Privacy Act 2020

YAO DONG*

I INTRODUCTION

Twenty-seven years after the Privacy Act 1993 (1993 Act) was enacted, the Privacy Act 2020 (2020 Act) has finally updated New Zealand's privacy law and brought it into the digital economy. The process was long and often delayed. The Law Commission undertook a five-year privacy project from 2006 to 2011. Its recommendations were mostly implemented in the Privacy Bill (Bill), which was introduced seven years later on 20 March 2018 by the Hon Andrew Little MP.[1] The Bill passed its third reading on 24 June 2020. It comes into force on 1 December 2020.

In summary, the key changes in the 2020 Act are:

(1) broader application of the statute to New Zealand and overseas agencies;
(2) introduction of an information privacy principle (IPP) covering disclosure of personal information overseas;
(3) a breach notification system;
(4) a compliance notice procedure to deal with breaches; and
(5) new criminal offences: to mislead an agency to access an individual's personal information, or to destroy personal information knowing that a request has been made in respect of that information.

However, significant aspects of the 2020 Act remain unchanged, leaving it partially unaligned with international privacy instruments and the privacy laws of New Zealand's trading partners. Most notably, the 2020 Act is not fully aligned with the Organisation for Economic Co-operation and Development (OECD) Guidelines,[2] the Privacy Act 1988 (Cth) of Australia and the General Data Protection Regulation (GDPR) of the European Union (EU).[3] Interestingly, the campaign by the Privacy Commissioner (Commissioner) for substantial civil penalties was ignored.

---

* Solicitor, Russell McVeagh. The author would like to thank Joe Edwards for his helpful comments.

1 Privacy Bill 2018 (34).

2 *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, C(80)58/FINAL as amended by C(2013)79, 11 July 2013) [OECD Guidelines].

3 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 [GDPR].

This note examines the key changes in the 2020 Act and how well these changes respond to the reasons the reforms were required, including keeping up with New Zealand's trading partners and technological developments. This note concludes that the 2020 Act plugs some gaping holes in the 1993 Act, but further and ongoing work on privacy reforms is required to bring and keep New Zealand up to date.

II BACKGROUND

The way we use personal information has changed dramatically since the 1993 Act. The intervening years have seen the rise of the Internet and the digital economy, and the emergence of new technologies such as social media platforms, e-commerce, Internet-connected devices and cloud storage.[4] These changes increasingly challenge the way we protect personal information as privacy values evolve. As early as 2006, the Law Commission began work with a view to updating the 1993 Act. The work was conducted in four stages, culminating in a review of the 1993 Act. The Law Commission published its final report on 30 June 2011.[5]

The intentions of the Law Commission's review of the 1993 Act were to ensure:[6]

> (1) consistency with international privacy instruments and the privacy laws of New Zealand's trading partners;
> (2) relevance and effectiveness as technology continues to develop;
> (3) that lessons are learned from practical experience as the 1993 Act aged; and
> (4) that privacy is balanced with other rights and interests.

The Law Commission saw a need to emphasise that other rights and interests can justifiably override privacy,[7] and recommended the inclusion of a purpose section that recognises privacy is not an absolute right or value.[8] Additionally, the Law Commission thought that the purpose section should refer to international privacy standards, including the OECD Guidelines.[9]

4 Privacy Bill 2018 (34) (explanatory note).
5 Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123, 2011).
6 At [1.15].
7 At [2.15]–[2.22].
8 At [2.34].
9 At [2.35].

