NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

Input of the New Zealand Human Rights Commission: OHCHR Report on the Right to Privacy in the Digital Age

10 April 2018

Contact:

John Hancock / Eleanor Vermunt
Senior Legal Adviser / Legal Adviser
New Zealand Human Rights Commission
johnh@hrc.co.nz / eleanorv@hrc.co.nz

Input of the New Zealand Human Rights Commission:
OHCHR report on right to privacy in the digital age

Introduction

1. The Human Rights Commission ("Commission") welcomes the opportunity to provide input into the OHCHR's report on the right to privacy in the digital age.[1] The Commission is New Zealand's National Human Rights Institution (NHRI) and is accredited with an "A Status" under the Paris Principle criteria. The Commission is an independent Crown Entity established under the Human Rights Act 1993.

2. As part of its advocacy work, the Commission has considered and engaged with a range of government agencies and non-governmental organisations on the human rights challenges relating to personal data and surveillance in the digital age.

3. New Zealand's Bill of Rights Act 1990 (BORA) affirms its commitment to the International Covenant on Civil and Political Rights and incorporates most of the rights in the Covenant.[2] However, a key right is omitted – the right to privacy equivalent to Article 17 of the Covenant. The Commission,[3] the Office of the Privacy Commissioner,[4] and human rights advocates and academics[5] have called for the inclusion of the right to privacy in the BORA or a written constitution for New Zealand. Importantly, this would ensure that the Attorney-General considers the effect of the right to privacy on any new bill introduced into parliament under its BORA reporting function.[6] Furthermore, it would allow the Courts to issue a declaration of inconsistency if they believe that legislation is inconsistent with the right to privacy.[7]

4. In the absence of a free-standing right to privacy in New Zealand law, the Government has taken a mixed approach to incorporating international standards and principles that underpin

---

[1] The New Zealand Office of the Privacy Commissioner was consulted for comment on this input.
[2] New Zealand Bill of Rights Act 1990, http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html.
[3] 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/our-work/review-new-zealands-constitutional-arrangements/.
[4] 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 .
[5] http://constitutionaotearoa.org.nz/the-conversation/rights-privacy/.
[6] Section 7, BORA.
[7] The question of whether the Courts have the inherent jurisdiction to grant a declaration of inconsistency as a remedy if they believe legislation is inconsistent with the Bill of Rights Act, was argued in the Supreme Court in February 2018. That same month, the Minister of Justice announced that Cabinet had agreed in principle to allow courts to make a declaration of inconsistency and that the Bill of Rights Act will be amended to give the Courts this power.

the right to privacy in legislation and policy.[8] This input will discuss the Government's current approach by focusing on the following aspects of the OHCHR's proposed list of issues:

a. Recent developments in national legislation and policy
b. Predictive risk modelling, including in the child welfare sector
c. Procedural and institutional safeguards, oversight mechanisms and remedies

A. Recent Developments in national legislation, policy and practice

Privacy Bill

5. On 20 March 2018, a new Privacy Bill was introduced into Parliament to repeal and replace the existing Privacy Act 1993. The new Bill follows the 2011 Law Commission Review of the Privacy Act which contained 136 recommendations for change,[9] as well as calls by the Privacy Commissioner to modernise the Act.[10]

6. The existing law, the Privacy Act 1993, regulates the collection, use and disclosure of information about individuals. At the core of the Act are the 12 information privacy principles (IPPs) that guide the way that government agencies and private companies (referred to in the legislation as Agents) handle personal information, including in relation to the collection, storage, security, access, accuracy, retention, and disclosure of personal information.[11]

7. The new Bill modernises that Privacy Act in response to the way technology has revolutionized the handling of personal data, while retaining the 12 IPPs. The IPPs largely remain the same under the Bill, with the exception of IPP 11 on disclosure of information and IPP 4 on the manner of collection of personal information. IPP 11 strengthens the requirements relating to the disclosure of information to an overseas person. Among the new requirements are that the disclosing agency must not disclose the personal information unless the agency believes on reasonable grounds that the overseas person is required to protect the information in a way that, overall, provides comparable safeguards to those in the Act.[12] IPP 4 is amended to require an agency to consider the age of an individual when deciding whether the means of collection of personal information is fair and not unreasonably intrusive.[13]

