Supplement to
December 2015 Periodic Update Report
On
Developments in Data Protection Law
In New Zealand

(2013-2015)

_____

Report to the European Commission

by the competent supervisory authority

for the application of the legal data protection standards

in New Zealand

2 March 2016

_____

Privacy Commissioner
Te Mana Matapono Matatapu
New Zealand

Table of Contents

Bruno Gencarrelli
Head of Unit - Data Protection European Commission
Directorate-General for Justice
Brussels
Belgium

Dear Bruno

Supplement to December 2015 update report on developments in New Zealand data protection law

I refer to Ralf Sauer's message of 19 January 2016.

I record your confirmation that the format adopted for the first report, and the proposed six-monthly frequency of further updates, serves the Commission's purposes well bearing in mind the opportunity to ask further questions as required.

The December 2015 report invited the European Commission to contact my office if it required further information on any aspect of the report. I am pleased to supply this response to questions posed by Ralf Sauer on your behalf. I have prepared the material by way of a supplementary report so that the answers may be kept alongside the original report for purposes of completeness, transparency and accountability.

Yours sincerely

John Edwards
New Zealand Privacy Commissioner

2 March 2016

1. Background

On 19 December 2012 The European Commission (EC) formally decided that for the purposes of Article 25(2) of the Directive 95/46/EC (the EU Data Protection Directive), New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the European Union.

The EC has a responsibility to monitor the functioning of the decision. To assist the EC to undertake this monitoring, the New Zealand Privacy Commissioner as 'the competent supervisory authority for the application of the legal data protection standards in New Zealand' has undertaken periodically to submit update reports on developments in New Zealand data protection law.

On 22 December 2015 the NZ Privacy Commissioner submitted the first report that briefly surveyed developments since the commencement of the EC decision in 2013.[1] The EC acknowledged receipt of the report and, by email of 19 January 2016, sought clarification on several points.

The original report and this supplement are submitted in the Privacy Commissioner's capacity as the independent supervisory authority with competence under Article 1(2) of the decision. It is understood by the EC that the Privacy Commissioner does not purport to speak for the New Zealand Government.

[1] The report is available at: https://privacy.org.nz/assets/Files/International-APPA-APEC/Report-on-NZ-Adequacy-to-EC-December-2015.pdf.

2. Government Communications Security Bureau Amendment Act 2013

You acknowledge the enactment of the GCSB Amendment Act 2013 as a positive development. You also enquire how the concept of "reasonableness" is interpreted in practice (e.g., in those places where it is stated that the Bureau must not collect personal information unless "the collection of the information is reasonably necessary" for a lawful purpose, or that the Bureau must do "everything reasonably within" its powers to prevent unauthorised use or disclosure).

It would be premature to provide any but the most general answer to that question at this stage. The GCSB policy to give effect to the Amendment Act has not yet been promulgated although, as mentioned in the update report, the GCSB has commenced work to formulate the required policies on personal information. The GCSB is required to consult with with both the Inspector-General of Intelligence and Security and the Privacy Commissioner in formulating that policy. I expect that a clearer answer to your question could be offered when that work is complete perhaps by the time of the next periodic report.

3. The "serious threat" exception to the Privacy Principles

You refer to the widening of the "serious threat" exception to the information privacy principles which relies upon the "reasonable" belief of agencies that certain events will happen in the future, without these being imminent. You would like to understand better the limits to such an assessment.

The precise ambit of the exception has been widened and thus this exception can rightly be characterised as a weakening of privacy protections for one set of individuals. However, the justification for the exception, and the widening of the exception, is based upon the perceived impact on the safety of other individuals and so easily fits within the usual framework of a human rights or privacy law whereby competing rights are set against each other and reconciled in a way that maintains fundamental values as far as possible.

The New Zealand Parliament altered the standard only after 20 years of experience of the exception in its original form and after taking expert law reform advice from the Law Commission. The concern essentially arose from cases where the existence of a threat appeared readily to be able to be identified but the time at when that threat would be manifest could not be so readily anticipated. The perception was that the exception in its more restrictive form inhibited the exercise of discretionary disclosure as a precautionary measure to contain threats. The Law Commission took the view that the exception could be recast in such a way that the fundamental rights and values remained preserved while allowing greater flexibility to make pre-emptive disclosure to address a threat.

