Privacy Act Review

Q & A

What is the Privacy Act?

The Privacy Act regulates what can be done with information about individuals. It applies to all "agencies," which includes the government, business and voluntary sectors, and non-government organisations.

The Act generally requires agencies to handle personal information in line with 12 information privacy principles, which guide how personal information can be collected, used, stored and disclosed. The principles are designed to govern personal information at all points of its lifecycle, from its collection to destruction.

Why does the Privacy Act need to be revised?

The current Act was enacted in 1993, and since then, advances in technology have dramatically changed how information is collected, stored and shared. The Act needs updating and future proofing.

These proposed reforms will put strong incentives in place to ensure that organisations that hold or deal with people's personal information take privacy seriously.

Sound privacy law is good for people, business, and government. The reforms we are proposing will help improve public confidence in privacy laws and assist agencies that use personal information to operate effectively.

What are the key changes?

The reforms put the onus on information holders to identify and address risks before they occur.

If they don't put appropriate measures in place to protect personal information or people's privacy is breached, the Privacy Commissioner will be able to take action.

The key proposals include:

- **Mandatory reporting:** Agencies will have to report data breaches to the Privacy Commissioner, and notify affected individuals in serious cases. Specific criteria in the new Act will determine which breaches must be notified.

- **New offences and increased fines:** Agencies that fail to notify the Commissioner of a privacy breach could be fined up to $10,000.

  It will be against the law to impersonate a person or pretend to have their authorisation to obtain that individual's personal information, or to have it altered or destroyed. Also, it will be illegal to destroy documents containing personal information that a person has sought access to. Both offences will carry a fine of up to $10,000.

Existing maximum fines (for example, for obstructing the Commissioner) will increase from $2,000 to $10,000

- **Enhanced powers:** the Privacy Commissioner will have new powers, such as the ability to issue compliance notices. The Commissioner's current power to independently decide to investigate a privacy issue will be enhanced.

- **Global protections:** the revised Act will clarify an agency's obligations when they send personal information off-shore for storage or processing. It will also introduce a new obligation where an agency discloses information overseas, to ensure that the information is protected and subject to acceptable privacy standards in the country it is disclosed to.

- **Guidance and clarity:** The Office of the Privacy Commissioner will provide more guidance about how to comply with the Privacy Act. Also, technical improvements to the Act will make it clearer and easier to understand.

The proposals are in line with recommendations made by the Law Commission in its review of New Zealand's privacy laws.

What difference will these proposals make to the public?

The reforms will give people greater confidence that agencies are handling their information appropriately.

The changes will also ensure people's privacy is better protected if a breach occurs.

What difference will these proposals make to businesses, organisations and government agencies?

It will be easier for agencies to comply with the Act and to make good decisions about privacy issues.

The reforms will also allow government and businesses to efficiently and effectively use information to deliver services and grow the economy.

Would the changes have made a difference to the privacy breaches covered in the media in recent years?

It's difficult to answer without looking at each case and assessing how and why the breach happened.

Regardless, these proposals will help identify privacy risks earlier and reduce the risk of harm to individuals when breaches do occur.

What protections does the Act currently offer people?

If someone believes their privacy has been breached and they cannot resolve the issue with the agency concerned, they may complain to the Privacy Commissioner. The Commissioner can also decide to investigate privacy issues they become aware of.

The Commissioner will attempt to help people and agencies reach an agreement. They can also make recommendations to address issues following an investigation. However, the Commissioner cannot impose penalties, such as awarding damages.

If the Commissioner cannot resolve a dispute, they may ask the Director of Human Rights Proceedings to consider taking the matter to the Human Rights Review Tribunal.

The Tribunal can require an agency to do something or to stop doing something, and has the power to award damages if the person who complained has been harmed.

What new powers will the Privacy Commissioner have?

Currently the Privacy Commissioner has limited powers to help prevent breaches from occurring, or to take action if they do.

The revised Act will bolster the Commissioner's awareness of breaches, and improve the Office's ability to conduct investigations and take appropriate action.

