TCF Submission on the New Zealand Privacy Bill

May 2018

Introduction

This submission is made by the New Zealand Telecommunications Forum (TCF) in relation to the proposed New Zealand Privacy Bill (the Bill). The proposed changes to New Zealand privacy legislation are generally fit for purpose but need to be considered in the international context in which New Zealand operates.

The TCF is the telecommunications sector's industry body and has a vital role in bringing together the telecommunications industry and key stakeholders to resolve regulatory, technical and policy issues for the benefit of the sector and consumers. Its members represent 95% of the sector; 2degrees, AWACS, Chorus, DTS, Enable Networks, Kordia, Northpower, NOW NZ, Spark, Symbio Networks, Trustpower, Ultrafast Fibre, Vector, Vocus and Vodafone.

The TCF proposes four amendments:

- Increasing the threshold for breach reporting to prevent excessive and unnecessary reporting. Excessive reporting creates consumer fatigue and consumers failing to identify the reports they need to act upon.
- A mandatory review of New Zealand privacy legislation against the European Union (EU) General Data Protection Regulation (GDPR) within the next two years and the legislation consequently updated to ensure New Zealand retains its EU adequacy status.
- Tighter obligations and timeframes for the publication of prescribed country white lists and a period of three years to renegotiate contracts where appropriate.
- Clarify the approach to dealing with consumer information requests relating to whether a warrant has been served on the private sector agency by a public sector agency.

These amendments will facilitate efficient operation of New Zealand businesses without adversely impacting the privacy rights of New Zealanders. Amendments to the breach reporting provisions would also benefit consumers by ensuring they are not overwhelmed by notifications about inconsequential data events.

Breach Reporting

The current threshold for triggering privacy breach reporting in the Bill is too low. This effectively means that privacy breaches must be reported no matter how minor or insignificant. The risk of this

approach, combined with a broad definition of privacy breaches, is that consumers could receive so many breach notifications that they simply ignore them, even where the breach is significant.

Both the EU GDPR and the Australian legislation have higher thresholds for reporting. For example, in Australia the obligation to report applies only to breaches which are reasonably likely to result in serious harm and additional exemptions are included if an agency is able to prevent serious harm through remedial action. The Bill's criteria is too wide, requiring reporting as long as 'there is a risk' of certain types of harm and without these additional exemptions.

We request that an approach along the lines of the Australian legislation is adopted. This would mean changing the standard from harm to "serious harm", moving from "there is a risk of" to "there is reasonably likely to be" serious harm, and including a secondary condition or exemption that the entity has not been able to take steps to prevent that harm.

Mandatory review of New Zealand Privacy Legislation to ensure New Zealand will retain its EU adequacy status

In our increasingly connected world, overseas organisations can transfer data and content for hosting and processing in New Zealand, and this is hugely beneficial for New Zealand businesses. New Zealand has been recognised by the EU as having adequate data protection and has consequently been given the status of "EU adequacy". Our EU adequacy status is an important recognition, and if New Zealand were to lose this status we would likely see a reduction in overseas organisations using New Zealand companies to assist them with data storage and processing.

It is vital for international competitiveness that New Zealand retains its EU adequacy status. The EU GDPR has resulted in some significant changes to the EU data protection framework and our domestic legislation needs to ensure it remains consistent in the key areas required to retain our status.

We recommend that the Bill requires a review of New Zealand legislation within two years to ensure that it remains fit for purpose, and any necessary changes to maintain EU adequacy are made before our EU adequacy is next up for review. If we do nothing, the TCF is concerned that New Zealand's EU adequacy status will be lost which will significantly disadvantage New Zealand businesses.

Transfer of data overseas - prescribed countries and transition period

Similar to the EU adequacy point above, New Zealand companies need certainty of which countries they can do business with directly, and which require additional contractual protections to meet New Zealand Privacy Law. The prescribed country white list plays an important role in this.