The Law Commission explained their recommendation as follows[2]:

> *We proposed in the issues paper that the word "imminent" should be deleted from these exceptions. The ALRC [Australian Law Reform Commission] has recommended the deletion of "imminent" from equivalent exceptions in the Privacy Act 1988 [Commonwealth of Australia], and this recommendation has been reflected in … a new set of Australian Privacy Principles. In the issues paper we noted the following arguments in favour of deleting "imminent":*
>
> - *Sometimes a threat will be serious, but the harm may not eventuate for some time. For example, the disclosure of genetic information to an individual's relatives could relate to a genetic condition that has very serious consequences, but may not show up for many years.*

[2] New Zealand Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (R123), para 3.119 ff.

- *An assessment of whether or not a threat is "serious" necessarily involves consideration of the likelihood of a particular outcome, as well as the possible consequences of the outcome.*
- *An agency wishing to rely on the exception would still need to have reasonable grounds for believing that the use or disclosure is necessary to prevent or lessen the threat, not merely that it is convenient or desirable.*

Submissions were overwhelmingly in favour of the proposed amendment. Submitters gave various examples of situations in which the deletion of the requirement that the threat be imminent would allow for the sharing of information about serious threats to health or safety. These included examples relating to child neglect, disease, risk of self-harm, and the disclosure of information about New Zealanders travelling overseas who are in situations of serious but not necessarily imminent danger. … In addition, coroners have, from time to time, forwarded to the Law Commission coroners' findings in which failure to disclose information because a threat was not seen as being imminent is considered by the coroner to have contributed to a death.

…

For the reasons given above, we recommend that "imminent" should be deleted from the health and safety exceptions to principles 10 and 11. We consider that the concerns raised by some submitters can be addressed by spelling out in the Act the elements that must be taken into account in assessing whether or not a threat is "serious". These elements are:

- *Likelihood – is it highly probable that the threat will eventuate?*
- *Consequences – is the threat likely to cause a significant level of harm if it eventuates?*
- *Imminence – is the threat likely to eventuate soon?*

An agency would not need to believe that all three of these elements are present before it could rely on the exception, but it would need to consider each element in making its assessment. We recommend that these criteria for assessing the seriousness of a threat to health or safety should be spelled out in the Act, and should apply not only to the exceptions to principles 10 and 11 …. This recommendation means that agencies will still need to consider the imminence of a threat, but will not be precluded from relying on the exception where disclosure is necessary to deal with a threat that is not imminent but is likely and potentially serious in its consequences.

There have not yet been any cases before our Human Rights Review Tribunal offering definitive interpretative guidance on the change to the provisions.

4. Data sharing agreements between authorities

You refer to the new statutory arrangements for information sharing agreements as possibly weakening privacy protections as the new law "authorizes exemptions from or modifications to information privacy principles". You would like to understand better what these exemptions/ modifications entail.

My first comment is that the framework itself should probably not be seen as representing a weakening of privacy protections – although that might possibly happen in a particular case. Rather the framework now set out in Part 9A of the Privacy Act should be viewed as an alternative process for authorising particular programmes of information sharing for governmental purposes that is accompanied by enhanced arrangements for scrutiny, regulation and review that might not be present for other processes of authorisation (such as the use of enactments that override the privacy principles). With those accompanying arrangements the outcome for Part 9A information sharing agreements might in some cases be an enhancement of privacy protections rather than their weakening.

Part 9A is quite a lengthy part of the Privacy Act – running to 26 sections and 16 pages of statute – so it would not be appropriate to describe it in detail here. My Office has created a new section of its website devoted to Part 9 information sharing which I expect will help explain its objectives and operation.[3] The Ministry of Justice has also posted materials on the human rights part of its website.[4] Both those sources describe the processes and safeguards.

You signal a particular interest in the fact that authorised information sharing agreements (AISAs) authorize exemptions from or modifications to information privacy principles. This can be explained by the fact that the AISAs are approved by the Governor-General by Order in Council and thus have the status of regulations.[5] The Privacy Act has always provided that other enactments, including regulations, will prevail over the information privacy principles[6] and thus this aspect cannot really be seen as a weakening of privacy protections but a continuation of the constitutional balance struck in 1993.

[3] See https://privacy.org.nz/information-sharing/information-sharing-introduction/ and linked pages.
[4] See http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/domestic-human-rights-protection/privacy-act-1993/approved-information-sharing-agreements/approved-information-sharing-agreements-aisa.
[5] See Privacy Act 1993, ss. 96J-96M.
[6] Privacy Act 1993, s.7 refers.

5. Further information

Further information about any aspect of this report may be requested from Blair Stewart, Assistant Commissioner (Auckland), Office of the Privacy Commissioner at blair.stewart@privacy.org.nz.