The Law Commission recommended the enactment of a new Act rather than amending the old Act, due to the numerous changes proposed.[10] Overall, the Law Commission concluded that the 1993 Act struck the right balance between privacy and other rights and interests through the inclusion of exceptions and exemptions.[11] Despite this, the Law Commission's recommendations would involve some rebalancing in particular areas.[12]

The Law Commission believed that the 12 IPPs, which were fundamental to the 1993 Act's operation, should be assessed against four criteria. The principles should be high-level statements of standards and responsibilities, not detailed or prescriptive (although with room for a higher level of detail in the exceptions), general in scope and application, and clear and simple.[13] The IPPs had generally worked well for almost 20 years at the time of the review, so the Law Commission approached the reform of the IPPs as an exercise in improvement, rather than replacement.[14]

Between the Law Commission's final report in 2011 and the introduction of the Bill in 2018, there were a number of important developments in international privacy instruments and the privacy laws of New Zealand's trading partners. The OECD revised its Guidelines in 2013 and introduced, among other things, the concept of data security breach notifications.[15] Australia passed major privacy reforms by amending the Privacy Act 1988 (Cth).[16] The amendments took effect on 12 March 2014. Further, in 2017, Australia established a Notifiable Data Breaches scheme that commenced on 22 February 2018.[17] In the EU, the GDPR passed on 27 April 2016 and entered into force on 25 May 2018. This regulation established data protection requirements for controllers and processors that process personal data on data subjects in the EU, regardless of the controller or processor's geographic location. Under the GDPR, data subjects have strong enforceable rights, harmonisation across EU Member States has increased and international data transfers are only permitted if the European Commission has determined that the destination country offers an adequate level of data protection.[18]

10 At [2.5].
11 At [2.15] and [2.22].
12 At [2.22].
13 At [3.3].
14 At [3.2].
15 OECD Guidelines, above n 2, at 26–27.
16 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth).
17 Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).
18 European Commission "Commission report: EU data protection rules empower citizens and are fit for the digital age" (press release, 24 June 2020); and GDPR, art 45.

III LEGISLATIVE PROCESS

By the time the Bill was introduced on 20 March 2018, privacy reforms were long overdue. Mr Little referred to the revised OECD Guidelines and the GDPR in his introduction speech on the Bill.[19] The Bill was intended to better align New Zealand's privacy law with the OECD Guidelines and GDPR so that New Zealand could maintain its adequacy status under the GDPR when it entered into force a little over two months later.[20] The Bill was also introduced as a Bill to modernise privacy protection, and a regime focused on risk management rather than retrospective remedies.[21]

The Bill was referred to the Justice Committee on 11 April 2018. The Justice Committee considered 162 submissions.[22] It made a number of key changes to the Bill, including the insertion of an application section and a new IPP, and the threshold for mandatory notification of privacy breaches.[23] The Bill passed its second reading on 7 August 2019.

Final changes to the Bill were made by a supplementary order in the Committee of the whole House.[24] The Bill passed its third reading on 24 June 2020, under urgency to make up for lost time from the COVID-19 lockdown. It enjoyed cross-party support from the first reading through to the passing of the 2020 Act, in light of the fact that the National Government began preparation of the Bill in 2012 and the Labour Government introduced it in 2018. The most controversial aspect of the parliamentary debates on the Bill was who should receive credit.

IV KEY CHANGES IN THE 2020 ACT

While there are important changes in the 2020 Act covered in this section, it should be noted that the 2020 Act is still principles-based, following the Law Commission's recommendation. In submissions to the Law Commission for retaining the 1993 Act's principles-based approach, rather than moving towards a more prescriptive, rules-based approach.[25] This was consistent with the Law Commission's concern with ensuring that the 1993 Act would be future-proof and flexible.

19 (10 April 2018) 728 NZPD 3105.
20 At 3105.
21 At 3104.
22 (7 August 2019) 740 NZPD 13045.
23 Privacy Bill 2018 (34-2), cls 3A, 19 and 117(1).
24 Supplementary Order Paper 2020 (482) Privacy Bill 2018 (34-2).
25 Law Commission, above n 5, at [2.11].

Purpose Section

The 2020 Act has a new purpose section. It states that the Act's purpose is to promote and protect individual privacy by providing a framework for protecting information privacy, and giving effect to internationally recognised privacy obligations and standards in relation to information privacy.[26] Following the Law Commission's recommendations, the purpose section recognises that privacy may need to be balanced with other rights and interests. The section refers to the OECD Guidelines, as well as the International Covenant on Civil and Political Rights.

