New Zealand: Is the Privacy Bill out of step with global privacy law reform?

New Zealand's Justice Select Committee ('the Committee') published its report ('the Report') on the Privacy Bill ('the Bill'), on 14 March 2019. Frith Tweedie and Grace Abbott, of EY Law, provide commentary on the Committee's recommendations and clarifications in the Report, and ask whether they go far enough to keep up with global privacy law reform and ensure that New Zealand retains its EU adequacy status.

A higher threshold for notification of privacy breaches, clarification of the application of the Bill to offshore giants like Facebook and Google, and clearer rules on the use of service providers. Those are some of the recommendations made by the Committee in the Report on the Bill. First introduced into the House on 20 March 2018 by Justice Minister Andrew Little, the Bill is the first major reform of New Zealand's privacy law in 25 years. It aims to better align New Zealand's privacy law with international developments such as the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), as well as recent changes to Australian privacy law.

While the Committee made some helpful recommendations to amend and clarify aspects of the Bill, it still leaves New Zealand out of step with the GDPR and other laws with which it purports to align itself. Notably absent are meaningful civil penalties for non-compliance, rights of deletion and data portability, and requirements in relation to automated decision-making and profiling, Privacy by Design, Privacy Impact Assessments and unambiguous consent.
Is New Zealand at risk then of losing its coveted EU adequacy status? The European Commission's adequacy ruling in December 2012 enabled the unrestricted transfer of European data for New Zealand organisations, giving New Zealand a competitive trade advantage, but if New Zealand's privacy laws are seen to have fallen behind international standards, formal EU recognition that its privacy laws meet EU standards may be withdrawn.

There is a notable lack of real and meaningful consequences for non-compliance. The Office of the Privacy Commissioner of New Zealand ('OPCNZ') previously recommended fines of up to NZD 1 million (approx. €588,240) for organisations who seriously breach their privacy obligations, but the maximum fine on conviction for an offence under the Bill remains at NZD 10,000 (approx. €5,880), in stark contrast to the GDPR's maximum civil penalties of up to €20 million or 4% of global annual turnover, whichever is greater. Similarly, the Australian Government recently indicated that it will increase maximum fines for serious or repeated privacy law breaches from AUD 2.1 million (approx. €1,314,040) to whichever is the greater of AUD $10 million (approx €6,257,350), 10% of the organisation's annual Australian turnover, or three times the value of any benefit obtained through misuse of personal information.

**Key recommendations from the Report**

**Higher threshold for breach notification**

The Committee's recommendations on introducing a new threshold of 'serious harm' will help align New Zealand's approach to breach notification requirements with those of Australia and other key trading partners.

The original wording of the Bill only required breach notification to the OPCNZ and affected individuals where it caused or was likely to cause 'harm.' The Committee agreed with the many submissions by arguing the threshold was too low, risking over notification of minor breaches and 'notification fatigue.' The Report recommends a new threshold of 'serious harm,' which means a 'notifiable privacy breach' will be one where it is reasonable to believe that the breach has caused, or is likely to cause, serious harm to affected individuals. The Report additionally recommended certain considerations to help assess whether a privacy breach is likely to cause 'serious harm'.

Failure to notify a notifiable breach of privacy will be an offence under the Bill, making an 'agency' (that is, any person or private or public-sector entity subject to the Bill) liable for a maximum penalty on conviction of NZD 10,000.

**Clarity on use of service providers**

The Committee recommends various changes relevant to the increasingly commonplace use by New Zealand organisations of third parties like cloud service providers ('CSPs') for the storage and processing of personal information.

**Agencies remain liable for personal information stored in the cloud**

Under the recommended changes, an agency would remain accountable for personal information stored or held by a CSP or similar service provider on its behalf, whether the service provider is based in New Zealand or overseas.

