Human Rights Commission
Te Kāhui Tika Tangata

Submission on the Privacy Bill

24 May 2018

Contact: **John Hancock**
Senior Legal Adviser
JohnH@hrc.co.nz

Submission of the Human Rights Commission on the Privacy Bill

Introduction

1. The Human Rights Commission ("the Commission") welcomes the opportunity to provide this submission on the Privacy Bill ("the Bill") to Parliament's Justice and Electoral Committee ("the Committee").

2. The Bill has been several years in the making. Its foundations were set in place by the Law Commission's 2011 review of the Privacy Act 1993, which called for the current Act to be modernised so that it may better respond to the transformative advancements in information technology that have occurred since its enactment 25 years ago. Following the Law Commission's final report[1] and prior to the Bill's eventual introduction to the House, the Ministry of Justice has issued three Regulatory Impact Statements (RIS) in 2012[2], 2014[3] and 2016[4] on various aspects of proposed legislative reform.

3. In line with the approach recommended by the Law Commission, the Bill repeals and replaces the current Act. Nevertheless, many of the reforms it introduces are more incremental in nature than transformative. Much of the current Act, including the Information Privacy Principles (IPPs) remain substantially intact, although the Bill does make some notable changes to the placement of current provisions within the legislative structure.

4. In the Commission's view, there are some missed opportunities. Of most significance is the failure of the Bill to introduce a new IPP concerning the de-identification and re-identification of personal information, particularly given the previous analysis and recommendations on this issue contained in the 2016 RIS on the Bill. In addition, the Bill does not address directly the privacy issues that arise from new data analytic

[1] Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*, Report 123, June 2011, Wellington, http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf
[2] Ministry of Justice, *Privacy Act Reform Regulatory Impact Statement # 1,* March 2012 https://www.justice.govt.nz/assets/Documents/Publications/Regulatory-Impact-Statement-Privacy-Act-Reform.pdf
[3] Ministry of Justice, *Regulatory Impact Statement: Supplementary Government Response to Law Commission's report "Review of the Privacy Act 1993",* 13 March 2014, https://www.justice.govt.nz/assets/Documents/Publications/Regulatory-Impact-Statement-Review-of-the-privacy-act-1993.pdf
[4] Ministry of Justice, *Regulatory Impact Statement: Additional decisions for the Privacy Bill*, 4 February 2016, Wellington https://www.justice.govt.nz/assets/Documents/Publications/20160204-RIS-Privacy-Bill-further-Cabinet-decisions-final.pdf

techniques underpinned by advanced algorithmic processing and artificial intelligence. These techniques include predictive risk modelling, a methodology contemplated for use in our child protection sector. The Bill's lack of focus in this area appears somewhat incongruous with New Zealand's international position within the "Digital 7" group of countries, whose aim is to ensure that human rights standards are protected in the digital environment through the creation of a multinational framework for digital rights [5].

5. Furthermore, in light of the recent coming into force of the EU General Data Protection Regulation (GDPR), a law that many New Zealand state and private sector organisations will have to familiarise themselves with, the Bill appears antiquated and conservative in its approach to affirming and protecting privacy and human rights. As the Privacy Commissioner has observed, the Bill may have been fit for purpose in 2013, but it is questionable as to whether it remains so[6].

6. However, despite these limitations, the Bill's overall effect is to advance New Zealand's privacy standards. This includes the introduction of a new purposive provision that brings the policy focus of the legislation further into alignment with international privacy and human rights standards. It also introduces a number of reforms that strengthen the both the role and functions of the Privacy Commissioner and the statutory compliance, complaints and investigations infrastructure that the Commissioner oversees.

Summary of the Commission's key recommendations

7. In this submission, the Commission has made a number of recommendations aimed at enhancing the Bill's ability to address emerging issues through greater alignment with both international human rights standards and the rights-affirmative, future-focused approach taken by the GDPR. A full list of these recommendations is set out in an annexure at the end of the submission. Our key recommendations can be summarised as follows:

    a. **Strengthen the Bill's objectives in protecting and promoting human rights standards in line with the approach taken by the GDPR.**

[5] The group originally comprised of five countries, including New Zealand, known as the Digital 5. However, Uruguay and Canada joined in 2018- see https://www.beehive.govt.nz/release/leading-digital-nations-put-digital-rights-heart-their-agenda

[6] https://www.stuff.co.nz/national/104126249/all-you-need-to-know-about-the-proposed-privacy-laws

b. **Further enhance the Privacy Commissioner's functions to promote international instruments and make public statements on privacy and data rights.**
c. **Insert a new IPP on de-identified and re-identified personal information.**
d. **Assess the current suite of IPPs against the rights set out in the GDPR and take measures to address any identified shortfalls.**
e. **Provide that the Privacy Commissioner issue guidance materials or protocols on mandatory breach notifications, compliance orders and access requests.**
f. **Introduce a requirement that human rights impact assessments are undertaken as a matter of course in any information sharing initiative undertaken under Part 7.**
g. **Introduce a presumptive right of natural persons not to be subject to any decision arising from automated processing or profiling that produces a significant legal effect, similar to that provided under the GDPR.**

The Bill's Preliminary Provisions

Clause 3 - Purpose of Act

8. The Bill's introduction of a purpose clause is an important new development. The current Act does not have a purpose provision. Instead its purpose is set out in its long title which describes it, among things, as:

> *"an Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*…" (the OECD Guidelines[7]).