Application

The 2020 Act applies more broadly than the 1993 Act. The whole of the 2020 Act, except s 212 in relation to offences, applies to New Zealand agencies, overseas agencies carrying on business in New Zealand and non-resident individuals who collect or hold information in New Zealand.[27] Notably, this affects overseas agencies such as Google and Facebook.[28]

Section 212 applies to New Zealand agencies, overseas agencies, individuals present in New Zealand, and overseas persons who commit any part of an offence in New Zealand or cause any event necessary to complete an offence in New Zealand.

New IPP

A new IPP 12 limits disclosure of personal information under IPP 11.[29] An agency can only disclose personal information to a foreign person or entity if, among other things, the agency believes on reasonable grounds that the foreign person or entity is subject to comparable privacy laws or the privacy laws of a prescribed country.[30] It may also be disclosed when said information is otherwise protected in a way comparable to the 2020 Act — for example, under a contract.[31] Failing belief on reasonable grounds that the information will have comparable protection, an agency can only disclose personal information to a foreign person or entity if it informs the individual concerned of the risks, and the individual consents.[32] This reflects a push by the Commissioner for consent to disclosure.[33]

26 Privacy Act 2020, s 3.
27 Section 4(1).
28 Graydon Hayes "Privacy 2.0: Key changes in the Privacy Act 2020" (16 June 2020) Privacy Commissioner <www.privacy.org.nz>.
29 Section 22 IPP 12.
30 Section 22 IPP 12(1).
31 Section 22 IPP 12(1)(f).
32 Section 22 IPP 12(1)(a).
33 John Edwards "Privacy Commissioner's Submission on the Privacy Bill to the Justice and Electoral Select Committee" at [3.33]–[3.35].

Breach Notification System

The 2020 Act implements a breach notification system, which mandates notification of some privacy breaches.[34] A notifiable privacy breach involves:[35]

> (a) "unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of", personal information; or
> (b) an action that prevents an agency from accessing personal information on either a temporary or permanent basis; where it is reasonable to believe that the privacy breach has caused, or is likely to cause, serious harm to an affected individual.

The rationale behind this system is that notification would allow the individual to mitigate the harm from the privacy breach in serious cases.[36] The threshold had increased from risk of harm in the first version of the Bill to likely serious harm in the second version. This change came after a large number of submissions to the Justice Committee expressed concern that too many privacy breaches would be notified with the original threshold, which was lower than the thresholds in Australia and the EU.[37] Under the 2020 Act, in assessing the likelihood of serious harm, the agency must consider:[38]

> (a) any action taken by it to reduce the risk of harm following the privacy breach;
> (b) sensitivity of the personal information;
> (c) the nature of the harm;
> (d) the person that may have obtained the information;
> (e) any security measures protecting the information; and
> (f) any other relevant matters.

After becoming aware that a notifiable privacy breach has occurred, the agency must notify the Commissioner as soon as practicable.[39] It must also notify the affected individual(s) unless it is not reasonably practicable to do so, in which case the agency must give public notice.[40] There are exceptions to the obligation to notify and grounds to delay notification.[41] Failure to notify

34 Sections 114 and 115.
35 Section 112(1).
36 Law Commission, above n 5, at [7.19].
37 (7 August 2019) 740 NZPD 13045.
38 Section 113.
39 Section 114.
40 Section 115.
41 Section 116.

the Commissioner is an offence, with a possible defence that the agency did not consider the privacy breach to be notifiable on reasonable grounds.[42]

Compliance Notice Procedure

The 2020 Act empowers the Commissioner to issue compliance notices if they consider there has been a breach of the 2020 Act, an action that is deemed a breach of an IPP or a breach of a code of practice issued under the 2020 Act.[43] This is a significant development. It addresses the Law Commission's concern that the complaints process under the 1993 Act did not always provide a solution as quickly or efficiently as it should and that, like any complaints process, it was ad hoc and ineffective in dealing with systemic problems.[44]

