

Presentation to Unplugged 2019, ComplyWith NZ Ltd

Te Papa, Wellington

Joanna Hayward, Principal Adviser, Office of the Privacy Commissioner

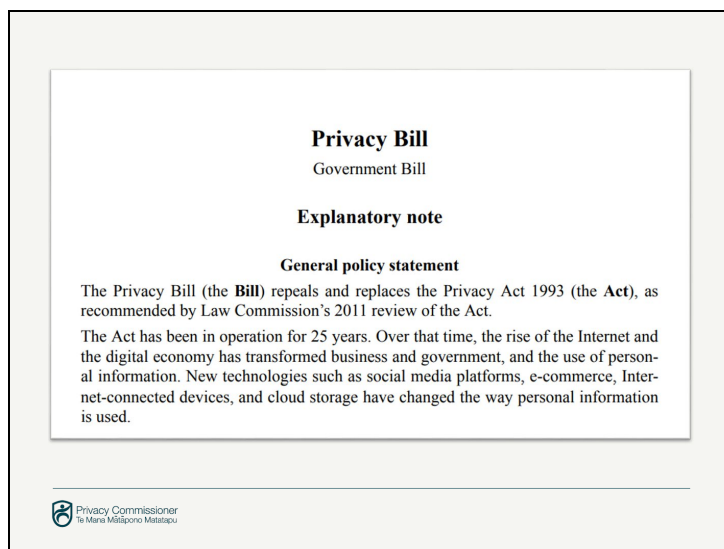
25 July, 2019



The Privacy Act – getting ready for 2020

Hi - Great to be with you to talk about privacy and compliance.

The key takeaway for you today is that it's a great time for organisations to be thinking about privacy and compliance.



With the new Privacy Act approaching, this should be featuring in organisational planning in the current 2019-20 financial year.

For organisations that already have a sound approach to compliance, you can build on this to get ready for new regulation – you won't need to start again from scratch– the new legislation is a lot like the current Act, but with some new requirements added on top. And there's still time to work on compliance to address the new regulation that's coming.

For organisations that are lagging behind in meeting the current requirements, now is the ideal time to catch up with addressing existing weaknesses, so that there's a good foundation in place for the new regulation.

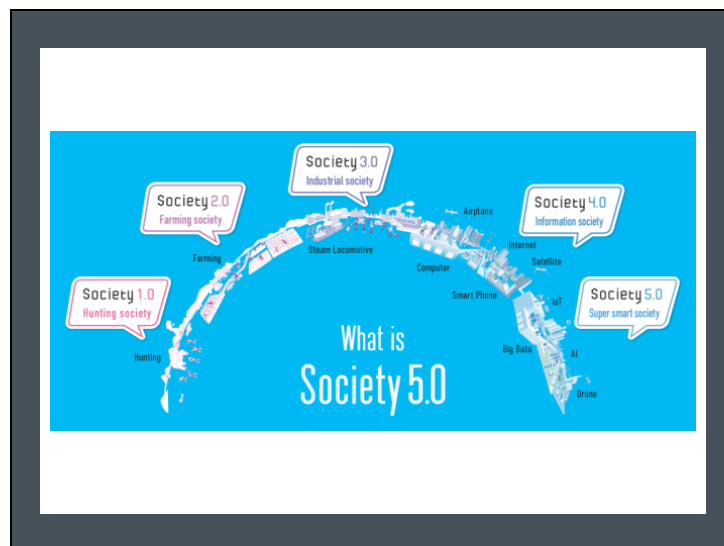
We're estimating it may be about 12 months until the new Privacy Act will come into force i.e. July 2020. We hope the Bill will get through its final stages this year, and be enacted by the end of 2019, and then there's a 6 month lead in period before the new requirements come into effect. So that's a nice buffer of time for organisations to prepare.

Those dates are an estimate, it will depend on the Bill's progress in Parliament, but that's our best guess for now.

But it's not just the Privacy Bill, there are other reasons why it's great timing for organisations to be about privacy right now.

In a nutshell - Data privacy is on trend in a major way.

To break that down a bit I wanted to highlight for you some of key trends that are putting data privacy in the spotlight.