9. The long title also sets out the Act's primary operative purposes, namely the establishment of principles concerning collection, use, disclosure of and access to

[7] The OECD Guidelines were adopted on 23 September 1980, and most recently updated in 2013. The Preface to the OECD Guidelines notes that *"OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it".*

personal information and the appointment of the Privacy Commissioner to investigate complaints about interference with individual privacy.

10. However, the current wording of the long title does not expressly mention the existence of any freestanding *right* to privacy[8], nor does the body of the current Act. The right to privacy is also missing from New Zealand's statutory charter of civil and political rights, the New Zealand Bill of Rights Act 1990 (BORA), the preamble of which affirms New Zealand's commitments under the International Covenant on Civil and Political Rights (ICCPR).

11. As the Committee will no doubt be aware, the right to privacy is a fundamental human right conferred under Article 17 of the ICCPR, as well as a number of other human rights treaties ratified by New Zealand. Its lack of recognition within New Zealand legislation has been a concern for some time[9]. The Human Rights Commission[10], the Office of the Privacy Commissioner[11] and human rights advocates and academics[12] have called for the inclusion of the right to privacy in the BORA or a written constitution.

12. Against this context, the Bill's introduction of a purpose clause that expressly acknowledges the right to privacy is a positive development. Clause 3 provides that:

> The purpose of this Act is to promote and protect individual privacy by—
>
> a. providing a framework for protecting an *individual's right to privacy of personal information*, while recognising that other rights and interests may at times also need to be taken into account; and
>
> b. to give effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the *International Covenant on Civil and Political Rights.*

[8] Although paragraph 11 of the OECD Guidelines refer to the "general" protections referred to in the ICCPR and European Convention on Human Rights.
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[9] Human Rights Commission, *Privacy, Data and Technology: Human Rights Challenges in the Digital Age*, 2018, p 17, https://www.hrc.co.nz/files/5715/2575/3415/Privacy_Data_Technology_-_Human_Rights_Challenges_in_the_Digital_Age_FINAL.pdf

[10] See Submission of the Human Rights Commission on the Review of New Zealand's Constitutional Arrangements to the Constitutional Advisory Panel https://www.hrc.co.nz/your-rights/indigenous-rights/ourwork/review-new-zealands-constitutional-arrangements/.

[11] See Office of the Privacy Commissioner's Submission to the Constitutional Advisory Panel, https://www.privacy.org.nz/assets/Uploads/2017-12-08-Constitution-Aotearoa-Submission-Final.pdf

[12] http://constitutionaotearoa.org.nz/the-conversation/rights-privacy/.

13. However, when compared with the broad objective contained in Article 1 of the GDPR to *"protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data",* clause 3 appears rather equivocal. The Commission accordingly recommends that the purpose statement in clause 3 is amended to adopt similarly rights affirmative language.

<u>Recommendation 1:</u> Amend clause 3 to provide that "the purpose of this Act is to promote and protect the fundamental rights and freedoms of all persons, in particular individual privacy by…"

14. The proviso *"recognising that other rights and interests may at times also need to be taken into account"* is (probably deliberately) vague. In practice it will be important for the principles of legality, necessity and proportionality, which provide the basis for permissible limitations to the right to privacy under international human rights law[13], to be applied when considering competing rights and interests[14]. It is notable that these principles have recently been directly adopted in Ministerial Policy Statements issued under the Intelligence and Security Act 2017 that concern the activities of the intelligence and security agencies[15].

15. In order to ensure that clause 3 is interpreted in a way that is consistent with the human rights principles and jurisprudence that emanate from the right to privacy under Article 17 of the ICCPR, the Commission recommends that sub-clause 3(b) is amended to expressly refer to *human rights standards*.

16. However, we further recommend that the Committee should also consider whether a more prescriptive principles clause, similar to that provided under Article 5 of the GDPR is required to accompany a purpose clause. Article 5 sets out a number of over-riding principles that apply across the various provisions contained in the GDPR. These principles include:

    - Lawfulness, fairness and transparency

[13] Human Rights Commission, *Privacy, Data and Technology: Human Rights Challenges in the Digital Age*, 2018, p 26-27

[14] This includes recent policy developments concerning the production of group data sets. The Oranga Tamariki amendments, for example, provide that agencies that hold information relating to both individual children *and* any class of children may use and disclose that information. Agencies may also use any information relating to an individual child to produce, link or analyse datasets of information and produce combined datasetsChildren, Young Persons and their Families (Oranga Tamariki) Legislation Act 2017, sections 66C and 66D

[15] MPS [add cite]

- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

17. Article 5(2) goes on to establish an "accountability" principle that provides that controllers of personal data must be able to demonstrate compliance with the above principles.

<u>Recommendation 2:</u> Amend clause 3(b) of the Bill so that it provides that its purpose is to "to give effect to internationally recognised privacy obligations and *human rights* standards…"

<u>Recommendation 3:</u> Consider inserting a general principles clause based on the statements of principles and duties set out in Article 5 of the GDPR.