There are mandatory considerations that the Commissioner must take into account before issuing a compliance notice.[45] However, they only have to be considered to the extent they are relevant and readily available to the Commissioner.[46] The Commissioner must give the agency concerned a reasonable opportunity to comment before issuing a compliance notice.[47] Once a compliance notice is received, the agency must comply with the notice as soon as practicable and remedy the breach by the date stated in the notice unless the notice is cancelled, suspended, varied or modified.[48]

The Commissioner has power to publish details of a compliance notice if they consider publication to be in the public interest.[49] Compliance with a notice is enforceable by proceedings in the Human Rights Review Tribunal (Tribunal).[50] The only ground for objection to enforcement proceedings is if the agency believes that there has been full compliance with the notice.[51] The Tribunal may grant enforcement orders and costs.[52] Failure to comply with an enforcement order is an offence punishable by a fine of up to $10,000.[53]

New Offences

There are two new offences under s 212 of the Act. The first is the offence of misleading an agency by impersonating an individual, or falsely pretending to be an individual or to be acting under the authority of an individual, to obtain access to that individual's personal information or to have that individual's

42 Section 118(1) and (3).
43 Section 123(1).
44 Law Commission, above n 5, at [6.19] and [6.63].
45 Privacy Act 2020, s 124(1).
46 Section 124(2).
47 Section 124(3).
48 Section 126(2).
49 Section 129.
50 Section 130.
51 Section 130(2).
52 Section 133(1)(a) and (c).
53 Section 133(3).

personal information used, altered or destroyed.[54] The second is the offence of destroying any document containing personal information, knowing that an access request has been made in respect of that information.[55]

Health and Safety Exceptions

Health and safety is an area where the 2020 Act rebalanced privacy with other rights and interests in accordance with the Law Commission's recommendations. New health and safety exceptions were inserted in the IPPs and other parts of the 2020 Act.

A new exception to IPP 2 allows the collection of personal information from a person other than the individual concerned if the agency believes on reasonable grounds that non-compliance is necessary to prevent or lessen a serious threat to life or health.[56] Section 49(1)(a)(i) provides a new health and safety ground for refusing access to personal information under IPP 6. An agency may refuse access to personal information if disclosure would be likely to pose a serious threat to *public* health or *public* safety, or to the life, health or safety of *any* individual. "Serious threat" is a higher threshold than "prejudice" to the physical or mental health of the individual requesting the information, which was an existing ground under s 29(1)(c) of the 1993 Act.[57] This ground continues to exist under s 49(1)(b) of the 2020 Act, but the range of practitioners that the agency can (and is required to) consult has been expanded.[58]

Related to the new health and safety ground under s 49(1)(a)(i) is a separate ground under s 49(1)(a)(ii) for refusal of access where disclosure of the information would "create a significant likelihood of serious harassment of an individual". There is also a third new ground for refusal in this area, under s 49(1)(a)(iii), where providing the information under IPP 6 would include disclosure of information about a victim of an offence or alleged offence, and would cause significant distress, loss of dignity or injury to feelings of this victim.

Other Changes in Relation to IPPs

A new sub-clause in IPP 1 now expressly prohibits the collection of an individual's identifying information if the lawful purpose for which personal information about the individual is collected does not require identifying information.[59] This change was intended to facilitate anonymity and pseudonymity in interactions with agencies.[60] This sub-clause has a

54 Section 212(2)(c).
55 Section 212(2)(d).
56 Section 22 IPP 2(2)(e)(v).
57 Law Commission, above n 5, at [3.87].
58 Section 49(2).
59 Privacy Act 2020, s 22 IPP 1(2).
60 Law Commission, above n 5, at [3.148].

counterpart in Australia's Privacy Act 1988 (Cth), which provides that individuals must have the option of not identifying themselves or using a pseudonym when dealing with an APP entity.[61] This applies unless the APP entity is required or authorised by law to deal with individuals who have identified themselves, or anonymity is impracticable.[62] The new sub-clause in IPP 1 is more open-textured.