Trend 1. Data itself is a hot topic

- It's the fuel for the Fourth Industrial Revolution (according to the World Economic Forum) and for the shift from the information Society 4.0 to super smart Society 5.0 (as coined by Japan). It's predicted that more and more data is going to connect and inform everything we do.
- And it's valuable – it's a key asset for the Silicon Valley giants as well as small start-ups (a lot of whom now start digital) and for the growth of medium size businesses

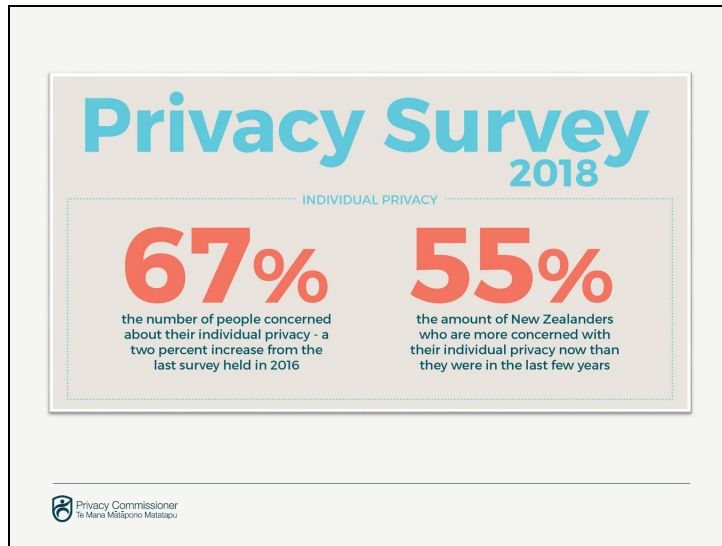


Trend 2. Privacy is a hot consumer topic, and more than ever is equated to trust and accountability.

What's getting a lot of attention and discussion internationally is that the data economy can only operate successfully where there is consumer trust in the way that personal data is managed.

The UK Information Commissioner put it like this. She said:

For me, trust means citizens knowing how their data is being used, how they can control its use, where the data is going, and that no matter where it goes that someone – a privacy commissioner – has their back.



At OPC we monitor trust levels in public surveys.

The 2018 survey results confirm that Kiwis care about their privacy.

Here are some of the stats:

- 67% are concerned about their privacy (a 2% increase from 2016)
- 55% are more concerned than 2 years ago
- 62% trust government agencies with their personal information (a 9% drop from 2014)
- Contrast that with 32% of New Zealanders trust companies with their personal information.

To promote consumer trust, the concept of privacy accountability by organisations who collect and use personal data is becoming an influential concept in privacy regulation. The Australian Information Commissioner described accountability like this. She said:

“Only by demonstrating a commitment to privacy can organisations build and maintain people's trust and a social licence for innovative uses of data,”

What this means in practice is that to be accountable and transparent about the use of personal data, organisations need to have the practices, systems and procedures in place to ensure their privacy compliance and to be able to demonstrate it to consumers and privacy regulators.

Research has found that companies that have embedded accountability for compliance are less likely to have security breaches, or where they do have a security breach, its impact will be smaller.

OPC NZ surveyed the uptake of privacy accountability for last year's global sweep for the Privacy Enforcement Network.

We saw encouraging trends regarding the seniority of privacy officers and clear reporting lines to executive management.

But there did appear to be less focus on privacy accountability in the private sector than in the public sector - several organisations seemed to have minimal privacy or data protection policies in place.

We also found that some organisations had no processes in place to deal with privacy complaints and were not equipped to handle data security incidents appropriately.

This shows us there is still a way to go in embedding accountability in organisations to drive consumer trust.



Trend 3 -Technology continues to make waves

Technology is constantly introducing new privacy challenges for organisations to manage - from digital advertising and chatbots to facial recognition and Artificial Intelligence.

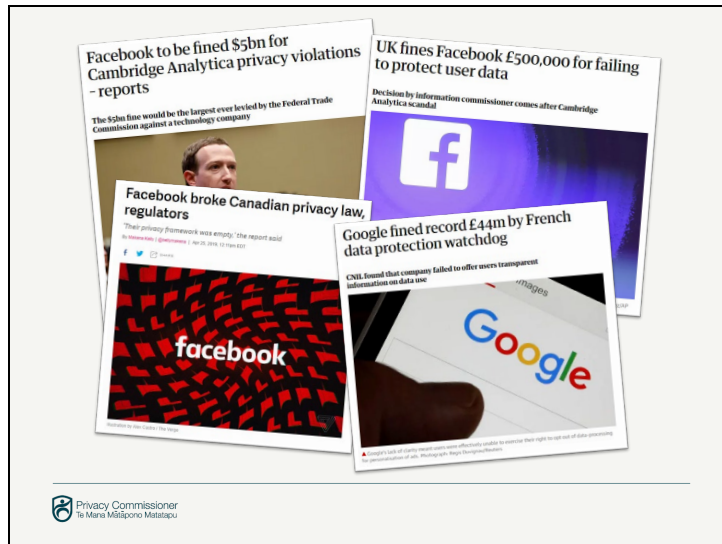
New tech provides market opportunities, greater efficiencies and growth. But it can also create privacy risks that need to be factored in before the roll-out.