Sub-Part 2 – clauses 6-9

18. The Commission notes that much of the current Act is retained in the preliminary provisions of the Bill set out under this sub-part. The interpretation provisions, set out under clause 6, remain substantially the same but for three amendments, all of which are necessary to ensure the updated legislation has sufficient coverage. These are:

    - "*collects"* is broadened to include attempting to obtain information
    - "*publicly available information"* is updated include electronic publications, information that requires a fee charged for access and statutory registers able to be accessed by the public.
    - "*unique identifiers"* is amended to clarify that this term includes identifiers other than individual names

19. Clauses 7 and 8 simplify the wording of the current provisions in s 3 of the Act concerning "information held by an agency". It is notable that clause 8, which regards "personal information treated as being held by an agency under certain circumstances" appears to remove the current requirement under s 3(4) that an agency holding information on behalf of another agency is not the liable agency so long as it does not use or disclose the information for its own purposes. The effect of

clause 8 therefore appears to place sole liability on the principal agency (referred to as **Agency A** in the provision).

The role and functions the Privacy Commissioner

20. The Bill maintains the Privacy Commissioner's current status as an Independent Crown Entity and corporation sole.

21. Clause 14 of the Bill has simplified the Privacy Commissioner's functions under s 13 of the current Act. Some functions have been removed, including the Commissioner's auditing function under s 13(1)(b) and the monitoring of compliance with the privacy register principles under s 13(1)(e).

22. The Commission welcomes the addition of a new function under cl 14(1)(j) to:

> "undertake research into, and to monitor developments in, data processing and technology to ensure that any adverse effects of the developments on the privacy of individuals are minimised"

23. However, we recommend that this important function is given further ballast by providing the Privacy Commissioner with:

- An additional function to promote new international instruments concerning privacy and data rights; and

- A strengthened "public statements" function that applies to any matter (including actions of Government) that affects or infringes the privacy rights of individuals and groups, whether or not those rights are affirmed in New Zealand domestic law or international law.

24. This would align the Privacy Commissioner's functions in this regard with the Human Rights Commission's promotion[16] and public statements[17] functions under the Human Rights Act 1993. It would also strengthen the Privacy Commissioner's current roles under s 14 of the Act (retained by clause 18 of the Bill) to "take account of international

[16] Human Rights Act 1993 s 5(2)(kc)
[17] Ibid s 5(2)(c)

obligations" and "consider any developing general international guidelines relevant to the better protection of individual privacy".

25. More generally, the Commission notes that the Privacy Commissioner's monitoring and reporting function[18], the parliamentary reporting duty[19] and "duty to act independently"[20] are re-enacted in stand-alone provisions.[21] However, we note that the current Privacy Commissioner's function to undertake declaratory judgment proceedings under current s 20 has been relegated to a "miscellaneous provision" under clause 204 of the Bill. This reduces its visibility and the likelihood that it will be utilised. We recommend that it is retained in the suite of core functions under Part 2 of the Bill. We note that the Human Rights Commission's equivalent function is placed upfront in s 6 of the Human Rights Act.

<u>Recommendation 4:</u> Amend clause 14 of the Bill to provide the Privacy Commissioner with the following additional functions:

- **Promotion of new international instruments concerning privacy and data rights**
- **A strengthened "public statements" function to includes matters affecting or, infringing the privacy rights of individuals and groups, whether or not those rights are affirmed in New Zealand domestic law or international law, and including statements commenting on the position of the Government in relation to that matter:**

<u>Recommendation 5:</u> Place the Privacy Commissioner's function to undertake declaratory judgment proceedings in Part 2 of the Bill

[18] Privacy Bill, Clause 15
[19] Ibid Clause 16
[20] Ibid Clause 17
[21] We note that the current functions of the Commissioner concerning directories of personal information, supply of information under ss 21-22 of the Act are all missing from the Bill. This follows that Law Commission's recommendation that s 13(1)(d) and s 21 are repealed – see *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4,* chapter 5, rec 48; paras 5.15-5.17. This recommendation considered input from the Office of the Privacy Commissioner that maintaining a s 21 directory presents significant practical difficulties, requires much resources and does not produce a significant public benefit.

Clause 19 – the Information Privacy Principles

26. The Information Privacy Principles (IPPs), currently established under s 6 of the Act, sit at the heart of New Zealand privacy law and practice. Under the Bill, the IPPs have been shifted to clause 19. The Bill leaves the current IPPs largely intact. However, it makes a few minor amendments, some of which are of a technical nature and others of which have a more substantive effect.

27. *IPP 2* is amended to provide an additional exception that enables an agency to collect personal information from a source other than the individual concerned if the agency believes, on reasonable grounds, that it is necessary to collect the information from that source to prevent or lessen a serious threat to the life or health of any individual. This follows the Law Commission's recommendation that a "health and safety" exception is introduced into the provisions of IPP 2[22].

28. *IPP 3* is amended to remove existing exception under current IPP 3(4)(a) that permits an agency to collect personal information from the individual concerned without ensuring the individual is aware of specified matters, if the collection is authorised by the individual. The Commission supports this amendment as affirmative of the principles of informed consent and protection against arbitrary interference to privacy under Article 17 of ICCPR.

29. *IPP 4* is amended to require an agency to have particular regard to the age of the individual concerned to ensure the means by which personal information is collected is fair and does not intrude to an unreasonable extent upon the affairs of that individual. The Commission considers this amendment improves the alignment of the legislation with the rights of children to protection from interference to their privacy under Article 16 of the UN Convention on the Rights of the Child**.**

30. *IPP 7* is changed with the procedural provisions of existing *IPP 7(3) and (5)* being moved to *Part 4*:

31. The disclosure principles under *IPP 11* are changed in two respects. Firstly, the Bill introduced a *new subclause (2)* which clarifies that an agency may rely on the exception in *IPP 11(1)(e)(i)* (the maintenance of the law exception) to report any

[22] Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4,* Recommendation 12, p 82

reasonably held belief that an offence has been, or may be, committed. This is not a substantive amendment and simply clarifies that reporting to police constitutes as an example of permissible disclosure under IPP 11(e)(i).