Under IPP 4, an agency is now required to consider what constitutes a fair and not unreasonably intrusive means of collecting personal information with particular reference to the circumstances of the case where children or young persons are involved.[63]

The Commissioner is now able to issue an access direction after completing an investigation in relation to access to personal information under IPP 6. If the parties cannot settle the complaint, the Commissioner has the option of making an access direction, referring the complaint to the Director of Human Rights Proceedings (Director), or taking any other action that the Commissioner considers appropriate.[64] An access direction may require an agency to provide access to personal information.[65] Compliance with an access direction is enforceable by an access order granted by the Tribunal.[66] Allowing the Commissioner to make access directions should improve efficiency, especially in cases where the individual requires access to their personal information quickly.[67]

In relation to IPP 8, under the 2020 Act an agency cannot use *or disclose* personal information without taking reasonable steps to ensure that the information is "accurate, up to date, complete, relevant, and not misleading".[68] Previously, the agency only had to take reasonable steps to ensure these matters before using (and not before disclosing) personal information.[69]

News Entity Exclusion

The 2020 Act does not apply to news entities because they are excluded from the definition of "New Zealand agency" under s 8. This exclusion was previously the "news medium" exclusion under the 1993 Act. The definition of "news entity" under the 2020 Act is different to the definition of "news medium" under the 1993 Act.[70] News entities must not only be in the business of or partly in the business of a news activity (which includes publishing on the Internet), but also be subject to independent oversight that includes a

61 Privacy Act 1988 (Cth), sch 1 cl 2.1.
62 Schedule 1 cl 2.2.
63 Privacy Act 2020, s 22 IPP 4(b).
64 Section 91(5).
65 Section 92(1).
66 Section 104.
67 Law Commission, above n 5, at [6.45].
68 Section 22 IPP 8.
69 Privacy Act 1993, s 6 IPP 8.
70 Privacy Act 2020, s 7(1); and Privacy Act 1993, s 2(1).

complaints procedure.[71] Examples of such overseers are the Broadcasting Standards Authority or the New Zealand Media Council. Further, Radio New Zealand and Television New Zealand are no longer treated differently to private broadcasters, and are no longer subject to the application of IPPs 6 and 7, as they were in the 1993 Act.[72]

Regard to Cultural Perspectives on Privacy

The concept of privacy is focused on the individual and conflicts with collective interests.[73] There is a question as to how well the flexible principles-based approach of the 2020 Act can accommodate different cultural views about the nature and value of personal information. For example, the concepts of whānau and hapū rely on sharing within a group, and information may belong to the group rather than an individual.[74] Other cultural and religious communities may also have different views on the sharing of personal information.[75] Under the 2020 Act, a new matter that the Commissioner must have regard to is "cultural perspectives on privacy".[76] This is limited acknowledgement of cultural diversity in an area of law that is inherently based on a Western concept.

V CHANGES NOT MADE

Despite the desire for consistency with international privacy instruments and the privacy laws of New Zealand's trading partners, and lobbying by certain parties, some changes that would have brought New Zealand into line with legislation in other jurisdictions such as Australia did not make it into the 2020 Act. For example, the 2020 Act continues to not require agencies to notify individuals in relation to the collection of their personal information if it is not collected from the individual concerned (because one of the exceptions under IPP 2 applies). The Australian Privacy Act 1988 (Cth) treats any unsolicited personal information that an APP entity receives, and is not required to destroy or de-identify, in the same way as solicited information collected by the APP entity.[77] However, in New Zealand there was opposition to a change that would require notification for information not collected from the individual. Some submissions to the Law Commission argued there was no identified problem with the status quo, the benefits of the change did not warrant the compliance costs, individual notification would often be impracticable and a