---

[8] Note that the Court of Appeal has found that the Common Law could be developed to recognise a free-standing tort of privacy that protects persons against the publication of private facts in certain circumstances. See *Hosking v Runting* [2004] 1 NZLR 1.
[9] http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf .
[10] See https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf .
[11] Part 2 of the Privacy Act 1993, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html .
[12] Privacy Bill, Clause 19, http://www.legislation.govt.nz/bill/government/2018/0034/latest/whole.html#LMS23342 .
[13] Ibid.

8. Importantly, the purpose statement of the Bill has been strengthened to contain a clearer focus on protecting and promoting privacy. It directly incorporates an "individual's right to privacy of personal information" and recognises "privacy obligations and standards in relation to the privacy of personal information, including … the International Covenant for Civil and Political Rights."

9. The most significant reforms to the law are the increased accountability mechanisms supporting the early identification of systematic privacy risks. These changes are outlined below in Section C on safeguards and remedies.

10. While the Bill has a number of positive aspects, several important recommendations made by the Privacy Commissioner and Law Commission have not been addressed, particularly in relation to re-identification of individuals from information held by agencies and the ability for individuals to interact with agencies anonymously or under a pseudonym. However, these are issues that the current government has indicated it will continue to work on as the Bill progresses through the House. The Bill does not directly address issues related to the impact of advanced "Big Data"[14] techniques upon personal information, such as the use of algorithms and artificial intelligence for predictive purposes. However, the broad principles-based approach of the current Act, which is carried over to the new Bill, is designed to address issues relating to new technologies without requiring explicit legislative provisions.

Intelligence and Security Law and Policy

11. In March 2016, a major independent review of the intelligence and security legislation was presented to parliament.[15] The review itself was conducted in the wake of the arrest and surveillance of Kim Dotcom by New Zealand intelligence and law enforcement agencies in 2013, an event which highlighted significant deficiencies in New Zealand's legislative framework. Reflecting the earlier recommendations of the Human Rights Commission,[16] the terms of reference of the review included scrutiny of New Zealand law against international human rights law and standards. It included recommendations to consolidate the legislation into one statute and strengthen oversight and accountability mechanisms, including those

[14] As regards the term "Big Data" we refer to the characterisation given to it by the UN Special Rapporteur on the Right to Privacy *as a "term commonly used to describe the large and increasing volume of data and the advanced analytical techniques used to search, correlate, analyse and draw conclusions from it* – see Report of Special Rapporteur on the Right to Privacy (24 February 2017) para 36.
[15] See Report of the First Independent Review of Intelligence and Security in New Zealand, *Intelligence and Security in a Free Society*, by Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM publicly released on 9 March 2016 http://www.igis.govt.nz/assets/Uploads/Review-report-Part-1.pdf .
[16] Human Rights Commission, *Report to the Prime Minister: Government Communications Security Bureau and Related Legislation Amendment Bill; Telecommunications (Interception Capability and Security) Bill and associated wider issues relating to surveillance and the human rights of people in New Zealand*, 9 July 2013.

regarding access to information from other government agencies, and set out a proposed authorisation framework for intelligence and security activities.

12. The Government accepted most of the reviewers' recommendations and in April 2017 the Intelligence and Security Act was enacted, replacing the four separate laws that previously governed this area.[17] The strong human rights-based approach adopted in the review is reflected in the new legislation, resulting in human rights considerations being elevated among the purposes of the law and decision-making principles.