32. Secondly, a more substantive change to IPP 11 is made by the inclusion of *new subclauses (3) to (6)*. These new provisions impose additional obligations on agencies when disclosing personal information to an overseas person to ensure the protection of that information. They provide that disclosure to an overseas person will generally only be permissible if:

    - the individual concerned consents to the disclosure of his or her information to the overseas person; or
    - the overseas person is in a country that is prescribed in regulations as having privacy laws comparable to New Zealand; or
    - the agency believes that the overseas person is required to protect the information in a way that, overall, is comparable to the protections afforded by our New Zealand legislation.

33. This amendment to IPP 11, read together with the agency obligations set out in clause 8, have the effect of adopting the Law Commission's recommendation that the Privacy Act should include an express statement of full accountability for cross-border outsourcing arrangements.[23]

34. The Law Commission also recommended that the Act is updated to:

    - Provide that the Privacy Commissioner issue guidance for agencies on conducting risk assessment prior to outsourcing personal information overseas and on the use of contractual or other means to ensure the application of privacy standards of a kind comparable to the New Zealand Privacy Act[24].

[23] Law Commission, R 107 at p 280 - based on the Canadian Personal Information Protection and Electronic Documents Act 2000, which provide that agencies are responsible for personal information it holds, including information that has been transferred to a third party for storage, custody or processing
[24] Ibid R 108

- include a provision allowing for the future adoption of a cross-border privacy rules system in New Zealand[25] and which concerns enhancement of co-operative powers with external agencies[26]

35. The Commission supports the imposition of additional obligations on agencies as regards their dealings with overseas entities. They essentially will require agencies to undertake some degree of due diligence in respect of any overseas entity with whom they may share personal information. However, these obligations do not apply to the exceptions under IPP 11 (1)(e)-(f) that concern maintenance and enforcement of the law, protection of public revenue, judicial proceedings and "serious threat" matters.

36. Furthermore, the Commission considers that protection of individual privacy rights in should be strengthened by amending sub-section (3) to provide for a presumption that disclosure to an overseas person will not occur without individual consent, unless it not reasonably practicable for that consent to be obtained in the circumstances.

37. The Bill also makes a number of changes to the requirements concerning unique identifiers under IPP 12. Most notable among these is new IPP 12(5) which places a positive obligation upon agencies to take all reasonable steps to minimise the risk of misuse of that identifier, prior to disclosure to an external agency.

Other issues regarding the IPPs:

Lack of an IPP concerning de-identification and re-identification

38. The Bill's omission of a new IPP that concerns the de-identification and subsequent re-identification of personal information data is disappointing. In its 2016 RIS on the Bill, the Ministry of Justice undertook an extensive analysis of this issue and, after assessment of the various options, recommended that a new IPP be introduced to address emerging privacy concerns raised by the Data Futures Partnership (DPF) and the Office of the Privacy Commissioner concerning de-identified and re-identified data.[27] The Ministry recommended that this amendment be accompanied with

[25] Ibid R 115 p 289
[26] Ibid R 114 p 288
[27] Ministry of Justice, *Regulatory Impact Statement: Additional decisions for the Privacy Bill*, 4 February 2016, https://www.justice.govt.nz/assets/Documents/Publications/20160204-RIS-Privacy-Bill-further-Cabinet-decisions-final.pdf at p 16 and 24

additional legislative guidance and definitions for ease of understanding and implementation.

39. In coming to this recommendation, the Ministry referred to the 2015 resolution by the UN General Assembly on the right to privacy in the digital age, which noted the rapid pace of technological development and the potential for the aggregation of certain types of metadata to reveal personal information[28]. The Ministry went on to observe that:

> "Re-identification has the potential to cause harm and damage public trust in how government and business handles the data of individuals. These are the sorts of outcomes that potentially undermine public service delivery and disrupt a workable framework for the protection of personal information".[29]

40. US legal commentary[30] has identified similar concerns:

> "Data re-identification occurs when personally identifying information is discoverable in scrubbed or so-called "anonymized" data. When a scrubbed data set is re-identified, either direct or indirect identifiers become known and the individual can be identified. Direct identifiers reveal the real identity of the person involved, while the indirect identifiers will often provide more information about the person's preferences and habits. Scrubbed data can be re-identified through three methods: insufficient de-identification, pseudonym reversal, or combing datasets. These techniques are not mutually exclusive; all three can be used in tandem to re-identify scrubbed data
>
> The current regulatory framework is predicated on the supposition that data that has been scrubbed of direct identifiers is "anonymized" and can be readily sold and disseminated without regulation because, in theory, it cannot be traced back to the individual involved. However, today's techniques of re-identification can nullify scrubbing and compromise privacy"

41. The Commission notes that the Ministry's Departmental Disclosure Statement[31] states that a new IPP was put on hold pending the outcome of work on the issue by the DPF.