71 Privacy Act 2020, s 7(1).
72 Privacy Act 1993, s 2(1).
73 Law Commission, above n 5, at [12.35].
74 At [12.36].
75 At [12.38].
76 Privacy Act 2020, s 21(c).
77 Privacy Act 1988 (Cth), sch 1 cl 4.4.

notification requirement could backfire if the notification went to the wrong person.[78]

The 2020 Act also does not include an openness principle, which appears in the Privacy Act 1988 (Cth), the GDPR and the OECD Guidelines.[79] An openness principle would require agencies to make information about their handling of personal information more widely available.[80] The Law Commission did not support the inclusion of an openness principle. It considered that it would be unreasonable to expect very small agencies to develop a privacy policy, and it would be very difficult to set a threshold that agencies would be required to comply with.[81]

Some rights recognised under the GDPR were not included in the 2020 Act, despite support from the Commissioner and other submissions to the Justice Committee. For example, the GDPR contains rights to data portability, erasure and algorithmic transparency.[82] Further, the Commissioner argued strongly for civil penalties for serious or repeated privacy breaches, these penalties being available in Australia and the EU.[83] These changes were not recommended by the Justice Committee — there was scepticism that they would be needed in New Zealand.[84] Mr Little commented that further consideration was required, and such changes should be considered in future work on privacy reforms, rather than delaying the progress of the Bill.[85]

One of the Law Commission's most significant recommendations that was not adopted in the 2020 Act was that the Commissioner should be able to decide whether to bring proceedings in the Tribunal, without referring the matter to the Director.[86] The Law Commission considered that the rationale for splitting conciliation and litigation functions was weak, there was confusion about the role of the Director and the system seemed inefficient.[87] The potential disadvantages of the recommendation were that the Office of the Commissioner would require greater resources and may have its neutrality compromised.[88]

78 Law Commission, above n 5, at [3.24].
79 Privacy Act 1988 (Cth), sch 1 cl 1; GDPR, art 5(1)(a); and OECD Guidelines, cl 12.
80 Privacy Act 1988 (Cth), sch 1 cl 1; GDPR, recital 39; and Law Commission, above n 5, at [3.159].
81 Law Commission, above n 5, at [3.162].
82 (18 June 2019) 739 NZPD 12058; and GDPR, arts 20, 17, 13, 21 and 22.
83 Edwards, above n 33, at [2.1]–[2.9].
84 (30 July 2019) 739 NZPD 12735.
85 (18 June 2019) 739 NZPD 12058.
86 Law Commission, above n 5, at [6.35].
87 At [6.31]–[6.33].
88 At [6.36].

VI CONCLUSION

The 2020 Act implemented some much needed privacy reforms. Without such reforms, New Zealand's privacy law would still be a relic of the early 1990s, when the World Wide Web was in its infancy. The long and delayed process leading up to the 2020 Act meant that New Zealand lacked privacy protection measures that its trading partners had. These included clear provisions applying to overseas agencies carrying on business in New Zealand, restrictions on the disclosure of personal information overseas, a breach notification system, a compliance notice procedure and certain criminal offences. New Zealand was in danger of losing its adequacy status under the GDPR, which affects international data flows and trade.

The 2020 Act is not fully aligned with international privacy instruments and the privacy laws of New Zealand's trading partners. The pressing need to pass the Bill compromised consideration of some significant features that appear in the OECD Guidelines, the Privacy Act 1988 (Cth) and the GDPR. As it stands, the 2020 Act may be criticised for lacking teeth, as it does not incorporate civil penalties for non-compliance, and for lacking rights that are increasingly important in the digital economy (where data is currency). Questions will continue to be raised about the adequacy of the 2020 Act to deal with developments in technology, despite hopes that the 2020 Act's technology-neutral IPPs will stay relevant. Further and ongoing work on privacy reforms is needed to bring *and keep* New Zealand up to date with international privacy instruments, the privacy laws of New Zealand's trading partners and technological developments.