Privacy Foundation NZ

Position Paper on Privacy Act 2020

- ✓ *Where we stand*
- ✓ *What is needed*
- ✓ *Future law reform*

NOVEMBER 2020

www.privacyfoundation.nz

Position Paper on Privacy Act 2020

Where we stand | What action is needed | Further law reform

The Privacy Foundation NZ has warmly welcomed the enactment of the Privacy Act 2020.[1] The new Act has the potential to do many good things. We acknowledge and celebrate the improvements from the 1993 law. However, the 2020 Act is not a perfect law. We have held some concerns from when the law was first proposed in Parliament and made a submission and contributed to the reform process.[2] We have identified further concerns now that the bill is enacted.

Some of the concerns we hold can be minimised or fixed by the way the law is implemented. Others may warrant amendment when an opportunity arises to change the law. We have prepared this position paper as a resource for anyone interested in privacy law and as an aid to the Foundation's work as we move forward.

The report works through the Act Part by Part and then notes some "missing pieces" not appearing in the law. Foundation documents elaborating on some points are footnoted.

This is a living document and may be revised from time to time as the strengths and weaknesses of the Act become apparent and in relation to other developments.

Contents

Highlights … 3
Parts 1-9 of the Act … 3-10
The missing pieces: what the law is lacking … 11-12

[1] Privacy Foundation, New Privacy Bill welcomed, March 2018, and Privacy Foundation welcomes new privacy law, June 2020.
[2] Privacy Foundation, Submission on Privacy Bill, May 2018 ("2018 submission").

Highlights

The Foundation particularly supports the following reforms made by the 2020 Act:

- ✓ the extended application to overseas agencies;
- ✓ the reforms to the news entities exemption;
- ✓ the additional determination and enforcement powers placed with the Privacy Commissioner;
- ✓ the requirement for the Privacy Commissioner to "take account of cultural perspectives on privacy"
- ✓ the emphasis on collection minimisation (IPP 1);
- ✓ the heightened attention paid to collection from children and young persons (IPP 4);
- ✓ the cross-border transfer principle (IPP 12);
- ✓ the obligation on agencies to minimise the risk of misuse of unique identifiers (IPP 13);
- ✓ the streamlined access determination and enforcement arrangements;
- ✓ mandatory breach notification;
- ✓ the power of the Privacy Commissioner to issue compliance notices; and
- ✓ the newly created offence provisions and the increase in penalties from those applying under the 1993 Act.

However, the reforms will only achieve their potential if the new requirements are vigorously implemented by agencies and the new powers are fully and effectively exercised by the Privacy Commissioner. The Foundation offers some suggestions and encourages agencies, privacy officers, the Office of the Privacy Commissioner (OPC) and other stakeholders in the task.

There are a number of areas where the Foundation considers the new Act needs amendment or further reform. In particular, we call upon the Minister of Justice to commence reform work to address GDPR-type privacy protections where that reform work was postponed until after the bill was enacted.

Part by Part comments: Parts 1-9 of the Act

Part 1 Preliminary provisions

Part 1 contains 'machinery' provisions that are critical throughout the Act such as definitions and rules about the application of the law to agencies, overseas agencies, employees and agencies processing information.

Observation: Much of the content is carried over from the 1993 Act unaltered. One significant change is the extended application to overseas agencies. Another is the narrowing of the news media exemption to entities subject to complaints procedures.

Foundation position: The Foundation supports:

- the extended application to overseas agencies;[3]
- the reforms to the news entities exemption.[4]

Implementation actions needed:

- Some of the provisions related to application are complicated: Entities such as OPC, the Government Chief Privacy Officer and industry associations need to provide clear explanatory materials to stakeholders.
- Special attention needs to be paid in the implementation to the position of "overseas agencies" to ensure that the potential of the extended application is achieved and to avoid "business as usual" e.g. overseas agencies carrying on business in New Zealand must appoint a privacy officer and that person needs to be accessible to New Zealanders.

Reform:

- The time lag between the Law Commission review of privacy law completed in 2011 on which the Act is based and the enactment of the 2020 Act, has meant that the law has failed to fully address identified privacy challenges of our digital age. For example, close attention should be paid to the new rights and obligations incorporated in international privacy instruments after 2011.
- Consideration should be given to reforming the definition of "personal information" to address individuation (the ability to disambiguate or 'single out' a person in the crowd, such that they could, at an individual level, be tracked, profiled, targeted, contacted, or subject to a decision or action which impacts upon them - even if that individual's 'identity' is not known or knowable).[5]
- The exemption for members of Parliament in their official capacities should be reviewed following the leaking of medical information by an MP with a view to ensuring the application of standards and accountabilities in a constitutionally appropriate way.