---

[28] A/HRC/28/L.27, 24 March 2015

[29] Ministry of Justice, *Regulatory Impact Statement: Additional decisions for the Privacy Bill*, 4 February 2016, a para 37

[30] Lubarsky B, Re-identifcation of Anonymized Data, Georgetown Law Review, April 2017 1 GEO.L.TECH.REV.202 (2017), https://www.georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/

[31] https://www.justice.govt.nz/justice-sector-policy/constitutional-issues-and-human-rights/regulatory-impact-statements/

It goes on to state this work was never completed due to the expiry of the DPF working groups contracts and that, "as such" the Bill does not include an IPP concerning re-identification.

42. In the Commission's view, this is an insufficient reason to hold up the introduction of the new IPP. The Ministry's 2016 RIS provided an extensive analysis and options comparison. The DPF also provided the Government with interim advice in July 2017 that recommended systemic amendments be made. The Commission accordingly recommends that the Committee amends the Bill to introduce a new IPP concerning de-identified and re-identified information.

<u>Recommendation 6:</u> Following technical advice from the Ministry of Justice and Office of the Privacy Commissioner, insert a new Information Privacy Principle regulating de-identification and re-identification of personal information.

Insertion of an anonymity/psuedonymity principles in IPP1

43. In its 2011 report, the Law Commission recommended that IPP 1 should be amended by adding a new sub-clause providing that "individuals should be able to interact with agencies anonymously or under a pseudonym, where it is lawful and practicable to do so in the circumstances".[32] The Law Commission noted that jurisdictions such as Australia and Germany provide for a right to anonymity and identified a number of situations[33] in which it will generally be lawful and practicable for an agency to interact with an individual anonymously, including:

    - Where an individual visits an agency's office or phones an agency to seek general information or to make a general inquiry.
    - Where an individual makes a general complaint to an agency, or fills in a comments form, regarding the level of service provided by the agency. The individual does not wish the agency to follow up with him or her, and is commenting on the level of service generally rather than on the actions of any individual.

[32] Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4,* Recommendation 35, p 122
[33] Ibid at 3.150

- Where an individual seeks counselling over the phone for a personal problem, but does not wish to establish an ongoing relationship with the agency providing the counselling.

44. The Commission further notes that Article 11 of the EU General Data Protection Regulation provides that "if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data…".

45. The Commission notes that the right to anonymity is accordingly becoming a standard principle in international instruments governing personal data collection and use. We accordingly recommend that the Bill is amended to insert a

<u>Recommendation 7:</u> That the Committee amend clause 19 of the Bill to insert within IPP 1 a right of individuals to anonymity along the lines of the Law Commission's 2011 recommendation.

Consistency of IPPs with GDPR rights

46. The EU General Data Protection Regulation (GDPR) introduces a number of important new privacy rights and concepts, many of which directly address emerging challenges to the right to privacy that have arisen due to recent advances in digital information technology. It would be fair to say that the GDPR is far in advance of the Bill and the current Act in responding to the contemporary technological environment.

47. The Commission therefore strongly recommends that the Committee assess the current scope of the IPPs under the Bill against the rights and principles introduced by the GDPR. We set out a number of the most important of these new rights and principles below.

The right to be forgotten/the right to erasure

48. Article 17 of the GDPR introduces a right to erasure, colloquially known as "the right to be forgotten. It provides an individual with the right to have a data controller erase his or her personal information, cease further dissemination of the information, and potentially halt the processing of that information by third parties.

49. The conditions for erasure under article 17 include where the individual's personal information is no longer being relevant to original purposes for processing, or where the individual withdraws consent to their information being used. Article 17 provides for limited exceptions where the ongoing processing of personal information data is:

    - Necessary to exercise the right to freedom of expression and information,
    - In the public interest as regards public health, legal compliance, scientific or historical purposes
    - Required for the establishment, exercise or defence of legal claims.

The right to data portability

50. Article 20 of the GDPR introduces a "right to data portability". This provides for a right of individuals to request and receive any personal information they have previously provided in a "structured, commonly used and machine-readable format". Individuals also have the right to transmit their personal information to another data controller "without hindrance".

51. Article 20 goes on to provide that an individual may exercise their right to data portability without prejudice to their ability to exercise their right to erasure under Article 17. Like Article 17, a public interest exception may be applied to data portability requests.

Privacy by design

52. The concept of "privacy by design" calls for the inclusion of data protection measures from the onset of the designing of systems, rather than as an addition. The GDPR incorporates this right in Article 25, which, among other things requires data controllers to implement effective "appropriate technical and organisational measures" that, among other things:

    - Are designed to meet the requirements of [the GDPR] and protect the rights of data subjects
    - Ensure that only personal data which is necessary for each specific purpose is processed. This obligation applies to collection, processing and storage of personal data.

Rights in respect of automated individual decision-making, including profiling

53. Article 22 of the GDPR provides that individuals have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

54. There are limited exceptions to this rule, namely where the decision is:

    - Necessary for the entering into a contract between the individual and the data controller, or
    - where the decision is authorised by State party law which include suitable safeguards as regards the individual's rights and freedoms and legitimate interests
    - based on the individual's explicit consent

55. It is notable that Article 22 provides that all the above exceptions are subject to a requirement that data controllers implement measures to safeguard the individual's rights and freedoms and legitimate interests. Article 22(3) provides that, as a minimum, this must enable the individual their right to "obtain human intervention on the part of a controller, to express his or her view and to contest the decision."