Those changes clarify the slightly opaque approach in the current drafting. It is now clear that where a New Zealand agency uses, for example, a CSP to store the agency's customer and employee personal information, then that information will be treated under the Bill as still being held by that agency, who will remain responsible for it and liable for any privacy breach caused by the CSP.

It is worth noting that this will only be the case if the service provider does nothing more than store or process the personal information as an agent. If the service provider uses or discloses that information for its own purposes, then under the recommended changes it will be considered to ‘hold’ that information as well as the primary agency, making it also accountable to affected individuals.

Whilst the Committee's recommendations are an improvement, the Bill still doesn't clarify exactly what it means for an organisation to hold information 'for its own purposes.' Arguably, GDPR-style distinctions between 'data controllers' and 'data processors' could have provided greater certainty to agencies entering into increasingly complex, multi-jurisdictional and multi-party data processing arrangements.

**Harder to disclose personal information to foreign entities**

Where the service provider is not using the information for its own purposes (that is, an agency relationship exists), data transferred between the two entities will not be classed as 'use' or 'disclosure' for the purposes of the Bill. This is important to note, because it means that new rules limiting the ability to transfer personal information to a ‘foreign person or entity’ will not apply. This has the practical result of making it easier for New Zealand agencies to store their data in the cloud and provides greater legal certainty around use of CSPs.

Where the service provider is offshore and cannot be considered an agent, then disclosure to such a 'foreign person or entity' would only be permitted in certain circumstances under the updated Information Privacy Principle ('IPP') 12 under the Bill, namely:

- If the individuals concerned ‘authorise’ the disclosure after being ‘expressly informed’ that the foreign entity may not be required to protect the information in a way that provides comparable safeguards to those in the Bill. The use of 'expressly informed' suggests that a privacy policy would not be an appropriate place to inform and obtain such authorisation and that something more is required, for example, a direct communication to affected individuals.
- The foreign entity carries on business in New Zealand and the New Zealand agency ‘believes on reasonable grounds’ that the foreign entity is subject to the Bill.
- The foreign entity is subject to privacy laws that provide comparable safeguards to those in the Bill. We note it is currently unclear exactly what would constitute ‘comparable safeguards’ or the key areas of comparison, but the Committee has suggested that the OPCNZ should provide guidance on this point.
- The foreign entity is in a ‘prescribed binding scheme,’ is subject to the privacy laws of a ‘prescribed country’ as specified in regulations made pursuant to the Bill, or otherwise is required to protect the information in a way that, overall, provides comparable safeguards to those in the Bill. The last aspect could be achieved by way of a contract between the parties.

**Agencies must notify individuals about a privacy breach**

If an agency outsources its data storage or processing to a CSP or similar service provider, the Committee recommends that the agency should remain responsible for informing individuals of a notifiable privacy breach, regardless of who actually caused the breach. This is because the primary agency will have the relationship with the individuals affected by a privacy breach. The Committee has said affected individuals should not be disadvantaged by an agency's decision to use service providers.
As a result, the Committee considers that 'it is appropriate' for agencies to have agreement with their service providers specifically addressing the handling of personal information. This is analogous to the GDPR requirements for data processing agreements between data controllers and data processors. The Committee recommends inserting a new Clause 122A to 'encourage' contractual provisions, which would set out when a service provider must notify the agency about a privacy breach.

While the proposed drafting does not make such agreements mandatory, prudent agencies will want to make sure appropriate provisions are included in their service provider contracts to ensure they are notified as soon as possible after a breach occurs. That will enable them to take the necessary steps, as quickly as possible, to contain and manage the breach and the notification process.

**The Bill could apply to foreign companies too**

The Committee recommended changes to the Bill to clarify its application to offshore companies that carry on business in New Zealand, regardless of whether they have a bricks-and-mortar presence in New Zealand.

