances.
- The GDPR says you may be subject to this law if you are effectively operating in Europe
- If you are selling Manuka honey from a website in Northland and somebody in The Netherlands has ordered it and shipped it, and you have their data in your data base, that does not make you subject to the GDPR
- Do you have a base in Europe?
- Are you advertising on your website in European languages?

- These are some of the tests that might indicate that you also have to comply with the legal framework in the GDPR
- Compliance with the New Zealand Privacy Act takes you quite a long way in terms of the GDPR and keeps you pretty safe
- It doesn't get you all the way, and there are a few unknowns about how extraterritorial law will apply – but I think some elements of that concern about companies around the world having to comply are a bit overstated.

Submission on the Employment Relations Act amendments

- One of my functions as Privacy Commissioner is examining new legislation for its possible impact on individual privacy.
- The general principle is that policy and legislation should be consistent with privacy rights unless there is very good reason (and evidence) to override those rights.
- I recently made a submission on The Employment Relations Amendment Bill.
- My submission focussed on a proposed new section which provides that employers must share certain information about new employees with the union unless the employee objects.
- I made it clear that I do not support this approach. It goes beyond what is necessary to achieve the policy objective of ensuring employees are being provided with a genuine choice about joining a union.
- Requiring an individual to opt-out of having their personal information disclosed is poor privacy practice and is against an individual's right to exercise some autonomy over their personal information.

What you can do

- With all this talk of new law, it's important you're up to date with your privacy responsibilities
- Become familiar with privacy and privacy law
- Lead by example
- Put measures in place to mitigate privacy issues

- Take responsibility when issues arise
- Ask OPC for help

Privacy principles

- Principle 1 – when an agency can collect personal information
- Principle 2 – where an agency can collect information from
- Principle 3 – what agencies should tell individuals when collecting their information
- Principle 4 – how agencies should collect information
- Principle 5 – storage and security of personal information
- Principle 6 – an individual's right to access information
- Principle 7 – an individual's right to seek correction
- Principle 8 – an agency's obligation to ensure information is accurate and up-to-date
- Principle 9 – how long an agency can retain information for
- Principle 10 – what an agency can use personal information for
- Principle 11 – disclosure – when to disclose e.g. when a child is at risk
- Principle 12 – using unique identifiers

Employment-related case notes

Staff told of employee sacked for drug use

- A woman was dismissed by her employer after drugs and drug-taking tools were seen in her car while it was parked in the company carpark.
- Three days after her dismissal, her manager emailed over 100 staff disclosing the circumstances of her dismissal.
- The woman found out about the email and complained to our office. She said she was humiliated, and the stress of situation had damaged her confidence and emotional state. She wanted the company to be held accountable and sought compensation.

- Raised concerns under principle 11
- The company said it included the information about the drug possession in the email because it was apparent that staff already knew the information, and because the company had strict policies on drugs and alcohol in the workplace.
- The company did not believe it had breached principle 11 or caused the woman harm because the information in the email was already widely known among staff
- Our view: exceptions in principle 11 do not include the circumstances where the information disclosed is already known to the recipient. And while there was gossip in the workplace about the woman, a disclosure made in an email from a senior manager had considerably more weight, and would have been significantly more humiliating and embarrassing.
- We believed there had been an interference with privacy.
- We attempted to mediate a resolution but both parties declined to participate as they had decided to resolve it themselves. They later reached a settlement.

Academic denied request for 12,000 work emails

- An academic who was dismissed from his university position requested all of his work emails from a 12 month period of his employment on a hard drive.
- The university refused the request. It said the information amounted to about 12,000 emails and they were university property.
- The academic complained to our office. He said the effect of being cut off from his email account meant a significant financial loss, as well as humiliation, loss of dignity and injury to feelings.
- He was applying for two jobs at the time and he said his candidacy for both roles was seriously undermined because of the sudden termination.
- Raised issues under principle 6
- The university disputed that all the emails contained personal information because the majority of them were work-related in content. Also said information wasn't readily retrievable and disclosing the information would involve the unwarranted disclosure of the affairs of another individual.

- Our view: work emails are personal information, but it was reasonable for the university to refuse to provide them on a hard drive.
- We agreed with the university that the mixed nature of the information requested meant the personal information was not readily retrievable.
- We accepted that processing a request for so many emails and determining what was and wasn't personal information would impair efficient administration.
- The university had made an offer to release approved emails in some other form, but the academic declined.
- We formed a final view that there was no interference with the academic's privacy.

OPC resources

- We provide free privacy training modules on our website
- The courses cover a variety of privacy topics, including one that covers privacy in the employment context
- Encouraging your employees to take these courses will make sure they're up to speed and foster a culture of privacy compliance
- If you want to try something new with personal information, do a privacy impact assessment to find out the potential risks
- Recent example from the news; facial recognition technology
- Search "privacy impact assessment" on our website to find our PIA toolkit