9 March 2018

Attorney-General

Privacy Bill (PCO 18441 v 20.1)
Our Ref: ATT395/279

1. We have reviewed the Privacy Bill ("the Bill") and concluded it is consistent with the New Zealand Bill of Rights Act 1990 ("the Bill of Rights Act").

Introduction

2. The Bill repeals and replaces the Privacy Act 1993 ("the current Act"). Many of the provisions of the current Act are retained. New provisions respond to the Law Commission's review of the current Act and reflect and respond to technological developments impacting on the way personal information is handled by agencies. The Bill strengthens the role of the Privacy Commissioner through requiring mandatory reporting by agencies of privacy breaches and authorising the Commissioner to issue compliance notices in response to privacy breaches. It also enables the Commissioner to make decisions on complaints about access to information rather than referring these to the Human Rights Review Tribunal.

3. In concluding that the Bill is consistent with the Bill of Rights Act we have considered, in particular, its consistency with s 14 (freedom of expression), s 21 (freedom from unreasonable search and seizure) and s 25(c) the presumption of innocence.

Freedom of expression

4. Section 14 of the Bill of Rights Act provides that everyone has the right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind in any form. The right to freedom of expression has been interpreted as including the right not to be compelled to say certain things or to provide certain information.[1]

[1] *For example, Slaight Communications v Davidson* 59 DLR (4th) 416; *Wooley v Maynard* 430 US 705 (1977).

Proposed Part 3 Information Privacy Principle ("IPPs"), Public Register Privacy Principles ("PRPPs") and Codes of Practice

Part 3, subpart 1 - IPPs

5. The IPPs govern and limit the manner in which agencies may collect, store, use and disclose personal information. IPP 12 governs circumstances in which unique identifiers may be assigned and disclosed. Individuals collecting information solely for the purpose of, or in connection with, their personal or domestic affairs are exempt from complying with most aspects of the IPPs.[2] News media are exempt in relation to their news activities.[3]

6. IPP 11(3) prohibits an agency which holds personal information from disclosing it to an overseas person in reliance on various grounds contained in IPP 11 unless certain requirements are met. Broadly, the requirements are that privacy protections comparable to those contained in the Bill will apply, or the overseas person holds the information as agent for a New Zealand agency or the disclosure is authorised by the individual concerned.[4]

7. An individual may ask an agency holding their personal information to correct it. If an agency declines the individual is entitled to ask the agency to attach to personal information a statement of the correction sought. An agency must take such steps, if any, as are reasonable in the circumstances, to attach the statement of correction in such a manner that it will always be read with the information. The agency must also inform the individual of the steps taken to attach the statement or correction or that no steps have been taken. As far as reasonably practicable, the agency must inform every other agency to whom personal information has been disclosed of the correction made or statement of correction attached.[5]

8. The above limits on use of personal information and the manner in which it is held raise issues of prima facie inconsistency with s 14.

9. The purposes of the Privacy Act are:[6]

   9.1 To provide a framework that promotes and protects an individual's right to privacy of personal information, while respecting other rights and interests that may also need to be taken into account; and

   9.2 To give effect to internationally recognised privacy obligations and standards, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

10. The restrictions contained in the IPPs are rationally connected to the above purposes and protect individual privacy in a proportionate and balanced way. Agencies require personal information to carry out their business or provide services and in return have obligations regarding the manner in which they collect, hold, use and disclose it.

---

2 Proposed s 24

3 Proposed s 6, and exclusion (xii) from the definition of "agency."

4 Proposed IPP 11(3) and proposed s 8.

5 IPP 7 and proposed ss 69-70.

6 Proposed s 3.

11. We conclude that the framework implemented by the IPPs constitutes a justified limitation on s 14 of the Bill of Rights Act.

Part 3, subparts 2 and 3 - PRPPs and Codes of Practice

12. An agency administering a public register must, in administering the register, comply as far as reasonably practicable, with the IPPs and PRPPs.[7] The PRPPs are contained in proposed part 3, subpart 2 of the Bill. They govern search, use, transmission of and charging for personal information held on a public register.

13. Codes of practice are addressed in part 3, subpart 3 of the Bill. The Privacy Commissioner may issue a code of practice for specified information, agencies, activities or industries which modifies the application of the IPPs. The Commissioner may also issue a code which modifies the application of any of the IPPs or PRPPs to a public register, or prescribes how they are to be complied with or imposes requirements not prescribed by any PRPP.[8]

14. For similar reasons, our conclusion that the framework of the IPPs comprises a justified limitation on s 14 of the Bill of Rights Act applies equally to the PRPPs and to the authority for the Privacy Commissioner to issue codes of practice. In addition, when issuing codes of practice the Privacy Commissioner must act consistently with the Bill of Rights Act.[9]

Part 8 – power to prohibit transfer of personal information outside New Zealand

15. Part 8 of the Bill empowers the Privacy Commissioner to prohibit the transfer of personal information outside New Zealand in certain circumstances. An order prohibiting the transfer of information restricts the right to impart information and therefore raises a prima facie issue of compliance with s 14 of the Bill of Rights Act.