Key elements of the new regime include mandatory notification of breaches; enhancements in the Commissioner's powers to independently decide to investigate a privacy issue; and compliance notices.

Mandatory data breach notification

Mandatory reporting of privacy breaches is critical for the Commissioner to become aware of, and begin to address, emerging issues prior to harm occurring.

The reforms propose a two-tier notification regime:

- **Tier one:** agencies will have to take reasonable steps to notify the Commissioner of any material breaches as soon as reasonably practicable. In deciding if breaches are material agencies will take into account factors such as the sensitivity of the information, the number of people involved and whether there are indications of a systemic problem.

- **Tier two:** for more serious breaches, agencies will have to take reasonable steps to notify the Commissioner and affected individuals of breaches where there is a real risk of harm (such as actual or potential loss, injury, significant humiliation or adverse effects on rights or benefits).

Agencies that do not notify the Commissioner of breaches will be liable, upon conviction, to a fine of up to $10,000 (a new offence).

Similar to existing fines in the current Act, this will only apply to private sector agencies. For now, the Government considers that the prospect of being 'named and shamed' is the most effective deterrent to ensure public sector agencies report breaches.

The two tier option outlined above will give the Commissioner a fuller picture of privacy risks across New Zealand and enable the identification of widespread problems before serious breaches occur.

Enhanced powers to initiate investigations

Investigations initiated by the Commissioner are known as 'own motion investigations'.

The proposed reforms will allow the Commissioner to make urgent requests, and increase the penalty for non-compliance with requests for information.

Currently the Commissioner can launch an "own motion inquiry" into any matter if it appears the privacy of an individual is being, or may be, infringed. The Commissioner has compulsory information-gathering powers and can summon witnesses.

Anyone who does not comply with the Commissioner's requests commits an offence and if convicted is currently liable to a fine of up to $2,000. This fine will increase to a maximum of $10,000, as will other existing fines (for example, for obstructing the Commissioner)

The Commissioner will also have discretion to decrease the 20 working days time frame within which agencies have to comply.

Compliance notices

The Commissioner will be able to issue compliance notices for breaches of the Act. Compliance notices will require an agency to do something, or to stop doing something.

Compliance notices will be enforced by the Human Rights Review Tribunal.

Currently the Commissioner can only make recommendations and has limited ability to act if they identify wider concerns with systems or procedures, or if agencies are unwilling to comply.

What obligations will there be for agencies that 'outsource' information for storage or processing?

It is common for private sector businesses, and some public sector agencies, to use overseas service providers to store or process information. Examples include when businesses use overseas based 'cloud computing' services or overseas call centres.

The revised Act will clarify that New Zealand agencies will be accountable for what happens to information they outsource to offshore service providers. For example, if the overseas company has a privacy breach, the New Zealand organisation may be subject to a complaint under the Act or may have to notify the breach. New Zealand agencies will not be accountable where the overseas service provider discloses information because foreign laws require them to.

Since this proposal clarifies what is generally understood to be required by existing law, there should be few, if any, costs for agencies that already comply with this obligation.

Agencies will also be accountable for information they outsource to a domestic service provider.

What are the proposed obligations for "cross-border disclosures"?

Cross-border disclosures occur when a New Zealand business or government agency gives information to a business or agency from a different country, for the latter's own use.

When disclosing information overseas, New Zealand businesses and agencies will have to ensure that acceptable privacy standards are in place on the receiving end.

To help New Zealand businesses and agencies meet this requirement, the Act will provide guidance about the definition of "acceptable privacy standards" and the steps they should take. The Commissioner will also be able to publish a list of countries with acceptable privacy laws, so that New Zealand businesses or agencies can determine relatively easily if overseas companies or organisations they are dealing with are likely to have adequate measures in place.

New Zealand businesses or agencies will not be accountable where the overseas agency breaches any contract, or discloses the information because foreign laws require them to. Also, there will be several exceptions to the cross-border disclosure rules, such as when individuals have given their permission, or when sharing the information will help maintain the law or address threats to health and safety.