[3] 2018 submission, para 23-25. See also Briefing for the Incoming Minister of Justice: Hon Andrew Little (Preserving New Zealand's Data Sovereignty), February 2018.
[4] 2018 submission, para 29.
[5] Anna Johnston, Individuation: re-imagining data privacy laws to protect against digital harms, BPW WP 624, July 2020.

- The exemption of the Ombudsmen from the Act is unjustified and should be removed or at least narrowed in relation to personal information about any employee or former employee of the Ombudsmen in their capacity as an employee.

Part 2 Privacy Commissioner

Part 2 contains provisions relating to the Privacy Commissioner.

Observation: Much of the content is carried over from the 1993 Act. One change is a requirement for the Privacy Commissioner to "take account of cultural perspectives on privacy".

Foundation position:

- The Foundation supports the additional powers placed with the Commissioner (generally under other Parts of the Act).
- The Foundation supports the requirement for the Privacy Commissioner to "take account of cultural perspectives on privacy".

Implementation actions needed:

- To achieve the potential of the new Act the functions and powers need to be fully exercised — this requires proper funding and strategic management.
- The powers and functions need to be exercised in a transparent way: in the transition from the 1993 to 2020 Act there needs to be public explanation of the way new powers are to be used and the positive benefits for individuals demonstrated.
- Ongoing research into, and discussion of, cultural perspectives on privacy is warranted.

Law reform:

- The new powers vested with the Privacy Commissioner will be beneficial but may prove not to be sufficient to enforce compliance. The need for additional powers should be kept under review and, in particular, the suggestion that the Commissioner be vested with the power to impose civil penalties should be considered.

Part 3 Information privacy principles and codes of practice

Part 3 contains 13 information privacy principles (IPPs) and provides for codes of practice.

Observation: Most of the IPPs are unchanged from the 1993 Act. A new IPP 12 (Disclosure of personal information outside New Zealand) is included and the unique identifier principle is changed. There are no longer any Public Register Privacy Principles nor provision for public register codes.

Foundation position: The Foundation supports the new cross-border transfer principle (IPP 12) and the new obligation on agencies to minimise the risk of misuse of unique identifiers (IPP 13).

Implementation actions needed:

- Review, research and concerted action are needed by both the Privacy Commissioner and agencies, to give effect to:
    - The new emphasis in IPP 1(2) on minimising collection of identifiable information, including creating and promoting anonymous and pseudonymous options.
    - The new emphasis in IPP 4(b) on fair and reasonable practice in relation to circumstances where personal information is being collected from children or young persons.
    - The new obligations in IPP 13(4)(b).
- Research and education of agencies in relation to techniques of de-identification and anonymization of personal information.

Law reform:

- Further IPPs are warranted to addresses the risks and opportunities of the digital age as exemplified by updates to international privacy instruments since 2011 including, for example, in relation to data portability (see "The missing pieces: What the law is lacking" below).

Part 4 Access to and correction of personal information

Part 4 sets out how access and correction requests are to be handled.

Observation: Part 4 continues the effect of Parts 4 and 5 of the 1993 Act although restructuring the ways in which the provisions are set out.

Foundation position: While the re-structuring of the provisions has not been an unqualified success with some opportunities missed to improve usability, the substantial improvements to the complaint procedures and enforceability (Part 5) for access should more than compensate for any presentational shortcomings.

Implementation actions needed:

- As the law remains substantially the same, it will be helpful for OPC to republish existing guidance, or an index, aligned with the new provisions.

Reform:

- The Foundation would like the "evaluative material" limitation on access narrowed in some way to reflect the greater expectation of transparency that should exist now compared with when these provisions were first conceived in 1981 by the Danks Committee.[6] The problem with refusing an access request for that reason is that the withheld information is being used to take a decision affecting an individual.
- The novel provision allowing for release of properly withheld information on conditions (s 54) should be reviewed to ensure that it is not open to abuse (particularly where third party interests are at stake) and that any conditions are enforceable.

Part 5 Complaints, investigations, and proceedings

Part 5 provides for complaints, investigations, and proceedings.

Observation: Part 5 continues the successful complaints handling arrangements from the 1993 Act but, amongst other things, streamlines and strengthens access arrangements through introduction of access directions.

Foundation position: The Foundation supports the streamlined access determination and enforcement arrangements.