Organisations first need to do their privacy due diligence – understanding the issues and risks, before diving in, so that the tech doesn't have unintended consequences that are then hard to dial back.

For example, there is a lot of discussion internationally about accountable and ethical approaches to AI.

Facial recognition is also making headlines over the last year– with privacy concerns being raised about the technology including issues of accuracy, bias and discrimination.

These issues can't be ignored when adopting new technology, but they can be anticipated and well managed.



Trend 4 - Privacy continues to make the news

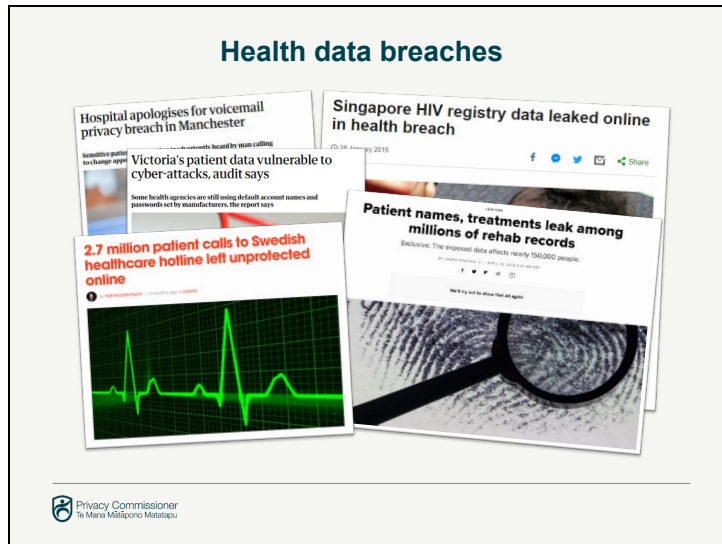
Privacy continues to make big headlines over 2018-19 (notably in a crowded news cycle).

The big tech companies have been in the spotlight, due to the scale of the breaches and hence the large regulatory fines imposed.

Facebook has faced investigations in the US, Canada and the UK stemming from the Cambridge Analytica scandal and the improper use of the private information of Facebook users.¹

Google has also received a large fine from the French data protection authority for a lack of transparency about its use of data for ad targeting.

¹ Netflix, the Great Hack <https://www.netflix.com/nz/title/80117542>



There have been lots of international data breach stories, and a number of health sector breaches.

These health sector examples illustrate the type of weaknesses that cause breaches:

- technology and security glitches in the cases of Manchester hospital where a man ringing to change his appointment heard sensitive voicemails left by other patients,
- an absence of proper security precautions:
 - firstly, in the case of the Swedish healthcare line that used an unsecure server and
 - secondly with the unsecure database of addictions treatment patients in the US,
- the risk of unauthorised access in the case of the breach of the Singapore HIV register, and
- a weak security culture in Victoria's public health system.



NZ privacy headlines

Back home NZ has had its own share of privacy headlines.

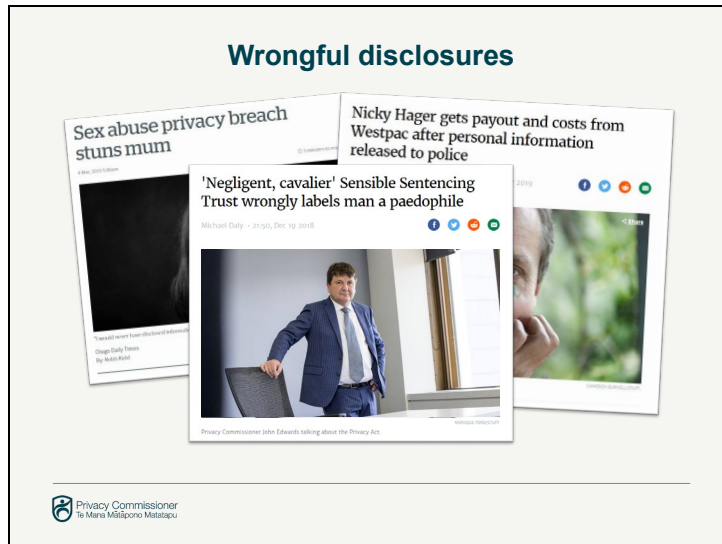
Manner of information collection

This example illustrates a privacy issue with the manner in which personal information was collected by MSD about beneficiaries.

