From: NZSIS Legal Adviser [redacted]
Sent: Thursday, 29 October 2020 4:21 pm
To: Privacy Code
Subject: NZSIS Submissions on replacement Privacy Codes

UNCLASSIFIED

Kia ora,

Thank you for your emails inquiring about classification and publication of the NZSIS submissions on the replacement Privacy Codes consulted on earlier this year. Please find below an unclassified copy of all of the NZSIS submissions on replacement Privacy codes.

Health Information Privacy Code

NZSIS has several comments on the proposed new Codes. This email contains our submissions on the Health Information Privacy Code. We note that the Privacy Commissioner's updates are not intended to enact policy changes aside from those implemented in the Privacy Act 2020. However, we suggest this is an opportunity for some minor updating amendments.

ISA exceptions ought to be incorporated into Codes

NZSIS's main general submission on the Codes is that it would be useful if the exceptions relating to intelligence and security agencies set out in the Privacy Acts (1993 and 2020), implemented by the Intelligence and Security Act 2017, were carried over into the Codes. While the Codes relate to information that is not at the centre of intelligence and security agencies' functions, the Codes do apply to the agencies at times – the Health Information Privacy Code, for example, applies to information collected by NZSIS in-house psychologists.

Application of Code could be clearer

In addition, NZSIS considers it would be useful if the Health Information Privacy Code specified the extent to which it applies to in-house health professionals who provide advice to organisations. The December 2008 Health Information Privacy Code contains commentary that "the code does not apply to employee information" and independent commentary (*Mental Health in New Zealand* [41.15.2.5]) notes that:

> However, not all health information that may be collected about an individual is necessarily protected by the Health Information Privacy Code 1994. Where a request for health information about an employee is initiated by an employer, for example, for the purposes of addressing the safety of a particular employee, such an evaluation does not allow for a doctor-patient relationship between an employee and the evaluating psychiatrist. Since the evaluator is effectively an employee of the company, standard laws regarding confidentiality do not apply.

NZSIS considers the position is not entirely clear, given rule (4)(2) provides that the Code applies to, among others, "a larger agency, a division or administrative unit (including an individual) which provides health or disability services to employees of the agency or some other limited class of persons". A clearer statement of the application of the Health Information Privacy Code would be useful.

Specific questions addressed

NZSIS agrees with the Privacy Commissioner that the existing rule 2(2)(c)(i) means that new IPP 2(2)(e)(v) does not need to be added to rule 2, as the current rule is broader than the new IPP. NZSIS does consider that it would be beneficial for the Code to expressly refer to s 30 of the new Act to ensure it is clear that those provisions apply, even though it has been removed from IPP 2.

We are happy to discuss our above comments in more detail should that be useful.

Credit Reporting Privacy Code

Thank you for the opportunity to comment on the proposed new Privacy Codes. This email contains the NZSIS submission in relation to the Credit Reporting Privacy Code. We note that the Privacy Commissioner's updates are not intended to enact policy changes aside from those implemented in the Privacy Act 2020. However we suggest this is an opportunity for some minor updating amendments.

Background

The functions of the NZSIS are to collect and analysis intelligence and to provide security services advice and assistance. These functions are set out in sections 10 and 11 if the Intelligence and Security Act 2017 **(the ISA)** respectively. Both these functions involve the collection of information from other government agencies as well as private third parties. Rule 11 of the Privacy Code differentiates between these two types of information collection activities.

NZSIS has statutory obligations of confidentiality under the ISA and robust internal policies concerning the retention and use of collected information. These obligations relate to both the collection of intelligence information as well as the provision of protective security services and advice.

In addition the ISA authorizes the Office of the Inspector General and Security (**the IGIS)** , an independent statutory body, to supervise the activities of the NZSIS. This includes any collection and retention of information by the NZSIS from any third party.

Amendment to Rule 11 of the Privacy Code

Rule 11(1)(d) currently permits a credit reporter to release information to an intelligence and security agency only when it is necessary to perform any of its functions, **other than the performance of a security clearance assessment**

(Emphasis added)

NZSIS submits that this rule should be amended to omit the phrase "other than the performance of a security clearance assessment". This is because the ISA obligations of confidentiality, as well as the IGIS oversight, applies to all functions (both section 10 and 11 of the ISA) which the NZSIS undertakes.

Amendment to Schedule 4 of the Privacy Code

Schedule 4 of the Privacy Code states that an intelligence and security agency must cooperate with all reasonable compliance checks and systematic reviews from the credit reporter. Although the Privacy Code deals with requests by NZSIS for information from a private third party, they have the potential to undermine the secrecy obligations set out in the ISA. As stated above, NZSIS has in place robust internal policies and is subject to rigorous oversight from the IGIS. This additional requirement is unnecessary and in many instances is unworkable

We would appreciate the opportunity to discuss these proposed changes with your office in more detail.

Telecommunications Information Privacy Code

Noting your advice that submissions might be made public or released under the OIA, it would be appreciated if you could please consider the implications for national security of disclosure of these submissions.