16. The Bill does not automatically restrict such a transfer but provides the Privacy Commissioner with a discretion to make prohibition orders. The Privacy Commissioner may make an order only if satisfied on reasonable grounds that:[10]

    16.1 the information has come from another State and is likely to be transferred to a third State where it would not be subject to comparable privacy safeguards to those in the Bill; and

    16.2 the transfer would be likely to lead to a contravention of the basic principles set out in Part 2 of the OECD Guidelines.

17. The Privacy Commissioner must also take into account other specified factors before making the order.[11]

18. The prohibition order is therefore available only in limited circumstances and is restricted by tight guidelines. Further, there is provision to apply for a variation or discharge of the order, and a right of appeal to the Human Rights Review Tribunal.

---

7 Proposed ss 21 and 31.

8 Proposed s 36.

9 Section 6 of the Bill of Rights Act and *Drew v Attorney-General* [2002] 1NZLR 58 (CA) at [68].

10 Proposed s 192.

11 Section 193.

19. Moreover, the discretionary power must be exercised consistently with the Bill of Rights Act.[12]

20. The prima facie restriction on the right to freedom of expression serves an important objective to which it is both rationally connected and proportionate. Accordingly, Part 8 is consistent with the Bill of Rights Act.

Section 118

21. Agencies are required to notify the Privacy Commissioner and, subject to exceptions, the affected individual, if they have suffered a notifiable privacy breach.[13] A notifiable privacy breach[14] is a privacy breach that has caused, or has a risk of causing, certain listed types of harm.[15] Agencies who fail to notify the Commissioner without reasonable excuse commit an offence.[16]

22. As previously noted, s 14 has been interpreted as including the right not to be compelled to provide information.

23. The Law Commission recommended mandatory notification of breaches for which notification would enable the recipient to take steps to mitigate risk of significant harm. For example, the affected individual may be able to take steps to mitigate and control the negative effects that could result from the breach.[17] Notification of the Commissioner would enable a statistical record to be compiled and identification of sectors where there are serious problems.[18] For example, the Commissioner might also be able to notify traders or bankers of possible criminal activity which has led to a security lapse.

24. The requirement to notify is rationally connected to the object of preventing harm to the individual and enabling the Privacy Commissioner to assist agencies to avoid future problems. It is proportionate, targeting only specified types of harm. We consider the requirement to be consistent with the Bill of Rights Act.

Search and Seizure

25. Section 21 of the Bill of Rights Act affirms that everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise. When Parliament gives an agency authority to demand, from another agency or person, information in which the subject of the information has a reasonable expectation of privacy, it creates a search power. The enactment creating that power will be consistent with s 21 of the Bill of Rights Act if the intrusion into privacy it authorises is justified by a sufficiently compelling public

---

12 Fn 9.

13 Sections 118 and 119 respectively.

14 Section 117 defines "privacy breach" in relation to personal information held by an agency as meaning, -

(i) the unauthorised or accidental access to, or disclosure , alteration, loss, or destruction of, that personal information; or

(ii)An action that prevents an agency itself from accessing that information or either a temporary or permanent basis;

Paragraph (b) of the definition of privacy breach explains either of the above applies whether caused by a person inside or outside the agency and whether or not it is attributable in whole or part to any action of the agency.

15 The types of harm are listed in s 75(2)(b).

16 Section 122.

17 Law Commission, *Review of the Privacy Act 1993 Review of the law of privacy stage 4* NZLC pp123, at [7.16] and recommendation 71.