Our recent inquiry found MSD's information gathering practices, to be intrusive on privacy due to unnecessarily broad requests for information from third parties including highly sensitive information such as text messages and birthing records.

The Privacy Commissioner therefore made a number of recommendations for changes to MSD's information collection practices.²

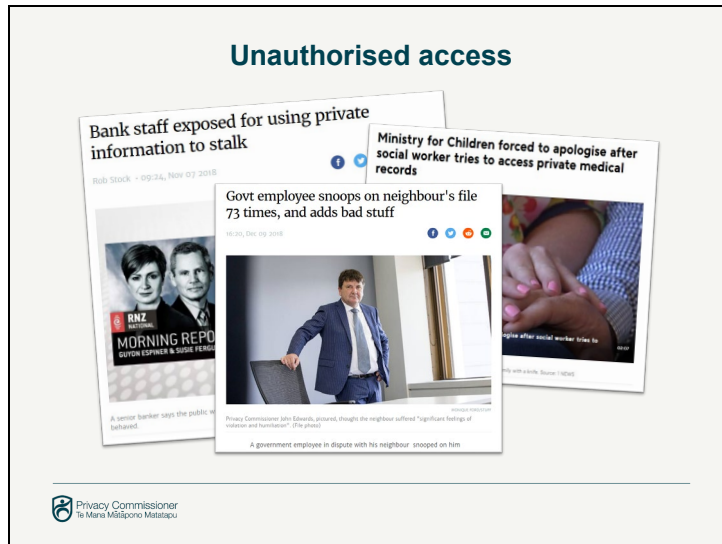
² <https://www.privacy.org.nz/news-and-publications/statements-media-releases/msd-fraud-investigations-privacy-commissioner/>



Wrongful disclosures

We also had examples of wrongful disclosures. For example, the Sensible Sentencing Trust was found to have interfered with a man's privacy by wrongly labelling him a convicted paedophile on its website. The trust failed to meet its obligation to ensure volunteers received appropriate privacy training, with serious consequences for the man's reputation and peace of mind.³

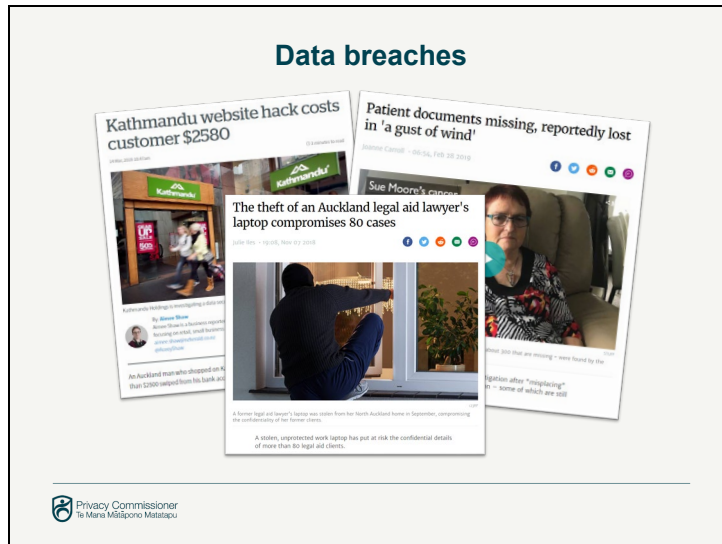
³ <https://www.privacy.org.nz/news-and-publications/statements-media-releases/naming-sensible-sentencing-trust/>



Unauthorised access

We had examples of unauthorised access to personal information within organisations. Notably, the Privacy Commissioner put banks on notice they need to do more to protect customers' private information from bank staff engaging in employee browsing, after a spate of complaints.⁴

⁴ <https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-calls-on-banks-to-do-more-to-protect-privacy/>



Examples of data breaches

And we had examples of data breaches. For example, the theft of a legal aid lawyer's unprotected laptop put the sensitive information of 80 clients at risk.⁵

There is more information on these stories on our website – you can subscribe to our online weekly newsletter to keep you posted about topical cases like these.