Those changes appear to be directed at large digital multinationals, who have previously run afoul of the Commissioner and others by arguing that they do not have to comply with New Zealand laws, including in relation to privacy. In May 2018, Facebook refused to co-operate with an investigation by the OPCNZ after it held that Facebook had breached the Privacy Act 1993. At the time, the OPNZ stated that "[i]f any organisation demonstrated an unwillingness to follow the orders of New Zealand's courts, that would be of considerable concern to the judiciary and Parliament."

Google declined to comply with New Zealand court-mandated suppression orders in May 2018, claiming that while Google New Zealand is bound by New Zealand laws, Google LLC (which runs its search engine) is not, because it is domiciled in the US.

The recommended changes are that the Bill will apply to an 'overseas agency' in relation to any action taken, and all personal information collected or held by that agency 'in the course of carrying on business in New Zealand,' regardless of where the information is collected or held. An agency will be treated as 'carrying on business in New Zealand' whether or not it has a physical place of business in New Zealand, any monetary payment is made for the supply of its goods or services, or it intends to make a profit from its business there.

This is a welcome development which addresses the borderless nature of the global digital economy. However, greater clarity, such as that which exists under the GDPR, on exactly who is subject and in what circumstances, would have been helpful. The Bill still doesn't provide clarity on the meaning of 'carrying on business,' and it remains to be seen whether case law in a non-privacy context will be relevant here.

**Data minimisation (of sorts)**

The Committee recommends inserting a further rule that agencies cannot require an individual's 'identifying information' if it is not necessary for the lawful purpose for which it is collected. The Committee has said that it wishes to discourage agencies collecting personal identifiers by default without considering whether it is necessary to do so.

While a laudable concept, the addition of that requirement may not in fact add much given the existing wording of IPP 1 already states that an agency can only collect personal information 'necessary' for a lawful purpose. We note the potential confusion introduced by the expression 'identifying information,' which is not defined but appears to be different from 'personal...
information.’ However, the recommended change does signal the importance of data minimisation, which is particularly relevant while many New Zealand organisations continue to try and amass as much data as they can in case it might prove useful later.

**OPCNZ and Human Rights Review Tribunal powers**

The OPCNZ’s key powers remain limited to issuing compliance orders and determinations when a person has requested access to personal information and been refused and providing guidance to agencies. It also has a general discretion to not investigate a complaint.

The Committee recommends giving the Human Rights Review Tribunal (‘the Tribunal’) an express power to hold closed hearings in certain circumstances, and the Chair of the Tribunal the ability to make decisions without having to convene a three-person tribunal. This may help tackle the backlog of work currently faced by the Tribunal and free up capacity.

**Unique identifiers**

Agencies must take all reasonable steps to minimise the risks of misuse of a unique identifier before disclosing it to another agency. This is aimed at unique identifiers like customer numbers and is designed to reduce identity theft.

**Stronger protections for children**

The Committee recommended that organisations be required to take into account the vulnerability of children when collecting their personal information.

**What happens now?**

The Bill is now scheduled to take effect from 1 March 2020, later than the July 2019 date originally proposed. It will progress in its second and third readings, with further changes still possible. While there have been no firm indications to date that members of Parliament have any appetite to push for significant changes to the Bill, it’s possible the debate surrounding the role of social media platforms, in the wake of the Christchurch terrorist attack, could stir political appetite to better align with international privacy regulation. Watch this space.

**Frith Tweedie** Digital Law Leader  
frith.tweedie@nz.ey.com  
**Grace Abbott** Senior Solicitor  
grace.abbott@nz.ey.com  
EY Law, Auckland

The views expressed in this article are the views of the author, not EY Law Limited. This article provides general information, does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information.

1. Available at: https://www.parliament.nz/resource/en-NZ/SCR_85172/cf492b3e12e7bcbb2b5ddf9fd9a5c287a5c79e2c  
4. See Clause 117(1) and proposed Clause 117A of the Bill.
5. Ibid, Clause 8.
6. Ibid, Clauses 8(2) and (3).
7. Ibid, Clause 8(5).
8. Ibid, Clause 14(1)(ca).