18 Fn 16 at [7.9] and recommendation 71.

interest and the search power is accompanied by adequate safeguards to ensure it will not be exercised unreasonably.[19]

Section 21 - Provisions authorising the Privacy Commissioner to obtain information

26. The Bill continues provisions of the current Act which authorise the Privacy Commissioner to obtain information for investigative purposes. The Commissioner may summon and examine on oath a person who the Commissioner considers is able to give information relevant to an investigation. He or she may also require any person to provide information, documents or things in their possession that the Commissioner considers may be relevant to the investigation by a specified date or, if no date is specified, within 20 working days. The Commissioner may also exercise these powers when:

    26.1 deciding whether to issue a compliance notice;[20]

    26.2 assessing compliance of information matching programmes with specified requirements of the Bill and the information matching rules.[21]

27. Operation of the Act depends upon the Privacy Commissioner being able to investigate whether agencies have complied with its requirements. To do so the Commissioner needs information held by the person or agency being investigated. A person must respond within the designated time but may also request, on specified grounds, an extension of time to reply. The Commissioner must grant an extension of time if satisfied any of the grounds for doing so are established.[22] The privileges applying to witnesses in a court of law apply.[23]

28. We conclude that the Commissioner's powers are rationally connected to the purpose for which they are provided and proportionate. Accordingly, they are consistent with the right to be secure against unreasonable search and seizure.

Part 7, subpart 1 - Information sharing

29. Part 7, subpart 1 repeats, with some updating, the information sharing provisions of part 9A of the current Act. It provides for information sharing in accordance with authorised information sharing agreements to facilitate the provision of public services. A request for information about an individual made by one agency to another under an information sharing agreement arguably amounts to a "search" in terms of s 21.[24] Although information about an individual is provided from one

---

19 Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, Lexis Nexis, Wellington 2015): p 936 at [18.9.2] "In *Hamed v R,* Blanchard J, supported by the majority of the Supreme Court, clarified the steps undertaken in determining whether there has been a "search" in terms of s 21. First, search has its ordinary meaning but is informed by the underlying expectation of privacy protected by s 21. The person complaining of the breach must have subjectively had such an expectation, and that expectation must be one "that society is prepared to recognise as reasonable" (footnotes omitted).

20 Proposed s 129(2).

21 Proposed s 183(4).

22 Proposed s 92(5).

23 Proposed s 94.

24 The meaning of search is not settled. In particular, it is yet to be decided whether s 21 applies to non-law enforcement activities, see *The New Zealand Airline Pilots Association v Civil Aviation Authority* HC Wellington CIV-2011-485-954 13 July 2011 at [79] – [82]. The Crown position is that it does not. The Courts have accepted that a request for information about an individual from a third party can be a search for the purpose of s 21, at least where a search is authorised by statute or warrant: see for example *New Zealand Stock Exchange v Commissioner of Inland Revenue* [1992] 3 NZLR 1 at 6 (the Privy Council was "content to assume" that requesting information from the New Zealand Stock Exchange about

agency to another under an information sharing agreement no inconsistency with s 21 arises because the agreement authorised by the Governor-General in Council under proposed s 145 must be consistent with the Bill of Rights Act.[25]

Part 7 - subpart 2 - Identity information

30. Part 7, subpart 2 of the Bill repeats Part 10A of the current Act which governs access to identity information and provided improved information sharing between law enforcement agencies and Customs. Part 10A implemented recommendations of the Government Inquiry into Matters concerning the escape of Phillip John Smith/Traynor.[26] Identity information means any information that identifies an individual and includes biographical details, biometric information, a photograph, details of an individual's travel document or certificate of identity and details of any distinguishing features.

31. The term "biometric information" means:[27]

    31.1 1 or more of the following kinds of personal information:

        31.1.1 A photograph of all or any part of the person's head and shoulders:

        31.1.2 Impressions of the person's fingerprints:

        31.1.3 A scan of the person's irises; and

    31.2 An electronic record of the personal information[28] that is capable of being used for biometric matching.

32. Proposed s 165 authorises the nominated agencies to access an individual's identity information held by a holder agency for specified purposes set out in Schedule 4. The specified purposes are to verify identity when the agency is exercising specified law enforcement or border control functions. Proposed s 168 enables Schedule 4 to be amended by Order in Council by adding, omitting or amending any item.[29]

Assessment of part 7 - subpart 2

33. An individual has a reasonable expectation of privacy in biometric information,[30] but given the access arrangements to this information go no further than verifying

---

members was a search). In *R v Javid* [2007] NZCA 232 at [45(a)] it was accepted that the obtaining of confidential information from a telecommunications company (text messages) by the Police was properly seen as a search and seizure.

25 Fn 9.

26 The inquiry at p 15, recommendation 1 found that the "justice sector management systems and practices did not facilitate inter-operability sufficiently to support administration of justice and protect the public against risks, particularly those arising from confusion about criminal identities."

27 Proposed s 164.

28 Proposed s 6: "Personal information means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995) or any former Act …."

29 The amendments gave effect to the recommendations of the Government Inquiry into Matters concerning the escape of Philip John Smith/Traynor that there be a step change in justice sector information sharing with full inter-operability within and across sectors and a strategic focus among all government agencies on biometric identity information.