This list will need to be reviewed when our domestic legislation changes, introducing an element of uncertainty over which countries will appear on the list of prescribed countries. We request that the power to specify the countries on the white list be given directly to the Privacy Commissioner rather than being made via regulations. This could be made following a consultation process, but without the need for regulations and would enable the prescribed country white list to be created and updated more quickly over time.

We support the option for appropriate safeguards to be put in place that reflect New Zealand Privacy Law, including via contractual means. In addition to this, it may be helpful for the Privacy Commissioner to have the power to specify contractual clauses that would be sufficient for parties transferring data overseas to reflect New Zealand law requirements. Having this as an additional option would not prevent agencies taking an alternative approach based on the primary provision,

but may assist smaller New Zealand organisations by providing certainty about a clear way of ensuring compliance.

We request greater commitment on the timeframe for updating the prescribed country white list. We also request that where a country is removed from a white list that companies are given a grace period of three years to renegotiate contracts with their partners in these countries as this may require comprehensive contract reviews to reflect the New Zealand privacy regime, and in some cases may conceivably require termination of relationships.

We also seek a three year transition period for the overseas data transfer provisions to enable agencies to implement arrangements, and for the first white list to be available within six months of the Act coming into force.

Content of breach notification notices

Clause 121(a) states that a notification to an affected individual must advise whether or not the agency has identified any person or body that the agency suspects may be in possession of the affected individuals' personal information – but also prohibits agencies from including any particulars that could identify that person or body. This potentially creates a problem where the identity of the person who has accessed or been provided with the information is relevant to the steps that the individual needs to take to mitigate the breach.

For example, in the event a rogue employee accesses some information about their ex-partner. We can tell the victim that there has been a breach but we are prevented from telling the victim who accessed it. In this case it may help the victim to take steps to protect their safety or the safety of others by letting the victim know it was their ex-partner who obtained access to the victim's information.

The Australian Privacy Commissioner Notification Guidelines specifically envisage that it may be appropriate to share the identity of the accessor where it would be relevant to the steps that individuals would need to take in response to the breach. The TCF submits that it would be useful to allow similar provisions in the Bill.

Reporting on Public Agency Warrants

TCF Members are occasionally asked by individuals to confirm whether a public agency has made any requests (e.g. via a production order) about them. This places the private sector agency in a difficult position as it does not have sufficient information to assess whether any of the potentially applicable exceptions under clauses 54 and 57 apply. Even advising an individual that there have not been any information requests may impact matters addressed under clauses 54 and 57. The public sector agency(s) concerned are best placed to consider whether the relevant exceptions apply, and this sets up a complex, and time consuming process between the private and public sector agencies. The customer's request could be better addressed in a more timely fashion if it were redirected to the public sector agency in the first instance.

We therefore request that;

- private sector agencies are not required to answer personal information requests concerning public agency information requests, production orders and warrants and, if they do receive a request from an individual, they can respond to the individual by directing them to send their request to the public sector agency(s) they believe is most appropriate to answer their query instead; and,

- when a public sector agency makes any form of request to private sector agencies for information about an individual or organisation, they are required to advise whether or not the private sector is prohibited from advising the individual / organisation to whom the request relates. (This would enable New Zealand agencies to progress transparency reporting practices).

Conclusion

The TCF considers that the proposed changes to the New Zealand privacy legislation are generally fit for purpose. However, the changes need to be considered in the international context in which New Zealand operates, particularly with respect to the EU adequacy status that New Zealand currently enjoys. Additional changes to the criteria for reporting breaches would enhance the effectiveness of these provisions.

Finally, it should not be left to private sector businesses to decide matters of National Security when asked for information about information requests and production orders. It should be public sector agencies which are able to exercise the power to requisition private information, to determine the appropriate response to individuals seeking information about whether they are the subject of such orders.

The TCF would like to appear in person to present its submission to the Select Committee.

Yours sincerely,

Geoff Thorn

Chief Executive Officer

New Zealand Telecommunications Forum (TCF)