Automated processing/profiling and freedom from discrimination (Article 9 GDPR)

56. Furthermore, Article 22(4) provides that the exception as regards State party actors do not apply to any of the special categories of personal data set out in Article 9(2) of the GDPR. Article 9(1) provides for a general prohibition against processing of personal data that:

    - reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
    - concerns genetic data, biometric data for the purpose of uniquely identifying a natural person
    - concerns health or data concerning a natural person's sex life or sexual orientation.

57. Article 9(2) sets out a number of limited exceptions (deemed "special categories). However, the effect of Article 22(4) is to prohibit automated processing and profiling

in respect of any of those special categories, excepting situations where the individual has given explicit consent (unless legally prevented from doing so under statute) or where processing is authorised under statute and is of 'substantial public interest". In both cases, any authorising law shall be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

<u>Recommendation 8</u>: That the Committee assess the current suite of IPPs against the privacy rights guaranteed under the GDPR, including but not limited to, the following GDPR Articles:

- **The right to erasure (Article 17)**
- **The right to data portability (Article 20)**
- **The concept of privacy by design (Articles 24 and 25)**
- **Rights of persons in respect of automated individual decision-making, including profiling (Articles 22 and 9)**

The Commission recommends that the Committee subsequently takes advice from the Ministry of Justice and the Privacy Commissioner on measures required to address shortfalls.

The role and responsibilities of data protection officers (DPOs)

58. The GDPR removes a previous mandatory requirement that all organisations that control and process personal information appoint data protection officers (DPOs). It provides that DPOs will only be mandatory for those data controllers and processors whose core activities consist of processing operations which require *"regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences".*

59. It also requires that DPOs are appointed on the basis of professional qualities and have expert knowledge on data protection law and practices. DPOs must also be provided with resources appropriate to carry out their tasks and maintain their expertise, must report directly to the highest tier of management and must not carry out any task that could result in a conflict of interest.

60. The equivalent role in the Bill is that of a privacy officer, established under clause 201 which is simply a re-enactment of the current privacy officer provision under s 23 of the Act. This role is mandatory, but with much less responsibility and scope than the DPO role under the GDPR. Given the increasing complexities arising from the management of personal data, the Committee may wish to consider whether the DPO model set out in the GDPR should be adopted in New Zealand.

Other Key Changes

Mandatory reporting of privacy breaches

61. Clauses 117-123 of the Bill set out a system requiring that agencies report to the Privacy Commissioner any privacy breach that meets the "notifiable" threshold. This threshold is set out in clause 75(2)(b) of the Bill and applies to actions that:

    - has caused, or may cause, loss, detriment, damage, or injury to the individual; or
    - has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or
    - has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual

62. A privacy "breach" is subsequently defined under clause 117 as:

> "unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or an action that prevents the agency from accessing the information on either a temporary or permanent basis."

63. Clause 119 of the Bill provides that agencies must also notify individuals, or if that is not reasonably practicable, give public notice that the breach has occurred. The Bill provides that a failure to notify may constitute an "interference with privacy" and lead to investigation accordingly. Clause 120 sets out a series of exceptions to notification, where doing so would compromise security or defence; prejudice the maintenance of the law; endanger safety; reveal trade secrets; be contrary to the interests of a child aged under 16; and prejudice individual health (after consultation with physician).

64. Clause 122 provides that it is an offence for an agency to fail to report a notifiable breach, with a maximum penalty of a $10,000 fine. Liability is strict - there is no

defence that agency did not consider the matter reasonably reached the notifiable privacy breach threshold, nor whether it had taken prior steps to address and remedy the breach. This will undoubtedly pose a challenge for agencies, as among other things, they will be required to assess whether individual "rights, benefits, privileges, obligations, or interests" have been or may be adversely affected as a result of the breach. It is likely that agencies will adopt a low reporting threshold accordingly, in order to mitigate against their risk of liability.

65. The Bill's introduction of a mandatory breach notification system follows the 2011 recommendations of the Law Commission. The Law Commission commented that while a "*universal and absolute obligation to notify…would collapse under its own weight"*…

> *…in **particularly serious cases** the benefit of notification to affected individuals is so clear that it outweighs the disadvantages to the agency concerned, and those disadvantages will usually not be so great in any case. That will particularly be the case if notification enables the individual to contain or limit the damage, or otherwise to soften the impact.*[34]

66. The Law Commission went on to recommend the following threshold for mandatory notification[35]:

- if such notification will enable the recipient to take steps to mitigate a real risk of significant harm; or
- if the breach is a serious one

67. The Law Commission also recommended that when determining whether a breach is serious, the agency should take into account[36]:

- whether or not the information is particularly sensitive in nature;
- the hands into which it may fall or have fallen;
- whether it is reasonably foreseeable that significant harm might result; and
- the scale of the breach

68. The Bill notably departs from the Law Commission's recommended framework. The assessment criteria are more burdensome on agencies and do not expressly recognise the mitigatory purpose of reporting a breach. In addition, the Bill's

[34] Law Commission, para 7.19 p 210
[35] Law Commission, Rec 68 p 212
[36] Ibid R 69 at p 212

introduction of a strict liability offence goes beyond the Law Commission's recommendation that failure to report constitute a ground for complaint.[37]

69. The Bill also does not implement the Law Commission's recommendation[38] that the Privacy Commission should provide public guidance on mandatory breach notification:

> *we believe that clear explanatory guidance from the Privacy Commissioner will be important. We recommend that, should data breach notification become compulsory, the Privacy Commissioner should publish guidance on the subject. The existing voluntary guidelines should serve as a useful starting point*[39]

70. In general, the Commission supports the introduction of a mandatory breach notification regime. Similar requirements exist in similar overseas jurisdictions. For example, in Australia the Privacy Amendment (Notifiable Data Breaches) Bill 2016[40] was enacted and came into force on 22 February 2018. It applies a "serious breach" threshold for notification.