Implementation actions needed:

- Innovation is needed to take advantage of new provisions. OPC needs to find optimal ways of speeding up process.
- Requesters and agencies should work constructively with the new systems to achieve positive sum outcomes with faster access given and litigation reserved for specific points needing judicial determination.
- Relevant stakeholders - OPC, the Director of Human Rights Proceedings and the Chair of the Human Rights Review Tribunal - should develop administrative practices to support class actions as an effective way to use the Act's complaints and tribunal processes to address systemic issues.
- OPC should make it easier for individuals to access interpretation facilities for lodging complaints.

Law reform:

- Section 74(1)(a) risks imposing too high a burden on individuals and should be narrowed to encourage individuals to first complain to an agency where it is reasonable to do so rather

[6] Committee on Official Information, Supplementary Report, July 1981.

than make "reasonable efforts to resolve the complaint directly with the agency".[7] Indeed, sometimes it may be unsafe for the individual to engage with the respondent further than registering a complaint.

Part 6 Notifiable privacy breaches and compliance notices

Part 6 introduces notifiable privacy breaches and compliance notices to the Act's compliance toolbox.

Observation: The mandatory breach notification regime, and the power for the Commissioner to issue compliance notices, are amongst the Act's most significant innovations.

Foundation position: The Foundation supports:

- Mandatory breach notification; and
- The power of the Privacy Commissioner to issue compliance notices.

Implementation actions required:

- There needs to be transparency regarding all breach notifications received by the Privacy Commissioner if the full potential of the notification scheme is to be achieved. Comprehensive statistics, consistent with international practice, is the minimum expected but publication of full details (possibly after some delay and with redactions if warranted) would be desirable for the purpose of research and analysis.
- OPC needs to be willing to issue compliance notices early and in a variety of cases, and not restrict their use to a final resort in serious cases, if the full potential of the compliance scheme is to be achieved.
- Section 123(1)(a) OPC should issue guidance on types of breaches that might be subject to compliance notices in addition to those listed in s 69(2)(a) (breach of IPP, information sharing agreement, non-compliance with notification requirements) as clearly other breaches are contemplated. For example, failure to appoint a privacy officer (s 201).
- Section 123(1)(b) likewise OPC should issue guidance on what other actions may be targeted as a breach of an IPP or interference under another Act. Some examples of other Acts that may fall into this category are needed. For instance, might misuse of information contrary to the provisions of legislation governing public registers be targeted?
- Section 123(2)(a) also needs OPC guidance on what types of harm might be targeted other than the types listed in s 69(2)(b) (damage, loss of benefit, injury to feelings etc.). For

[7] Section 74(1)(a) provides that "The Commissioner may decide not to investigate a complaint if, in the Commissioner's opinion, the complainant has not made reasonable efforts to resolve the complaint directly with the agency concerned".

example, might data aggregators who source publicly available information from the Internet and other sources and on sell it or provide services using such information be included where this can cause harm from say lack of awareness of such practices or vulnerability on the part of individuals? Another example is harms from individuation (see Part 1 above). Should this be included even where an individual's identity is not known or knowable?

Law reform:

- Section 116(1)(d) which exempts an agency from notifying individuals of a breach because of a "trade secret" should be repealed or made subject to a public interest test.[8]

Part 7 Sharing, accessing, and matching personal information

Part 7 contains schemes for authorising and regulating sharing, accessing and matching information that might otherwise contravene the IPPs.

Observation: Part 7 consolidates the several Parts of the 1993 Act dealing with sharing, accessing, and matching personal information with little change. The principal change is provision for phasing out of information matching controls in favour of the looser information sharing regime.

Foundation's position: The Foundation takes the view that the sharing and matching authorised under this Part have the potential to adversely affect individual privacy and therefore must be strictly limited, include rigorous safeguards and provide redress for when things do not work as intended.

Implementation actions required:

- There should be more active efforts by agencies to describe and report on information sharing arrangements than occurred under the 1993 Act. These should be easy to find on a website, and made available in a timely way, even if key details are also reported in an agency's annual report.

Law reform:

[8] Section 116(1)(d) provides that "An agency is not required to notify an affected individual or give public notice of a notifiable privacy breach if the agency believes that the notification or notice would be likely to reveal a trade secret". It may be contrasted with s 52 which has a public interest test for trade secrets in the context of an access request ("Subsection (1) does not apply if, in the circumstances of the particular case, the withholding of that information is outweighed by other considerations that make it desirable, in the public interest, to make the information available.") See also 2018 submission, para 46.