⁵ <https://www.privacy.org.nz/blog/privacy-in-the-news-2-8-november-2018/>



Internationally regulation is ramping up

It's now a year since the European General Data Protection Regulation came into force. The GDPR has been a gamechanger in privacy regulation.

It's added new consumer privacy rights like data portability (the right for consumers to shift data between service providers), the consumer right to challenge automated decision making about them by organisations and the right to have personal data deleted in some circumstances.

The GDPR has had a big impact internationally because of the large fines that can be imposed for breaches and its global reach to any company doing business in Europe that uses the data of European citizens.

This includes NZ companies doing business in Europe and therefore need to calibrate their privacy compliance to GDPR standards. If you're already having to comply with the GDPR, then complying with the NZ Privacy Act will be pretty straightforward.



NZ is getting a new Privacy Act

This brings us to the Privacy Bill. Last year the Privacy Act 1993 celebrated 25 years.

That's a long time ago, the early days of the internet, when we had email and basic (i.e. not at all smart) phones but no Google, social networks or digital cameras. In 25 years, the digital age has completely overhauled the operating environment for privacy regulation.

Privacy law reform has therefore been talked about for a while now, and new legislation is on the horizon.

So what can we expect in the revamp?

On the one hand a lot hasn't changed. The reforms are incremental, rather than the gamechanger we've seen with the GDPR from Europe.

It's fair to say that the new Act is a refresh of the existing Act. It's going to look pretty familiar. All the core features of the old Act have been retained – the privacy principles, privacy complaint rights, Codes of Practice, OPC investigations and dispute resolution, and legal proceedings by complainants in the Human Rights Review Tribunal. All these key elements are still the foundation of the new legislation.

As much of the current Act is being kept, that means compliance systems don't have to be drastically changed, but updated and strengthened.

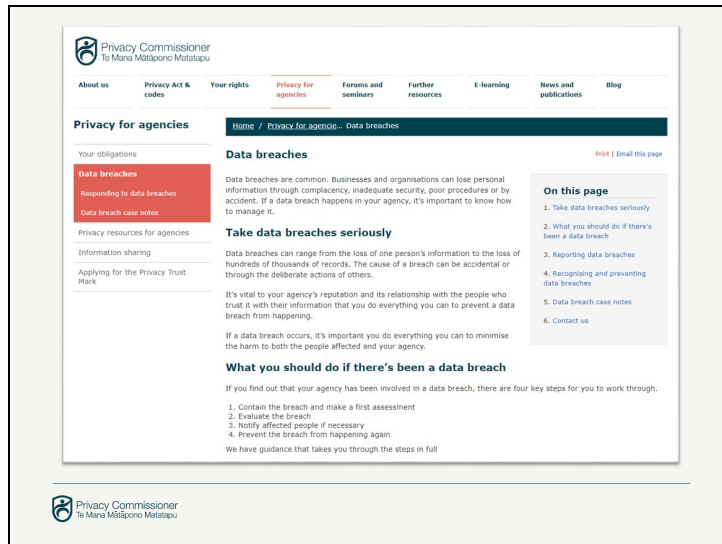
Privacy Bill 2019 – key changes

- Mandatory data breach notification
- Cross-border disclosure – new principle 12
- Compliance notices
- Access determinations

So what's being added?

There are 4 key changes recognising the need to beef up the regulatory framework in certain areas.

The first big change is the **new breach notification scheme**.



Currently, we have a voluntary data breach notification scheme and guidelines. Here's our current web help site.

If you're familiar with the current data breach guidelines, this will mean you should be in good shape for the new mandatory requirements but it's a good chance to check your data breach processes, and if there's one feature of the new law that you highlight to your employees, this should be it. Because everyone in an organisation contributes to a successful data breach strategy – both how to avoid breaches, what to watch out for, taking account of human error, and then the work of mitigating and containing a data breach when it happens.

We're now catching up with privacy regulation in other countries like Australia, the US and Europe that expressly require organisations to notify affected individuals and the relevant Privacy Commissioner when there's been a serious data breach – this fits with the accountability approach– that where something goes wrong when you're looking after peoples' data, organisations should take responsibility for informing them and be accountable to the privacy regulator.

There is a list of factors in the legislation to help work out if the data breach is sufficiently serious to report.