71. Mandatory notification is also a feature of the GDPR. Article 33 provides that data controllers must notify data breaches to the "supervising authority" of the state jurisdiction within 72 hours of awareness. Article 34 provides for a parallel duty to notify the individual data subject. Notification is presumptive. Non-notification may only occur in circumstances where the breach is "unlikely to result in a risk to the rights and freedoms of natural persons".[41]

72. It follows that the introduction of a mandatory breach notification and reporting system broadly aligns New Zealand law with international standards. It also, in a general sense, enables victims of a notifiable privacy breach to a remedy of sorts, consistent with the human right to a remedy conferred under Article 2(3) of the ICCPR.

---

[37] Ibid at 7.34
[38] Ibid R 79 at 215
[39] Ibid para 7.36
[40] https://www.oaic.gov.au/media-and-speeches/media-releases/mandatory-data-breach-notification-comes-into-force-this-thursday
[41] It is also notable that the GDPR introduces, under Article 35, an obligation on data controllers to undertake "data protection impact assessments" which apply all facets to the processing operations undertaken or utilised by data controllers and processers

73. However, given the potential complexities that exist for both agencies and individuals as regards its implementation, the Commission recommends that, in accordance with the Law Commissions recommendation, the Bill is amended to provide that the Privacy Commissioner publish guidance on the subject.

<u>Recommendation 9:</u> That the Bill is amended to provide for the production of protocols or guidance material on the mandatory breach notification and reporting system.

Compliance notices and Access requests

74. Clause 124 provides that the Privacy Commissioner may issue a compliance notice to an agency if he or she considers that one or both of the following may have occurred:

- a breach of the Privacy Act, including an action listed in section 75(2)(a) or non-compliance with a PRPP:
- an action that is to be treated as a breach of an IPP or an interference with the privacy of an individual *under another Act*.

75. The power is discretionary. Under clause 124(2), the Privacy Commissioner may weigh up the existence of harm and whether other means can be used to deal with the breach. The introduction of this power adopts the 2011 recommendation of the Law Commission[42] which, in making the recommendation noted that "a considerable number of PCs in cognate jurisdictions have such powers".

76. The framework in the Bill largely implements the procedures recommended by the Law Commission. It provides respondents with a right of notice under which they may provide the Privacy Commissioner with comment prior to determination. The Privacy Commissioner's powers are also fortified by the ability to take enforcement proceedings in the Human Rights Review Tribunal (HRRT)[43]. Conversely, respondents may appeal to the HRRT against a compliance order and seek interim orders suspending the notice pending determination of their appeal.

[42] Law Commission R 63, p 194
[43] Privacy Bill, Clause 130

77. Clause 96(5) of the Bill also provides the Privacy Commissioner with a new power to issue binding decisions in respect of access requests made under IPP 6. As with compliance notices, the Commissioner's exercise of this power is discretionary. The Privacy Commissioner may also, at his or her discretion, refer the matter to the Director of Proceedings to take action in the HRRT, or take any other action the Commissioner considers appropriate. Respondents retain a right of appeal to the HRRT in respect of any access decision made by the Privacy Commissioner under these provisions.

78. It is notable that, in respect of compliance notices, the Law Commission considered that it would be helpful that a protocol be issued. We support this recommendation and consider that such a protocol could also include guidance on the Commissioner's binding decision-making powers as regards access requests.

<u>Recommendation 10:</u> That the Privacy Commissioner issue a protocol or guidance materials concerning the exercise of his or her functions, and the corresponding rights and duties of respondents, concerning the issuance of compliance notices and binding decisions on access requests.

Part 7 of the Bill - Information sharing

79. Part 7 of the Bill (clauses 136 to 161) re-enacts the information sharing provisions currently set out in Part 9A and schedule 2A of the Act. This includes the provisions concerning the establishment of Approved Information Sharing Agreements (AISAs) between agencies.

80. As set out in the Bill's Explanatory Note, the Bill introduces substantive amendments to the provisions that determine the types of agencies who may enter into an AISA. The overall effect of these amendments is to broaden the types of agencies who qualify. The Bill removes the current requirement that at least one of the parties to an AISA be a department of state. Instead, an AISA will be required to have at least one "specified organisation" as a party, who will be able to be deemed as "the lead agency".

81. In addition, the current concept of a representative party is removed and replaced by a provision that enables AISAs to apply to a class of agencies and for any member of that class to become a party to an AISA by being named in a schedule affixed to it for

that purpose[44]. Parties that propose to enter into an AISA must accordingly consult and invite submissions from any person or organisation representing that class of agencies[45].

82. The Bill retains the current broader requirements under s 96O for agencies to consult with the Privacy Commissioner and persons or organisations whom the agencies consider should be consulted, including those who represent the interests of the classes of individuals who personal information will be shared under the AISA. The Privacy Commissioner's mandatory consideration of the privacy implications of the AISA is also retained.