13. The purposes of the Act include: "ensuring that the functions of the intelligence and security agencies are performed – in accordance with New Zealand law and human rights obligations recognised by New Zealand law"; and ensuring "that the powers of the intelligence and security agencies are subject to institutional oversight and appropriate safeguards." This has included enhancing the functions of the principal oversight entity, the Inspector-General of Intelligence and Security and requiring the responsible Minister must issue Ministerial Policy Statements (MPS) which set out policy and practice standards concerning the operational activities of the intelligence and security services18. These are covered in more detail at paragraphs 37-39 below.

14. Another legislative outcome of considerable significance was the amendment to section 57 of the Privacy Act to provide that intelligence and security agencies are subject to most of the Act's IPPs,[19] including the requirement under IPP 4(a) that personal information is collected by lawful means. Prior to the amendment, the agencies were exempt from this requirement, as well as most of the other IPPs.[20] This amendment was sought by the Privacy Commissioner and has the effect of significantly strengthening the application of privacy rights and standards to the surveillance and information gathering activities of the intelligence and security agencies.

[17] http://www.legislation.govt.nz/act/public/2017/0010/37.0/DLM6920823.html .
[18] Intelligence and Security Act 2017, s 208.
[19] Other than those regarding the source of personal information (IPP 2), collection of personal information (IPP3) and collection of personal information by unfair or unreasonably intrusive means (IPP 4(b)).
[20] Prior to the amendment, intelligence and security agencies were exempt from all IPPs, other than IPP 6 (regarding access to personal information which itself is a national security exemption under s 27), IPP 7 (regarding correction of personal information) and IPP 12 (which regulates the assignment and use of unique identifiers)

Law Commission review of the Search and Surveillance Act

15. The New Zealand Law Commission has undertaken a comprehensive review of the Search and Surveillance Act 2012, the statute governing the search and surveillance powers of New Zealand law enforcement agencies.[21]

16. As part of the review, the Law Commission considered, among other things, the statutory thresholds concerning the external authorisation of search and surveillance activities. In submissions and discussions with the Law Commission on this issue, the Commission has advocated for the adoption of a mandatory authorisation regime.[22]

17. The Commission considers that this position reflects international human rights standards, which indicate that authorisation is required for the discharge of invasive powers[23]. This is further supported by Principle 10 of the 2017 Global Principles on Protection of Freedom of Expression and Privacy (itself a syntheses of applicable international human rights standards) which provides that states should ensure that:

    a. Access to, and search and seizure of information is only justified if the measures strictly comply with the requirements of legality, legitimate aim, necessity, and proportionality;
    b. Search of individuals' home or workplace, online accounts, remote data storage, collection of metadata and any seizure of information may only be compatible with the rights to freedom of expression and privacy if ordered by a court and if strictly compliant with the requirements of legality, legitimate aim, necessity, and proportionality under international human rights law.

18. The Commission also submitted that, in reflection of the reforms to intelligence and security legislation, updated search and surveillance legislation should contain provisions that set out specific principles that require that functions undertaken under its jurisdiction conform with all domestic and international human rights obligations recognised by New Zealand law. The Commission has also sought that new legislation contain specific provisions that uphold human rights principles concerning journalistic sources and privilege[24] and the special

[21] http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-redacted-web.pdf.
[22] Human Rights Commission, *Submission on the Review of the Search and Surveillance Act 2012*,16 December 2016, para 5.
[23] Report of the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, A/HRC/14/46, 17 May 2010 and the OHCHR, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014
[24] See Global Principle 10(c) of the Global Principles on Protection of Freedom of Expression and Privacy

protection rights of vulnerable population groups, including children and people with disabilities.