If the breach is serious, there are several exceptions to having to tell individuals that their data has been breached. These exceptions balance up that in some situations it could be more harmful to tell the individual concerned or there are other public interests to take into account.

For example, it could present a security risk if there's a vulnerability that could be further exploited. These exceptions provide some useful leeway but organisations will need to justify relying on them when they report to the Privacy Commissioner on what's happened.

OPC will be issuing guidance and tools to help navigate the new requirements.

And we strongly advise organisations to get familiar with the new data breach scheme ahead of time and proactively develop and test your response strategy.



Cross border disclosures

The second new requirement to think about ahead of time is the new privacy principle 12 for cross border disclosures of personal information. If your organisation is one that discloses sensitive customer information to organisations outside NZ, then you'll need to take steps to check if the information is going to a destination that has data protection laws.

Why has this been added? In our increasingly interconnected world, as data now routinely flows across borders, New Zealanders' data needs to be protected by more than just the NZ Privacy Act – it also needs to be protected when it's being stored and used overseas, beyond the reach of the NZ regulation.

So it's a priority for organisations to review how and where personal data is being disclosed to foreign entities and whether or not there are data protection laws in place in the data destination.

The good news here is there are several practical exceptions that can be used to manage this requirement:

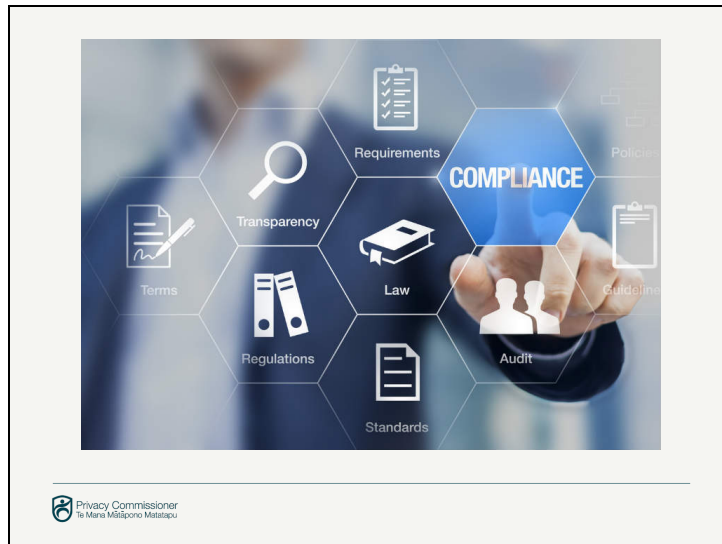
- 1st, the new principle doesn't apply if the foreign entity is subject to the NZ Act because it's carrying on business here. It's only when data is leaving the coverage of the NZ Privacy Act, that you need to do any checking.
- 2nd, if the foreign entity is a cloud service provider and is holding or processing the data on your behalf, then the new requirement doesn't apply because that's not considered to be a disclosure – you remain accountable for the personal data that you're housing in the cloud, and the data is still subject to the NZ Privacy Act.
- 3rd, if the disclosure is necessary because of a serious threat to health and safety, or to avoid prejudice to the maintenance of the law, and it's not reasonably practicable to comply with the new privacy principle, the disclosure can go ahead in these urgent circumstances.
- 4th, if you explain to the individual that the data won't be protected by comparable safeguards to NZ and the individual authorises the disclosure, it can proceed.

It's therefore advisable to do a stock take of what kind of personal information you disclose and to whom, what privacy laws are engaged, and which of the exceptions and mitigation strategies might be available to continue to enable those disclosures going forward.



What about the Privacy Commissioner's new powers?

Organisations need to factor in more proactive enforcement action by the Privacy Commissioner in calling out privacy breaches. Unlike our UK counterparts, we don't the power to enter premises in enforcement jackets but the NZ Commissioner does get some new powers.



Compliance notices

Under the new regime, we will continue to investigate complaints, but the Commissioner will also be able to look at issuing a compliance notice if he considers that an organisation is in breach of the Act or a code of practice.

The new compliance notice power is not unfettered, as it has a number of checks and balances:

- The Commissioner can't issue a compliance notice without first giving the organisation a chance to comment on a draft notice
- A compliance notice has to set out in reasonable detail what the issue is, what steps the organisation needs to take, and the timeframe for complying
- An organisation can appeal to the HRRT if it disagrees with all or part of the compliance notice.