30 Fn 18 at 943 at [18.11.3] Butler and Butler note that taking fingerprints (which are biometric information) is covered by a search: "Searches and seizure are, equally, subject to [Bill of Rights Act] unreasonableness scrutiny. A "physical" search or seizure in this context means … the compulsory taking of impressions such as fingerprints, palm print, footprints; …"

identity, the expectation would be easily displaced where the state has a legitimate purpose in verifying identity, as it would when making a decision to arrest a person or prevent their entry into or departure from New Zealand.

34. Schedule 4 limits access to identity information (which includes biometric information) by confining access to those occasions where its purpose is to confirm identity for specified law enforcement and border control purposes. The access arrangements limit a person's ability to avoid law enforcement or border control by adopting a different identity document, using an alias or pretending to be someone else. They also eliminate the risk of a person with the same name and date of birth as a person of interest to the authorities from being wrongly apprehended. In these circumstances we consider that the access arrangements authorised by Schedule 4 do not infringe the right to be free from unreasonable search or seizure.

35. The potential amendment or replacement of Schedule 4 by Order in Council does not alter our assessment. The recommendation of the Minister is made after consultation with the Privacy Commissioner. The Order-in-Council itself must be consistent with the Bill of Rights Act.[31]

Part 7, subpart 3 – law enforcement information

36. Subpart 3 of the Bill authorises specified public sector agencies to have access to law enforcement information if that access is authorised by the provisions of Schedule 5.[32] The sharing of law enforcement information in the manner specified is rationally connected to the operation of the justice system and proportionate. We consider it is consistent with the right to be free from unreasonable search and seizure.

Part 7, subpart 4 – authorised information matching programmes

37. Under s 178 an agency may disclose information to another agency under an authorised information matching provision only in accordance with a written agreement between agencies that includes provisions reflecting, or no less onerous than, the information matching rules contained in schedule 7.

38. The information matching provisions which provide for the disclosure are located in other, agency specific, legislation. The information matching agreements entered into by agencies and governing the disclosure must be consistent with the Bill of Rights Act..[33] Accordingly, no issue of inconsistency with s 21 of the Bill of Rights Act arises.

Presumption of innocence

39. Section 25(c) of the Bill of Rights provides for the right to be presumed innocent until proved guilty by according to law. The right to be presumed innocent requires the prosecution to prove an accused person's guilt beyond reasonable doubt. We have examined proposed s 211 and various offence provisions in light of s 25(c).

Section 211

40. Section 211 repeats s 126 of the current Act. Under proposed s 211(1)(a) an action done an employee is to be treated as done by both the employee and the employer.

---

31 Fn 9.

32 Section 172.

33 Fn 9.

Proposed s 211(2) provides that in proceedings against the employer for an alleged act of their employee, it is a defence to prove that the employer took such steps as were reasonably practicable to prevent the employee from doing the alleged act.

41. Proposed s 211(2) places on the defendant a persuasive burden of proving that such steps were taken. Proposed s 212 thereby raises a prima facie issue of compliance with s 25(c) of the Bill of Rights Act. Whether the defendant took such steps as were practicable to prevent an employee acting in breach of the Bill will be a matter particularly within the defendant's knowledge. Offences under the Act occur in a regulatory area and are punishable by fine only. In the circumstances we consider the provision to be a proportionate measure rationally connected to the purpose of effective enforcement of the Act and the limitation of the right under s 25(c) is justified.

Proposed offence provisions

42. Various offence provisions in the Bill provide for certain acts to constitute an offence if done "without reasonable excuse."[34]

43. "Without reasonable excuse" provisions were formerly considered to reverse the onus of proof (at least where the defendant was proceeded against summarily),[35] thereby limiting the defendant's right to be presumed innocent until proved guilty. However, since the repeal of s 67(8) of the Summary Proceedings Act 1961, offences of this nature can be interpreted consistently with the presumption of innocence. Accordingly, the prosecution must prove beyond a reasonable doubt that a defendant did not have a reasonable excuse once an evidential burden is met.[36]

44. This advice has been peer reviewed by Austin Powell, Senior Crown Counsel.

_____

Helen Carrad
Crown Counsel

Noted

_____

Hon David Parker
Attorney-General
/ /2018

[34] Proposed ss 197, 122(1), 197 and 212.

[35] *Flahive v Jeffries* [2014] DCR 61 – In this case the District Court applied s 67(8) of the Summary Proceedings Act 1961 and held that the words "without reasonable excuse" in s 127(b) of the current Act placed a persuasive burden on the defendant.

[36] *King v Police* [2016] NZHC 977 at [24].