19. The Law Commission released its report on 30 January 2018 and is currently awaiting a formal Government response. On the issue of authorisation, the Law Commission has recommended that, in preference to the mandatory authorisation approach advanced by that new legislation include a general principle that "conduct that may constitute an intrusion into the reasonable expectations of privacy of any individual should be carried out pursuant to a warrant, order, statutory power or policy statement."[25]

20. The Law Commission has also recommended the inclusion of a suite of other statutory principles, including the principle that:

    a. A warrant or order should be obtained in preference to exercising a warrantless power.
    b. State intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of the offence or the maintenance of the law.
    c. Powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected.
    d. Powers under the Act should be exercised having regard to *te ao Māori*[26] and any other relevant cultural, spiritual or religious considerations.
    e. Powers under the Act should be exercised in a manner that minimises the impact on children and vulnerable members of the community.
    f. Powers under the Act should be exercised in a manner that protects any privilege held by, or available to, any individual.

Citizen Based Analytics

21. New Zealand is taking a leading and innovative approach to the use of scientific evidence to inform public policy, led by the Office of the Prime Minister's Chief Science Advisor, Sir Peter Gluckman. In June 2017, the Office released a discussion paper on the benefits and limitations of how the Government can use big data to better inform social policy decisions,

[25] http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-redacted-web.pdf, para 4.34.
[26] Approximately translated to *'The Māori World'* – Māori are the indigenous people of New Zealand

an approach described as "social investment" in New Zealand.[27] The research was the result of a collaboration with European data statisticians via the European Commission.

22. The use of data and citizen-based analytics has been made possible in New Zealand through the development of the Integrated Data Infrastructure (IDI), a large research database containing microdata about people and households taken from a range of government agencies, Statistics NZ and NGOs.[28] Once the data is linked it is anonymised and placed under the custodianship of Statistics NZ. Researchers and analysts can then examine the data to look for trends and relationships between factors.[29] The IDI has been subject to privacy impact assessments and is subject to the privacy protocols of Statistics NZ.

23. Sir Peter Gluckman's research notes that there are also circumstances where identifiable client level data may be used and therefore appropriate data governance, safeguards, accountability and oversight must be in place to ensure social acceptability and the social license for the use of big data.[30] According to the discussion paper, in order to address the multiple uses of data, the Government Statistician, the Privacy Commissioner, the Chief Science Advisor and the Data Futures Programme[31] are working together to recommend an assurance and governance system for data access and use.

24. Countervailing privacy risks associated with policies that enable the state access to and use of client level data were addressed by the Privacy Commissioner in a major 2017 inquiry and report on a controversial policy of the previous government to require NGOs to disclose individual client level data to the Ministry of Social Development as a condition of their funding contracts.[32] The contracts were linked to MSD's four service lines – Work and Income, Child, Youth and Family, Family and Community Services, and the Ministry of Youth Development, including services that have a children, young person, family or whanau focus.[33] The coercive nature of the policy was of considerable concern to many NGO service providers working in those sectors.

---

[27] Using Evidence to Inform Social Policy: The Role of Citizen-based Analytics, A discussion Paper, Sir Peter Gluckman, 19 June 2017, http://www.pmcsa.org.nz/wp-content/uploads/17-06-19-Citizen-based-analytics.pdf.
[28] http://archive.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure.aspx
[29] Enhanced evidence-informed policy making, A report by the Prime Minister's Chief Science Advisor, July 2017 http://www.pmcsa.org.nz/wp-content/uploads/17-07-07-Enhancing-evidence-informed-policy-making.pdf
[30] Ibid.
[31] The Data Futures Programme is an independent group funded by the New Zealand Government that identified challenges in the data-use system and facilitates conversation with New Zealanders to understand their perspectives on data use in order to develop guidelines to help organisations build and maintain trust of those whose data they wish to use, http://datafutures.co.nz/our-work-2/.
[32] Office of the Privacy Commissioner, Inquiry into the Ministry of Social Development's Collection of Individual Client-level Data from NGOs, https://www.privacy.org.nz/assets/Files/Reports/2017-04-04-Inquiry-into-MSD-collection-of-individual-client-level-data-OPC-report.pdf
[33] Ibid., para. 3.3.4.