A valuable exercise when reviewing your approach to compliance is to ask yourself what are the weaknesses in your systems that could trigger a compliance notice? How serious are they, how could they be strengthened and what can you do now to reduce the risk of future regulatory attention?



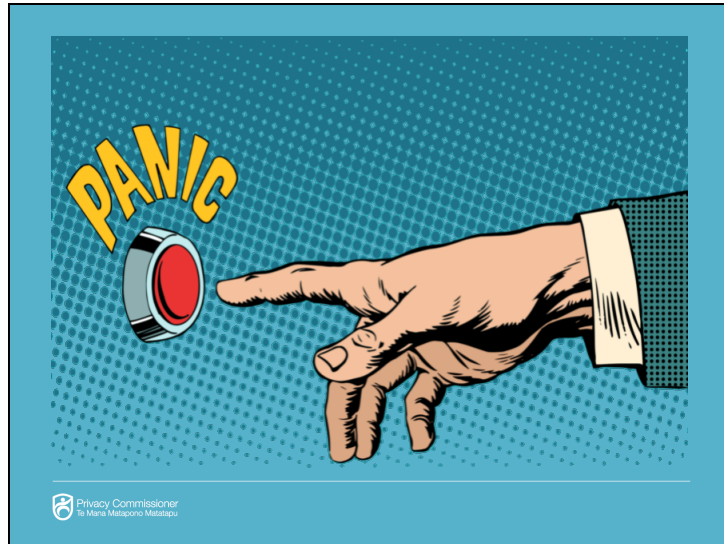
Access determinations

The other new power is that the Privacy Commissioner will become the decision-maker on access requests under principle 6 where an individual asks an organisation for their own personal information. This is an extremely important consumer right under the Privacy Act. People are entitled to ask for their own personal information without having to give any particular reason, and to get a response from the organisation within 20 working days. The individual is entitled to receive the information promptly unless there is a good basis for withholding the information.

This right remains at the heart of the Privacy Act and the Privacy Commissioner will now be able to direct an organisation to comply by issuing an access direction. An access direction will require the organisation to deliver an individual's personal information to them that the Commissioner considers they are entitled to.

The organisation can appeal an access direction to the Human Rights Review Tribunal.

Our strong advice is to make sure that your processes for access requests operate smoothly and efficiently so that you can be confident of compliance once the new regulatory powers become operational.




In conclusion

- Is it time to hit the panic button yet? – no it looks like there's still time to get ready
- Great opportunity to take stock and self-audit your compliance processes
- use the next 12 months to prepare
- All the basics still need to be done well – we recommend you check on those first
- Take time to understand your responsibilities under the new law
- Update your compliance processes to deal with the new responsibilities and accountabilities

Home / Blog / Privacy 2.0: The beginning

Print | Email this page

Privacy 2.0: The beginning Annabel Fordham 2 July 2019



This is the first in what will become a series of blog posts on the new Privacy Act, the changes, and what we'll be doing to implement those law changes.

We'll try and cover all the key changes in the law and give readers a clear view on any areas they will need to address.

This is the place to come to keep up to date with Privacy 2020. Let us know if there are topics you particularly want us to cover, and we'll do our best to prioritise those. Email: communications@privacy.org.nz


At the time of writing, the Privacy Bill is in the midst of its second reading in the House. There are no definite dates for enactment, but best guesses are in the last quarter of 2019, with a commencement date 6-months later.

The new Act will have a range of new enforcement tools. We'll outline those in coming posts.

One thing the new law will also give the Privacy Commissioner is a greater ability to say to complainants, "Sorry, that may be a concern, but this is not something we can take on." We've found over the years that there are issues that people bring to us that we cannot realistically help them with. For instance, it may have happened a long time ago. The new Act clarifies the grounds under which the Commissioner may decline to investigate a complaint. These additional grounds are:

Privacy Commissioner
Te Mana Māhiora Matatapu

Are you ready for breach notifications? Yves Blackwood 17 July 2019



As you may already know, both winter and privacy breach notifications are coming. And while you may have already prepared for winter and its influx of colds and flu, it's also important to prepare for mandatory breach notifications, so that your agency is ready when the requirements kick in.

New Zealand currently falls into a group of countries for which privacy breach reporting is voluntary – but the privacy law reform underway in Parliament will change that. The Privacy Bill, which is likely to be passed by Parliament this year and become law in 2020, will introduce a mandatory breach notification regime.