New Zealand agencies will be accountable if they do not take reasonable steps to protect personal information before it leaves their control. They will also be accountable if they do not confirm that an exception applies.

Will the proposals increase compliance costs for agencies? What is being done to mitigate these costs?

Overall, the reforms will create few – if any – additional costs for agencies that already have good systems in place to protect the privacy and security of people's personal information.

The proposals related to the Commissioner's new and enhanced powers will involve only marginal costs in comparison to existing obligations.

Increased guidance from the Privacy Commissioner will also help agencies to meet their obligations to identify and address risks before they occur.

This will help reduce the likelihood and severity of breaches, which would otherwise create significant costs for agencies and people affected by the fallout of such events.

Measures such as the requirement to notify affected individuals about serious breaches may create some compliance costs for agencies. However, the Government considers that both the need to protect people's privacy and the long-term benefits of increased public confidence in agencies outweigh the costs.

Are the changes consistent with international comparisons?

Yes. Generally, Canada, the United Kingdom and Australia either have broadly similar functions and powers in place, or will have in the near future.

The changes are also consistent with newly revised OECD Guidelines (adopted in July 2013). The OECD Guidelines form the basis of New Zealand's privacy regime.

Implementing these proposals will add to New Zealand's reputation as a good place to do international business, and will contribute to economic growth and prosperity.

The proposals will help ensure, for example, that New Zealand continues to enjoy its EU Adequacy status, which is a major advantage to New Zealand business.

How do these reforms support other Government privacy initiatives?

The Government takes all aspects of privacy and security seriously. There is work underway across government to help agencies build their privacy and security culture and capability, including the establishment of the Government Chief Privacy Officer, which will provide privacy leadership and support across State Service agencies.

Strengthening the role of the Privacy Commissioner reinforces this wider programme of work. The GCPO and the Privacy Commissioner are complementary roles and will work together to lift privacy performance.

How do these reforms relate to wider justice initiatives?

The proposed changes complement Government initiatives to protect New Zealanders online, such as the Harmful Digital Communications Bill.

That Bill introduces a range of measures to address damaging online communications and to ensure perpetrators can be held to account for their actions.

It includes a new offence of using a communications device with the intent of causing harm. This would apply to communications that are grossly offensive or indecent, obscene, menacing or knowingly false. It will carry a maximum penalty of up to 3 months' imprisonment, or a $2,000 fine.

The offence will also cover serious instances of intimate recordings being published online without a person's consent.

What decisions have been made previously?

The Government made preliminary decisions on the Law Commission's report in March 2012. Cabinet agreed that the Privacy Act should be repealed and replaced by a new Bill which retains the principle-based framework. Cabinet's recent decisions will shape the content of the new Bill.

Also, in early 2013, Parliament passed laws to improve information sharing between agencies that deliver public services.

The changes amended the Privacy Act to allow new information sharing agreements between government agencies, and between government agencies and non-government organisations that deliver public services.

The changes also ensure that agencies (such as medical professionals, social workers, Police, Civil Defence and others) can share personal information to address serious threats to public health or safety, or when a person's life or health is threatened. Previously a threat had to be both "serious and imminent".

What targeted consultation will take place before a Bill is introduced to Parliament?

An exposure draft of the Bill will be released for targeted technical consultation before the Bill is introduced into the House.

This will provide an opportunity for businesses and government agencies to comment on how well technical details in the draft Bill will work in practice.

Interest groups and members of the public will also have an opportunity to comment on the policy proposals during the Select Committee phase.

Will the Privacy Commissioner receive additional funding?

As previously announced in the 2014 Budget, the Government recently increased the Privacy Commissioner's funding to help keep up with a rise in demand for its services.

The Office's operational budget was $3.2 million a year for the past several years. It will receive an additional $7 million over the next four years – $1.9 million in 2014/15 and $1.7 million a year thereafter – to carry out the functions it currently performs under the Act.

Once the Privacy Act is revised and re-enacted, the Government will decide whether the Office will receive further funding to deliver the new functions related to these reforms.