25. The Privacy Commissioner accordingly utilised his statutory function under s 13 of the Privacy Act to undertake a self-directed inquiry into the policy. The Commissioner concluded that the policy was inconsistent with the Privacy Act.[34] He noted, among other things, that while the Government can legitimately require good information from its providers in order to evaluate the efficacy of a funded programme, the proposed policy was "excessive, disproportionate to the Government's legitimate needs and therefore…inconsistent with the information privacy principles."[35] He also noted that "the manner in which the policy change has been effected risks undermining the trust between individual service users and NGOs" and may accordingly "deter some of the most in need from accessing necessary help."[36] The Privacy Commissioner accordingly recommended that the policy be amended to conform with the IPPs under the Privacy Act.[37] Subsequently, the policy appears to have discontinued.

B. Predictive risk modelling, including in the child welfare sector

26. In New Zealand, the development of a proposed predictive risk modelling (PRM) programme in the child protection sector has significant implications for children's privacy rights. The aim of the proposed programme, developed by the Ministry of Social Development (MSD), is to identify children at risk of maltreatment as they enter the public welfare system in order to target interventions and service delivery. PRM is generated from a large data set of public welfare and child protection services information. An algorithmic program is applied to the data to generate 'risk' scores for individuals. Service responses are then ascertained according to the risk score.

27. Concerns have been raised about the ethics and human rights implications of PRM including in relation to the security of information; unanticipated uses of information; stigmatisation of people identified as having high risk scores; systematic discrimination occurring as a result of the algorithmic techniques used to filter data; and transparency in relation to the data used to create algorithmic design. In order to ensure that privacy, human rights and ethical considerations are factored into the development and implementation of PRM, MSD is currently developing a Privacy, Human Rights and Ethics (PHRAE) Framework as a procedural safeguard. More information on this initiative is set out below at paragraphs 35 and 36.

28. The advent of this approach has coincided with extensive reforms to the legislation governing New Zealand's child protection and youth justice jurisdictions. The Children, Young Person's

[34] Ibid, Executive Summary at point 8.
[35] Ibid., para 4.2.
[36] Ibid, Executive Summary, at point 5
[37] Ibid, point 8.

and their Families Act and Young Persons (Oranga Tamariki) Legislation Act has greatly expanded the powers of specified government agencies to share and use personal information held about children and their families, including enabling the creation of combined data sets.[38] In doing so, legislation expressly provides for a principle that the well-being and best interests of a child will generally take precedence over any duty of confidentiality owed to the child or young person or a member of the child's family.[39]

29. This is an example of primary legislation being used to over-ride the information privacy principles that otherwise would have applied under the Privacy Act in respect of sharing of personal information between agencies.[40] Other PRM initiatives, such as one that was directed at identifying young people at risk of long-term benefit dependency,[41] have relied upon Approved Information Sharing Agreements (AISAs) being ratified under the requirements of the Privacy Act in order to proceed. The Privacy Act provides for a number of procedural safeguards in respect of the development of AISAs. These are set out in more detail below at paragraph 34.

30. More generally, New Zealand academics at the University of Otago have commented on the use of PRM tools used by the Accident Compensation Corporation, New Zealand's government entity responsible for administration of the accidental injury compensation scheme. The academics found that the practice raised a number of fundamental questions that the government ought to be able to address when considering the implementation of PRM.[42] These questions include whether:

    a. The PRM tool is accurate – this requires both transparent evaluation processes and a thorough description of the data set on which it was assessed
    b. The responsible agency can explain how the PRM tool works so that clients can appeal a decision made by it
    c. The PRM tool distorts the way the agency pursues its policy objectives

[38] Children, Young Persons and the Families (Oranga Tamariki) Legislation Act 2017, Clause 41 (ss 65A-66Q) http://www.legislation.govt.nz/act/public/2017/0031/latest/DLM7064591.html (NOTE: at the date of writing it is still to commence).
[39] Clause 41, new s 66(2).
[40] See Office of the Privacy Commissioner submission on Oranga Tamariki Bill, https://privacy.org.nz/assets/Files/Reports-to-ParlGovt/Submission-on-the-CYPF-Oranga-Tamariki-Legislation-Bill.pdf.
[41] https://www.hrc.co.nz/files/7914/6483/4019/16g_Human_Rights_Commission_feedback_on_draft_Youth_Service_AISA.pdf.
[42] http://www.otago.ac.nz/humanities/news/otago664403.html.

d. The PRM tool enables the agency to 'duck' its responsibility to make fair and humane decisions
e. The PRM tool implicitly discriminates against individuals – evaluative processes should be used to identify whether this is the case
f. The responsible agency is effectively training employees in the use of the PRM tool and associated decision-making system

C. Procedural and institutional safeguards, oversight mechanisms and remedies

Informational Privacy

31. Under the Privacy Act, the Privacy Commissioner has the power to investigate a matter that is or may constitute interference with privacy. An example of this type of investigation is the inquiry into individual client level data referred to in paragraph 25.[43] The Privacy Commissioner can also receive complaints under the Act from anyone who believes that they are affected by a breach of the privacy principles. The Commissioner will then investigate whether the public or private sector agency has breached the Act.[44] If the complainant does not obtain a satisfactory outcome, they can take case to the Human Rights Review Tribunal which has the power to grant remedies including a declaration of interference with the right to privacy, an order that the agency should not repeat the behaviour or should redress any loss or damages, and compensation.[45]

32. In addition to the functions above, the Privacy Bill provides for new accountability mechanisms through the following new measures:

a. *Mandatory reporting of data breaches:* One of the major changes under the Bill is the introduction of a mandatory requirement for agencies to report privacy breaches to the Privacy Commissioner and affected individuals if the breach has caused or risks causing harm.[46] This is consistent with mandatory reporting regimes that are

[43] Privacy Act 1993, Part 8.
[44] For example, in April 2018, the Privacy Commissioner found that Facebook breached the Privacy Act because it failed to: properly respond to the complainant's request for information, acknowledge it was subject to the Privacy Act, and cooperate with the Commissioner's investigation and statutory demand for information. The Commissioner publicly named Facebook in accordance with his office's naming policy after first providing Facebook with an opportunity to comment on this finding https://privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/.
[45] See Privacy Act 1993, s 85.
[46] Privacy Bill, Clause 119. Harm is defined as an action that (i) has caused, or may cause, loss, detriment, damage, or injury to the individual; or (ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual; or (iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.

increasingly required in privacy legislation, including in Australia, Canada and the European Union. Notification must occur as soon as practicable after an agency becomes aware of a breach, and if it is not reasonably practicable to notify affected individuals, the agency must instead give public notice of the breach. It is an offence to fail to notify the Commissioner, with a maximum penalty of $10,000[47] and the Commissioner has the power to publish the identity of an agency that has notified him or her of the privacy breach, if the agency consents or if the Commissioner is satisfied that it is in the public interest to do so.[48]

b. *Compliance notices:* The Commissioner's functions are expanded under the new Bill. It allows the Commissioner to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with privacy law.[49] The Human Rights Review Tribunal will be able to enforce compliance notices and hear appeals.[50]

c. *Information-gathering powers:* The Bill expands the Commissioner's information-gathering powers when investigating complaints about an interference of privacy. The Commissioner can require any person to provide information or documents and can specify a time limit for providing information.[51]

d. *Access requests:* The Commissioner is also given a new power to direct an agency to confirm whether it holds specified information about an individual, permit access to that information or to make the information available in a particular way.[52] Under the current law, the Commissioner would be required to refer the issue to the Director of Human Rights Review Tribunal to make an access direction.

Harmful Communications

33. The Harmful Digital Communications Act sets out ten communication principles, including the principle that "a digital communication should not disclose sensitive personal facts about an individual."[53] An individual can make a complaint to Netsafe, the approved agency under the Act, if he or she believes that one of the principles has been breached. Netsafe will then

[47] Privacy Bill, Clause 122.
[48] Privacy Bill, Clause 123.
[49] Privacy Bill, Clause 124.
[50] Privacy Bill, Clause 130.
[51] Privacy Bill, Clause 92.
[52] Privacy Bill, Clause 96.
[53] http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#whole.

work with parties to find a resolution. However, if parties cannot agree, the agency will refer cases to the District Court. The Court can make a range of orders including for removal of content and for an apology to be published.[54] The Act also provides for criminal liability when a person does not comply with an order or when a person posts a digital communication with the intention that it cause harm and harm actually results.

Approved Information Sharing Agreements

34. In 2013, the Privacy Act was amended to introduce Approved Information Sharing Agreements (AISAs) which are the legal mechanism that authorises the sharing of information about an individual by one government agency to another, usually for a purpose unrelated to the reason for which the information was originally collected or provided. Currently, there are seven AISAs in place.[55] The Privacy Act provides for procedural safeguards in the formation of AISAs as well as continued oversight, including:

    a. Agencies must consult the Privacy Commissioner, any person or organisation representing the interests of the people whose information will be affects and any other person that the agencies consider should be consulted.[56]
    b. The Minister must be satisfied of a number of factors including that the AISA does not unreasonably impinge on privacy and it contains adequate safeguards.[57]
    c. The Privacy Commissioner also has the power to prepare a report on any privacy matters relating to the AISA.[58]

Privacy, Human Rights and Ethics Framework

35. In response to concerns relating to predictive risk modeling, the Ministry of Social Development has been developing a Privacy, Human Rights and Ethics (PHRAE) Framework to apply to proposed PRM and other data sharing initiatives. At the time of writing both the child protection PRM initiative and the PHRAE Framework are still under development and yet to be implemented. At this stage, it is understood that the PHRAE

[54] For more information see https://www.consumerprotection.govt.nz/consumer-law-and-your-rights/online-safety/harmful-digital-communications-act/.
[55] For example: Inland Revenue Department (IRD) and the Department of Internal Affairs to share information from adult passport applications with IRD for the purpose of contacting overseas-based student loan borrowers and child support liable parents who are in arrears; IRD and the New Zealand Police regarding disclosure of information for the purpose of prevention, detection, investigation or providing evidence of serious crime.
[56] Privacy Act 1993, section 96O.
[57] Privacy Act 1993, section 96N.
[58] Privacy Act 1993, section 96P.

framework is intended to be a policy-level process that will be undertaken by Ministry officials and is not intended to be vested under any specific legislative or regulatory provision.

36. It is notable that in 2016 the UN Committee on the Rights of the Child recommended that the New Zealand Government ensure "that 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."[59]

Intelligence and Security

Ministerial Policy Statements

37. Under the Act, Ministers responsible for the security and intelligence agencies must issue ministerial policy statements (MPS) to provide guidance on specific matters that security agencies must apply. The ten MPSs that been issued to date adopt a human rights-based approach to decision making each including a provision that their purpose "to ensure security and intelligence agencies functions are performed in accordance with New Zealand law and all human rights obligations recognised by New Zealand law." The principles in the MPS are based on the international human rights framework relating to the right to privacy, including a requirement for the assessment of the principles of legality, necessity and proportionality, as well as the need for effective oversight.

38. In particular, the MPS on Cooperation of New Zealand intelligence and security agencies with public overseas authorities adopts a strong human rights approach for the exercise of due diligence when determining whether it is appropriate to engage with a particular overseas public authority and determining whether proposed activities are consistent with the law, particularly with respect to ensuring that the security agencies do not become complicit in human rights abuses. The MPS lists the ICCPR and seven other ratified UN human rights treaties as being among New Zealand's "core human rights obligations." The MPS noted that "actions or activities that run contrary to the obligations within those instruments may constitute a human rights breach in the context of this MPS."

39. In terms of human rights obligations, security agencies must not cooperate with overseas public authorities where they know or assess that there is a real risk that the activity will lead to or has been obtained as a result of human rights breaches in that country. This includes a

[59] UN Committee on the Rights of the Child, *Concluding observations on the fifth periodic report of New Zealand*, CRC/C/NZL/CO/5 (21 October 2016) paras 20(a) and 20(b) http://www.refworld.org/docid/587ceb574.html.

duty of due diligence and this applies to requests to share intelligence on a case-by-case basis or within the context of a broader standing authorisation.

Inspector General of Intelligence and Security (IGIS)

40. The Intelligence and Security Act 2017, gives the IGIS the power to inquire into complaints by individuals who claim they have been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency.[60] During an inquiry the IGIS may compel giving of information, take evidence from witnesses in private, summon and examine under oath any person who is able to give information relevant to the inquiry. On the completion of the inquiry, the IGIS must prepare a written report containing his or her conclusions and recommendations which may include recommendations that the agency for the redress including remedies that involve the payment of compensation.[61] The report is published publicly and the report or findings cannot be challenged or reviewed or called into question by a court except on the grounds that of lack of jurisdiction.[62]

41. Other intelligence and security oversight mechanisms include the Chief Commissioner of Intelligence Warrants who considers applications (jointly with the Minister) for any warrant that targets a New Zealander and makes application by agencies to access "restricted information" that is subject to strict statutory restrictions; and the Intelligence and Security Committee, the parliamentary oversight committee for the intelligence agencies. The Committee's functions include examining policies of security agencies; considering bills or petitions relating to security agencies, and requesting the Inspector-General to conduct inquiry into any matter relating to compliance with NZ law, including human rights law and proprietary of activities.

Legislative

Legislative Advisory Committee Guidelines

42. Chapter 7 of the Legislation Advisory Committee (LAC) Guidelines on Process and Content of Legislation (LAC Guidelines), directs government officials as to their legal and ethical obligations regarding privacy and personal information when developing legislation.[63]

[60] Intelligence and Security Act 2017, s 171. The most common type of complaints relate to adverse recommendations by the NZSIS as to security clearances required for employment, http://www.igis.govt.nz/complaints/.
[61] Intelligence and Security Act 2017, s 185.
[62] Intelligence and Security Act 2017, section 190.
[63] The Guidelines provide: "The Government should respect privacy interests and ensure that the collection of information about people is done in a transparent manner, where the type and amount of information collected and

43. The LAC Guidelines provide that if proposed legislation affects the privacy of individuals, the Privacy Commissioner and the Government Chief Privacy Officer (GCPO)[64] should be consulted. Ministers and their officials are required to advise Cabinet of aspects of Bills that depart from principles in the Guidelines. The Guidelines also provide that if any policy development involves personal information then a Privacy Impact Assessment (PIA) should be carried out to assess the extent of the impact and how it can be managed in the policy development process. The Office of the Privacy Commissioner has produced guidance on whether a PIA is needed; and on how to complete a PIA. According to the PIA guidance, organisations should check that the legal framework complies with the principles in the Privacy Act; identify privacy risks and how to mitigate them, and produce and then act on a PIA report.[65]

Cabinet Office Manual

44. The Cabinet Office Manual requires that Ministers must confirm that bills comply with "the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993, the principles of the Privacy Act 1993 and international obligations.[66]

what is done with that information is clearly explained. Maintaining the community's trust that government will respect privacy interests is key to the Government's ability to collect the information it needs to provide many public services." http://www.ldac.org.nz/guidelines/lac-revised-guidelines/chapter-7/.

[64] The GCPO's role is to provide expert guidance and internal advice on privacy issues to the Government: https://www.ict.govt.nz/governance-and-leadership/the-gcio-team/government-chief-privacy-officer/.

[65] https://www.privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Assessment-Part-2-FA.pdf.

[66] Cabinet Office Manual 2017, para. 7.65 https://dpmc.govt.nz/sites/default/files/2017-06/cabinet-manual-2017.pdf.