83. It is notable that the Bill does not introduce any express requirement to ensure that human rights considerations are considered in the formation of an AISA. In the Commission's view this is a significant omission. Certain information sharing practices have clear human rights implications that extend beyond the right to privacy. Predictive risk modelling (PRM) for example, may target specific demographic populations and, as such, raise the possibility of discrimination. Advanced algorithmic techniques, such as PRM, are also likely to require legal authorisation by an AISA as they will generally be designed to apply to personal data gathered from a number of different agencies[46].

84. As AISAs are not primary legislative instruments, they are not subject to a mandatory rights assessment under s 7 of BORA. MSD is currently attempting to address this gap in its area of business through the development of a Privacy, Human Rights and Ethics (PHRAE) Framework to apply to its information sharing and data analytic practices, including PRM. The Commission supports MSDs efforts in this regard but notes that the PHRAE Framework is intended to be a policy tool only, has no legal effect and its application is at this stage intended to be limited to MSD's jurisdiction.

85. In its 2016 review of New Zealand, the UN Committee on the Rights of the Child noted the intention of the New Zealand Government to introduce PRM in the child protection sector. The UN Committee accordingly recommended that the New Zealand

[44] Privacy Bill, Clause 143
[45] Privacy Bill, Clause 150
[46] Such as MSD's proposed 2015 Youth Services AISA for example, see https://www.hrc.co.nz/files/7914/6483/4019/16g_Human_Rights_Commission_feedback_on_draft_Youth_Service_AISA.pdf

Government "take all measures necessary to fully protect the right of the child to privacy" and, in doing so, ensure that [47]:

- "any legislation enabling the collection, storage and sharing of personal information about children and their families include an explicit requirement to take into consideration the best interests of the child";
- "the Privacy, Human Rights and Ethics framework governing predictive risk modelling takes in consideration the potentially discriminatory impacts of this practice, is made public and is referenced in all relevant legislation"

86. The current Bill clearly falls well short in addressing either of these recommendations. It also falls well short of the standards that have recently been introduced in the EU under the GDPR. Articles 9 and 22 of the GDPR, for example, combine to set in place presumptive right of an individual:

- not to be subject to any decision arising from automated processing or profiling that produces a legal effect that significantly affects him or her.
- to protection from discrimination as a result of data processing, through a prohibition on the processing of personal data that reveals certain demographic information including racial and ethnic origin.

<u>Recommendation 11:</u> The Commission therefore strongly recommends that the Committee amend the Bill to introduce a requirement that human rights impact or due diligence assessments are undertaken as a matter of course in any information sharing initiative undertaken under Part 7.

<u>Recommendation 12:</u> We further recommend that a presumptive right not to be subject to any decision arising from automated processing or profiling that produces a significant legal effect, similar to that provided under Article 22 of the GDPR, is inserted in the Bill.

[47] CRC/C/NZL/CO/5, 21 October 2016, paragraphs 20, 20(a) and 20(b)

ANNEXURE

Human Rights Commission Submission on the Privacy Bill 2018

List of recommendations

Recommendation 1:

Amend clause 3 to provide that "the purpose of this Act is to promote and protect the fundamental rights and freedoms of all persons, in particular individual privacy by…"

Recommendation 2:

Amend clause 3(b) of the Bill so that it provides that its purpose is to "to give effect to internationally recognised privacy obligations and *human rights* standards…"

Recommendation 3:

Consider inserting a principles clause based on the statements of principles and duties set out in Article 5 of the GDPR.

Recommendation 4:

Amend clause 14 of the Bill to provide the Privacy Commissioner with the following additional functions:

- Promotion of new international instruments concerning privacy and data rights
- A strengthened "public statements" function to includes matters affecting or, infringing the privacy rights of individuals and groups, whether or not those rights are affirmed in New Zealand domestic law or international law, and including statements commenting on the position of the Government in relation to that matter:

Recommendation 5:

Place the Privacy Commissioner's function to undertake declaratory judgment proceedings in Part 2 of the Bill

Recommendation 6:

Following technical advice from the Ministry of Justice and Office of the Privacy Commissioner, insert a new Information Privacy Principle regulating de-identification and re-identification of personal information.

Recommendation 7:

That the Committee amend clause 19 of the Bill to insert within IPP 1 a right of individuals to anonymity along the lines of the Law Commission's 2011 recommendation.

Recommendation 8:

That the Committee assess the current suite of IPPs against the privacy rights guaranteed under the GDPR, including but not limited to, the following GDPR Articles:

- The right to erasure (Article 17)
- The right to data portability (Article 20)
- The concept of privacy by design (Articles 24 and 25)
- Rights of persons in respect of automated individual decision-making, including profiling (Articles 22 and 9)

The Commission recommends that the Committee subsequently takes advice from the Ministry of Justice and the Privacy Commissioner on measures required to address shortfalls.

Recommendation 9:

That the Bill is amended to provide for the production of protocols or guidance material on the mandatory breach notification and reporting system**.**

Recommendation 10:

That the Privacy Commissioner issue a protocol or guidance materials concerning the exercise of his or her functions, and the corresponding rights and duties of respondents, concerning the issuance of compliance notices and binding decisions on access requests.

Recommendation 11:

That the Committee amend the Bill to introduce a requirement that human rights impact assessments are undertaken as a matter of course in any information sharing initiative undertaken under Part 7.

Recommendation 12:

That a presumptive right not to be subject to any decision arising from automated processing or profiling that produces a significant legal effect, similar to that provided under Article 22 of the GDPR, is inserted in the Bill.