The effect of this is that your agency will have to notify both the individual and the Privacy Commissioner in certain circumstances if the agency experiences a serious privacy data breach.

What will I have to notify?

Agencies won't have to notify every single breach. The threshold for notifiable breaches isn't finalised, but it is likely to only cover privacy breaches where there is the risk of serious harm. The threshold aims to balance the compliance burden on agencies, while making sure that affected individuals are notified, and minimising the risk of 'notification fatigue'.

Once the Privacy Bill has passed, the Privacy Commissioner will publish more information on how the breach notification reporting will operate, and when privacy breaches must be reported.

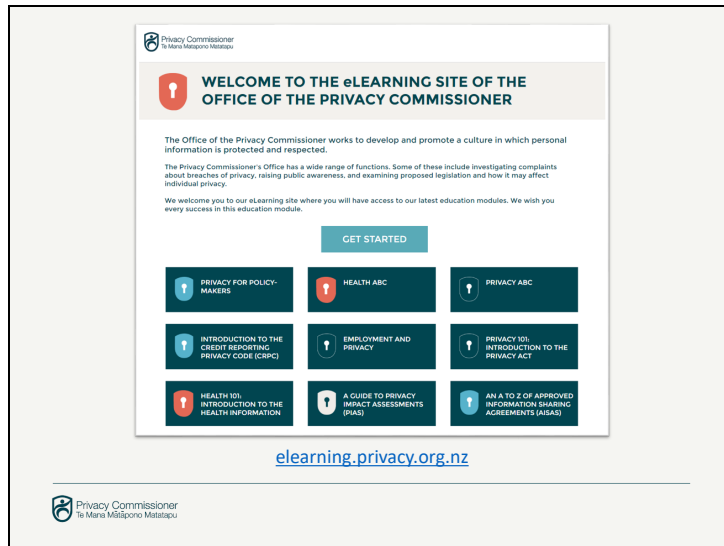
In the meantime, this is a great time to take stock of your existing policies and procedures to prevent, mitigate, and report data breaches, check that they're still best practice (update

Privacy Commissioner
Te Mana Māhiora Matatapu

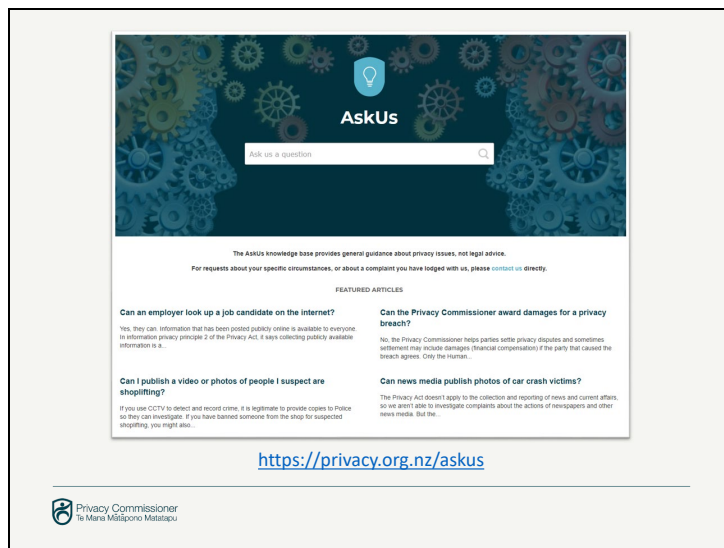
OPC resources

OPC has a range of resources and we will be updating these for the new legislation. It's a great time to subscribe to our newsletter for information.

Our first blogs on getting ready for the Privacy Bill have been published this month – intro blog on the Bill and getting ready for breach notification in the health sector.



You may also want to check out our free online training modules for staff who are responsible for privacy.



Your staff can also ask us privacy questions online at AskUs



The advertisement features a central image of a metallic, industrial-looking tank with two red-handled valves on top. The text "Priv-o-matic" is written in a stylized, cursive font across the tank, with the tagline "The easy privacy statement generator." underneath it. Below the image is a blue hyperlink: <https://privacy.org.nz/further-resources/privacy-statement-generator/>. At the bottom left, there is a logo for the Privacy Commissioner of New Zealand, with the text "Privacy Commissioner" and "Te Kaitiaki Take Kōwhiri" below it.

And if you need a simple privacy statement, try our Priv-o-matic privacy statement generator to get started.

From OPC, kia kaha and best of luck in getting ready as the new legislation approaches.

Thank you.