Subrule 2(2)(e)(iv): Serious threat to life/health or public health and public safety or prejudice the safety of any individual

It would be useful if consideration could be given to amending subrule 2(2)(e)(iv) with the wording used in the Health Information Privacy Code: instead of referring to non-compliance being necessary to "prevent or lessen a serious threat to the life or health of the individual concerned or any other individual," compliance would "prejudice the safety of any individual." While the current wording reflects IPP2(2)(e)(v), the HIPC wording proposed would also better suit the national security context in which telecommunications information sometimes needs to be collected. The proposed wording is broader than IPP 2(2)(e)(v) and will therefore capture the circumstances of the currently drafted provision (as with the HIPC). Alternatively, a reference instead to public health and public safety would reflect the language in IPP11(1)(f)Ii).

A similar amendment is not required for subrule 3(4) because national security circumstances are likely to be adequately provided for by subrule 3(4)(d) (compliance is not reasonably practicable in the circumstances of the particular case).

Rule 11: Limits on disclosure of telecommunications information

It would be helpful to revisit the New Zealand Intelligence Community's (NZIC) position expressed during consultation on the 2017 amendments to the Codes. We note the revision of the Code is not a platform for policy changes: this request supports consistent application of the exemptions across the Codes, and is focused on providing certainty and transparency for users and the public about the way in which the Intelligence and Security Act 2017 (ISA), Privacy Act and the Privacy Codes interact. The relevant subrule is:

11(1) A telecommunications agency that holds telecommunications information must not disclose the information unless the agency believes, on reasonable grounds,-

…

(h) except where the disclosure of the information may be sought in accordance with a business records direction under Part 5(4) of the Intelligence and Security Act 2017, that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;

As the Code currently reads, NZSIS may seek a business record access direction (BRAD) to obtain information from telecommunications agencies. However, the BRAD regime relates only to business records, so where the criteria for a BRAD are not met, NZSIS can use other information collection provisions, including requests for the voluntary provision of information or the mechanisms under the ISA (for example, a request under s 122).

We recall at the time there was a view by some of the telecommunications agencies that intelligence and security agencies should be required to use compulsory information collection mechanisms provided under the Act, rather than voluntary avenues. The NZIC argued against this at the time. Without being sighted on the extent of their submissions on the new Privacy Act 2020, we think it's meaningful the Information Privacy Principle underpinning Rule 11 in the Code remains unchanged from the 1993 Act:

Information Privacy Principle 11
Limits on disclosure of personal information

(1) An agency that holds personal information must not disclose the information to any other agency or person unless the agency believes, on reasonable grounds:

…

(g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;

Given the underlying IPP has recently gone through a legislative review process, and been confirmed in its current wording, it seems appropriate and timely that the Code is updated to reflect the Privacy Act 2020. The inclusion of the BRAD regime is unhelpful because it creates uncertainty about the extent to which common law and the other information collection provisions in the ISA can be used.

Minor amendments

You may have already identified this error, but the definitions in clause 2 of "telecommunications agency" and "telecommunications information" refer to lists in subclause 4(2) and 4(1) respectively. This should be subclause 5(2) and 5(1) respectively.

Questions for submitters

We turn now to the specific questions asked in the consultation draft Telecommunications Information Privacy Code, and agree:

a. It would be helpful to explicitly state in clause 4 that terms used but not defined in the Code have the same meaning as the Act. This is particularly important for NZSIS in relation to the definitions of "serious threat."

b. With the way new IPP 12 has been implemented into the Code, noting with thanks, the transfer reflects (in subrule 12(1)) the omission of IPP11(1)(g) in IPP12, which is a key threshold for the limits of Rule 12 (and IPP12).

c. The application of Rule 13 should reflect section 26 of the Privacy Act 2020.

We would prefer express reference to section 30 of the Privacy Act 2020 be retained in specific rules in the Codes, to ensure it is clear those provisions apply to the Codes (this would be explicit mention in Rule 2, Rule 10 and Rule 11).

We are happy to discuss our submissions in more detail should that be useful.

Civil Defence National Emergencies (Information Sharing) Privacy Code

Noting your advice that submissions might be made public or released under the OIA, it would be appreciated if you could please consider the implications for national security of disclosure of these submissions.

The functions of intelligence and security agencies in support of declared national emergencies appear to come within the permitted purpose in clause 5(1) and clause 5(2)(d), being the government management of response, and coordination and management of the emergency. The ISA would first be applied to decisions to collect, use and share information, but it is useful in this time of COVID-19 to confirm the agencies have a role under the Code.

In relation to the specific questions asked in the consultation draft Civil Defence National Emergencies (Information Sharing) Code, we:

a. agree it would be helpful to explicitly state in clause 4 that terms used but not defined in the Code have the same meaning as the Act; and

b. do find proposed clauses 6(2) and (4) clearer than the corresponding clauses in the 2013 Code.

We are happy to discuss our submissions in more detail should that be useful.

Ngā mihi,

Senior Legal Adviser
New Zealand Security Intelligence Service | Te Pā Whakamarumaru

[redacted]
PO Box 12-209, Wellington 6144
www.nzsis.govt.nz

New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru
