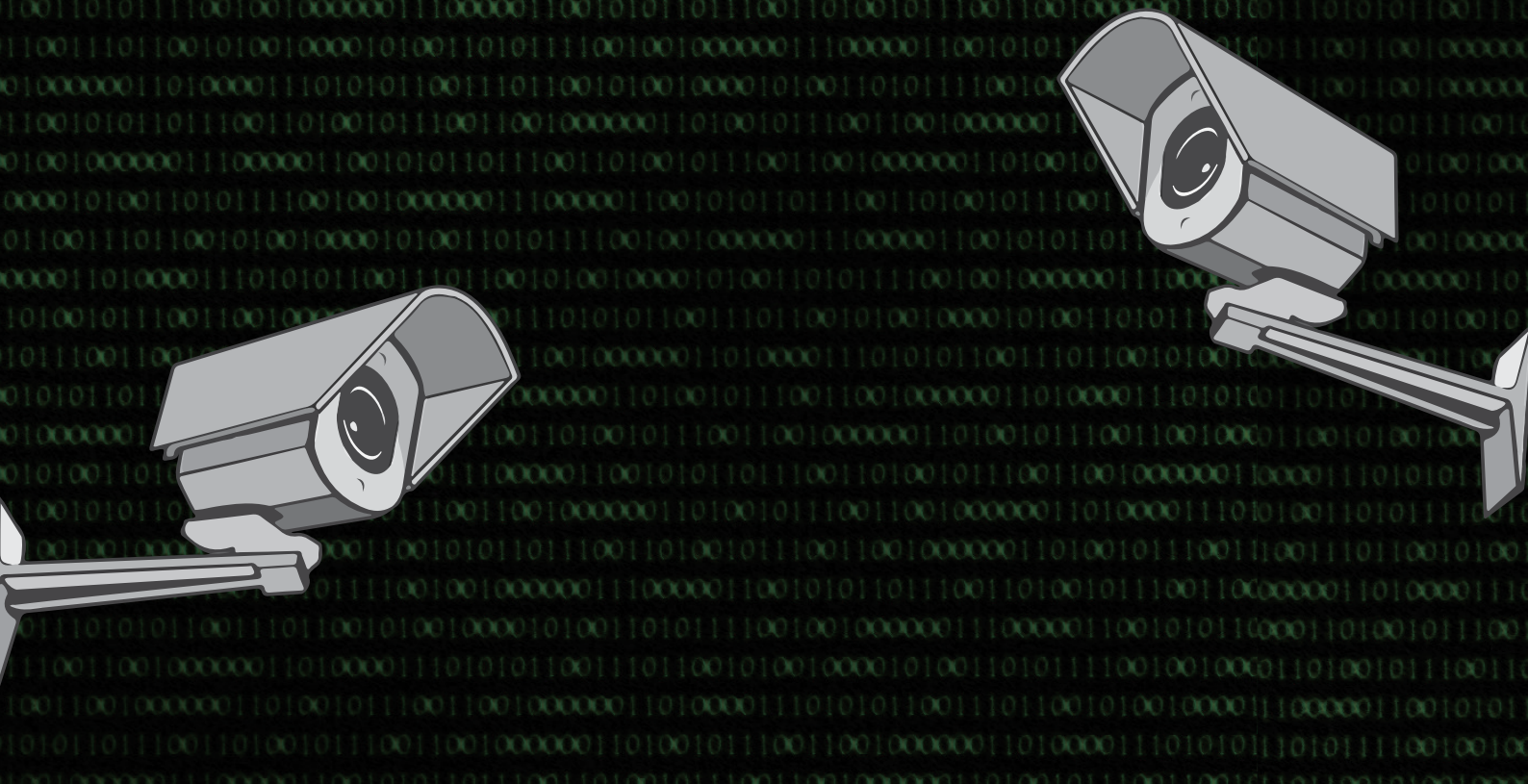
NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

# Privacy, Data and Technology: Human Rights Challenges in the Digital Age

A paper issued by the New Zealand Human Rights Commission

May 2018



**Privacy, Data and Technology: Human Rights Challenges in the Digital Age**

**A paper issued by the New Zealand Human Rights Commission**


Printed in Auckland, New Zealand

The Human Rights Commission was set up in 1977 and works under the Human Rights Act 1993. Our purpose is to promote and protect the human rights of all people in Aotearoa New Zealand. We work for a free, fair, safe and just New Zealand, where diversity is valued and human dignity and rights are respected.

For more information, please visit our website: www.hrc.co.nz

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

# CONTENTS

# ACRONYMS

AI ..... Artificial Intelligence
APEC ..... Asia-Pacific Economic Cooperation
BORA ..... New Zealand Bill of Rights Act
DFP ..... Data Futures Partnership
ECtHR ..... European Court of Human Rights
EU ..... European Union
GCSB ..... Government Communications Security Bureau
ICCPR ..... International Covenant for Civil and Political Rights
IGIS ..... Inspector-General of Intelligence and Security
IPPs ..... Information Privacy Principles
MSD ..... Ministry of Social Development
NZSIS ..... New Zealand Security Intelligence Services
OECD ..... Organisation for Economic Cooperation and Development
OHCHR ..... Office of the High Commissioner for Human Rights
PIA ..... Privacy Impact Assessment
PRM ..... Predictive Risk Modelling
SR ..... Special Rapporteur
UNHRC ..... United Nations Human Rights Committee
UN ..... United Nations
UNGPs ..... United Nations Guiding Principles on Business and Human Rights

## INTRODUCTION

Digital technology is integrating into our everyday lives at an ever-increasing rate. The digital interface is now the conduit for many of our interactions and activities and has altered, probably irreversibly, the way that we communicate and socialise with one another.

We produce vast amounts of data about ourselves in a variety of contexts through our use of smart phones and social media, our consumer activity, our use of on-line search engines, and our interactions with public services and institutions.

***Digital technology has created a symbiotic relationship of sorts. It enables us to access and share information for our own benefit. At the same time, the data we generate is of immense value to the public and private entities that facilitate and control our digital interactions.***

In this respect, digital technology has created a symbiotic relationship of sorts. It enables us to access and share information for our own benefit. At the same time, the data we generate is of immense value to the public and private entities that facilitate and control our digital interactions.

While this has the potential to produce great benefits and improve social outcomes, it also poses risks to our fundamental human rights. The surveillance and collection of vast amounts of personal information and meta data, and the processing of such data using new analytical techniques, has major implications for our right to privacy and our right to be free from discrimination.

The impact of digital technology on the right to privacy is of particular significance. Privacy is central to our enjoyment of personal dignity and autonomy. It enables the expression of individuality, facilitates trust, friendship and intimacy, empowers the individual against the state and is necessary for securing other human rights, such as the right to freedom of expression and opinion.

This paper provides a high-level summary of the key international and domestic human rights standards and principles that can guide legal and policy frameworks in responding to the rapid advance of digital technology. It is intended to assist anyone in New Zealand engaging in advocacy, research, policy or legislative development in this area, as well as those with a general interest in these issues.

Part I of the paper sets out the international human rights framework that applies to surveillance and personal data, with a focus on the right to privacy. Part II provides an overview of the legal and policy framework that applies in New Zealand and Part III outlines the permissible limitations on the right to privacy. Part IV discussed the safeguards that States should put in place to prevent adverse human rights impacts. This is followed by an overview of the remedies available for human rights violations relating to surveillance and personal data in Part V. The paper concludes with a focus on some of the emerging human rights challenges arising in the digital age.

These emerging challenges include the responsibilities of private businesses in this area. While governments are primarily responsible for protecting human rights, businesses also have a duty to respect human rights, as set out in the United Nations Guiding Principles on Business and Human Rights (UNGPs). While this paper touches on the UNGPs, it is mainly focused on public sector obligations. Nevertheless, we hope that businesses and other private sector

and non-government organisations find it a useful point of reference when considering the broad implications of their practices and policies concerning the use and protection of personal data.

# PART I: INTERNATIONAL HUMAN RIGHTS FRAMEWORK

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

The collection, storage, sharing and re-purposing of personal information, whether obtained by surveillance or interception, or freely provided by individuals, poses a challenge to universally recognised human rights.

International human rights law provides an instructive framework for the protection of the affected rights, including the right to privacy and its permissible limitations, freedom of expression and opinion, freedom of association, the right to be free from discrimination, and the right to be free from unreasonable search and seizure.

***The right to privacy is a fundamental human right, guaranteed under Article 12 of the Universal Declaration on Human Rights and Article 17 of the ICCPR.***

The first part of this paper is intended to provide readers with an overview of the international law and standards relevant to:

- Affected rights under the International Covenant for Civil and Political Rights (ICCPR)
- United Nations resolutions and reports on human rights in the digital age
- International and regional guidelines and standards regarding personal information

Together, these instruments, reports and standards provide a framework to guide the formation of law and policy concerning personal data, surveillance and human rights in New Zealand.

## 1.1 International Covenant for Civil and Political Rights

The right to privacy is a fundamental human right, guaranteed under Article 12 of the Universal Declaration on Human Rights and Article 17 of the ICCPR. In 1978, New Zealand agreed to be legally bound by the ICCPR. Article 17 of the Covenant affirms:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

In reflection of its status as a fundamental right, the right to privacy is included in similar terms in other international human rights treaties to which New Zealand is a party, protecting the rights of children, and people with disabilities.[1] The scope of the right under article 17 is broad. It not only protects individual privacy, but also interference with the individual's family and home life, written affairs, personal identity and standing. This illustrates how closely the right is linked to the human rights concepts of personal autonomy and dignity.[2] The right to privacy is also underpinned by a right to legal protection from arbitrary and unlawful interference.

The UN Human Rights Committee (UNHRC), the UN body of independent experts that monitors the implementation of the ICCPR, has issued interpretative guidance on the nature and scope of the right to privacy under article 17 in its General Comment No. 16. The UNHRC sets the following threshold for State compliance with the right to privacy:

> *In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they*

1 Convention on the Rights of the Child, Article 16; and Members of Their Families, Article 14; Convention on the Rights of Persons with Disabilities, Article 22.

2 On this point, see the observations of the UN Special Rapporteur on the right to privacy concerning the recognition of the relationship between privacy and personality, A/71/368 (30 August 2016) para. 40 http://undocs.org/A/71/368

*emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.*[3]

In other words, a robust legal framework that protects the right to privacy as a free-standing right and provides measures to prohibit and sanction breaches of the right, is a minimum requirement for State parties to the ICCPR to meet.

This was illustrated in the most recent review of New Zealand's compliance with the ICCPR, in which the UNHRC expressed concern that the right to privacy is not protected as a free-standing right in New Zealand legislation.[4] More specifically, the UNHRC expressed concern that surveillance activities carried out under New Zealand's intelligence and security legislation (at that time) lacked sufficient oversight and safeguards mechanisms, and did not meet the requirements of Article 17.[5] Similarly, the UN Committee on the Rights of the Child has recommended that New Zealand social sector policies that impact upon privacy rights fully protect the right to privacy and are included in relevant legislation.[6]

The right to freedom of expression and the right to hold opinions without interference, affirmed under article 19 of the ICCPR are also important. As stated in the preamble to the Global Principles on the Protection of Freedom of Expression and Privacy:

*Without privacy, individuals lack the space to think and speak without intrusion and to develop their own voice. Without freedom of expression, individuals would be unable to develop their sense of self. At the heart of the protection of these rights lies the respect for, and protection of, human dignity and individuals' ability to live freely and engage with one another.*[7]

The application of algorithms to data to predict future behaviour or generate risk assessments to inform social spending may also implicate the right to be free from discrimination under Article 26 of the ICCPR. This issue will be discussed further below.