- In accordance with good administrative law practice, there should be statutory criteria set out for the exercise of powers in s 153(b) to exempt an agency from giving notice of adverse action.[9]
- To maintain the Privacy Commissioner's independence, reference in s 158(2) to obtaining the Minister's consent before undertaking a review should be removed.

Part 8 Prohibiting onward transfer of personal information received in New Zealand from overseas

Part 8 provides for the issue of transfer prohibition notices.

Observation: The Part is unchanged from the 1993 Act.

Part 9 Miscellaneous provisions

Part 9 deals with several miscellaneous matters.

Observation: Part 9 continues largely without change provisions from the 1993 Act. Notable additions include several new offences and provision for regulations for recognising both other countries' privacy laws and binding schemes.

Foundation position: The Foundation:

- supports the newly created offence provisions and the increase in penalties from those applying under the 1993 Act; and
- calls for increased penalty levels so that fines may be effective, dissuasive and provide sufficient scope for sanctions that are proportionate to the offending.[10]

Law reform:

- The level of penalties applying to corporate bodies and for repeat or continuing offences should be substantially raised.[11]

[9] The *Legislation Guidelines*, Chapter 16, 2018 edition, issued by the Legislation Design and Advisory Committee (LDAC) and approved by Cabinet provide that "Legislation should set out the criteria for granting [an] exemption".
[10] The phrasing of this recommendation draws upon the EU GDPR which provides that corrective measures should be "effective, proportionate and dissuasive": GDPR article 83(1). See also EDPB, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 3 October 2017 endorsed 25 May, 2018.
[11] 2018 submission, para 48. See also Briefing for the Incoming Minister of Justice: Hon Andrew Little (The Potential for Abuse of Corporate Power), February 2018.

The missing pieces: What the law is lacking

The 2020 Act suffers from the 10-year gap between when the Law Commission undertook its research for the privacy review, culminating in its 2011 report, and the enactment of the new law. This delay meant that some of the features and problems of the digital age that are now apparent were then not then so well understood. Especially problematic is the fact that the 2011 review predated revisions of the key international instruments on privacy (completed respectively: OECD 2013, APEC 2015, EU 2016, Council of Europe 2018).[12] Given its international influence, the key oversight amongst these is the failure fully to assess and, where appropriate, adopt or adapt the new rights contained in the EU General Data Protection Regulation (GDPR).[13]

The Foundation recommends incorporation into the Act of provisions suitably adapted for New Zealand law dealing with the following GDPR-inspired rights or obligations:

- Right to personal information portability.[14]
- Algorithmic transparency and challenge.[15]
- Mandatory privacy impact assessment.[16]
- Right to erasure.[17]
- Special controls on biometrics.[18]

We consider these rights are important for the protection, and empowerment, of New Zealanders in the digital age. We also see the inclusion of some or all of them as desirable from an economic perspective to ensure than New Zealand maintains its status as providing an adequate level of data protection for the purposes of EU data protection law.[19]

We would like the Act's accountability mechanisms strengthened as has been recommended in privacy instruments adopted by OECD (2013) and APEC (2015). This would require agencies to be able to demonstrate to the Privacy Commissioner how they are complying with the law.[20]

---

[12] OECD = Organisation of Economic Cooperation and Development; APEC = Asia Pacific Economic Cooperation; EU = European Union.
[13] Media release, Privacy Foundation's initial response to Justice Committee's Report on Privacy Bill, 15 March 2019.
[14] 2018 submission, para 13-15.
[15] 2018 submission, para 57. GDPR, articles 21 and 22.
[16] GDPR, article 36. 2018 submission, para 57.
[17] 2018 submission, para 58.
[18] GDPR, article 9(1).
[19] 2018 submission, para 5-7, and Foundation letter to the Minister of Justice, Enactment of Privacy Bill remains vital during emergency, 8 May 2020. See also Briefing for the Incoming Minister of Justice: Hon Andrew Little (New Zealand's reputation and branding), February 2018.
[20] Media release, Privacy Foundation's initial response to Justice Committee's Report on Privacy Bill, 15 March 2019.

We have also previously called for the law to address the risks of re-identification of de-identified information.[21] We expect that this may be usefully accommodated in the proposal above to reform the definition of "personal information" to address "individuation". If that reform is not adopted then attention should be paid explicitly to the risks of re-identification of de-identified information.

We also recommend that special attention be given to the risks to personal safety in relation to publication of details on statutory registers.[22] We note that attention to these issues may be diminished by the repeal of the public register controls.

[21] 2018 submission, para 20-22.
[22] 2018 submission, para 53-56.