## 1.2 International Resolutions, Reports & Groups

The UNHRC's interpretation of the right to privacy in General Comment 16 is now approaching 30 years old. While its principles are still applicable, it does not specifically address the challenges that have arisen from the information technology revolution over that period.[8]

In recent years UN human rights entities such as the Human Rights Council[9], General Assembly[10], Special Rapporteurs[11] and the Office of the High Commissioner for Human Rights (OHCHR)[12] have produced numerous reports and resolutions on the human rights challenges brought about by the digital age. The principles and recommendations contained in these documents contribute to the international jurisprudence on the right to privacy and, as such, provide an important reference point when assessing the rights-consistency of domestic policies and practices that utilise digital technologies to gather, share and assess personal data.

3 UNHRC, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988)

4 UNHRC, Concluding Observations: New Zealand, CCPR/C/CO/NZL/6 (27 April 2016) para. 15 http://tbinternet.ohchr.org/_layouts/treaty-bodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNZL%2f-CO%2f6&Lang=en.

5 Ibid., para 16.

6 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

7 The Global Principles were written by Article 19, an NGO dedicated to upholding the freedom to speak and the freedom to know

8 There have accordingly been calls for the UNHRC to update its General Comment on the right to privacy.

9 The UN Human Rights Council is an inter-governmental body within the United Nations system made up of 47 States responsible for the promotion and protection of all human rights around the world.

10 The UN General Assembly is made up of all 193 Member States of the UN and is a forum used to work together and discuss a wide array of international issues covered by the UN Charter, such as development, peace and security, and international law.

11 UN Special Rapporteurs are independent human rights experts with mandates to report and advise on human rights from a thematic or country-specific perspective.

12 The UN OHCHR is the principal UN body that is committed to the promotion and protection of universal human rights.

## UN General Assembly and Human Rights Council

In December 2013, the UN General Assembly adopted its first resolution on the right to privacy in the digital age. The development of the resolution followed the 2013 Snowden revelations that the National Security Agency (NSA) in the United States and the General Communications Headquarters (GCHQ) in the United Kingdom were undertaking extensive surveillance and interception of global internet traffic, digital personal information records and metadata. [13]

The resolution expressed "deep concern at the negative impact that surveillance and interception of communications may have on human rights." In doing so, it emphasised the need for States to:

- Respect and protect the right to privacy;
- Review domestic practices and laws regarding communications surveillance, interception and collection of personal data in line with international human rights obligations;
- Establish effective oversight mechanisms; and
- Ensure that any practice that limits or interferes with the right to privacy is subject to a "careful and critical assessment" of its necessity, legitimacy and proportionality, in accordance with international law.[14]

Two further resolutions on the right to privacy in the digital age were adopted by the General Assembly in 2014 and 2016. Both resolutions reaffirmed and built upon the principles established in the 2013 resolution and included additional calls for:

- States to provide access to an effective remedy for individuals whose rights have been violated by the use of unlawful or arbitrary surveillance; and[15]
- Business enterprises to respect human rights in accordance with the UN Guiding Principles on Business and Human Rights; to establish transparency policies; and to take measures to enable secure communications and protect customers from interference with their privacy.[16]

On 1 April 2015, the Human Rights Council adopted a similar resolution on the right to privacy in the digital age. The resolution reflected the General Assembly's resolutions and, in recognition of the global nature of the internet and rapid advancement of information and communication technology, affirmed that "the same rights that people have offline must also be protected online."[17] Most significantly, the resolution established the role and mandate of the Special Rapporteur on the right to privacy, an independent expert appointed by the Human Rights Council to examine and report back on a country situation or a specific human rights theme in relation to the right to privacy.[18]

In March 2017, the Human Rights Council adopted an updated resolution on the same issue that reflects many of the points made in the General Assembly resolutions.[19]

## UN Reports

Since 2013, the OHCHR and several Special Rapporteurs have produced reports that further extrapolate the international human rights standards relevant to the interception, surveillance and sharing of digital communications. The reports of the Special Rapporteurs examine specific practices and are applicable to related policy development by

13 See Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37 (30 June 2014) paras. 4-5

14 General Assembly Resolution, Right to Privacy in the Digital Age, A/RES/68/167 (18 December 2013) http://undocs.org/A/RES/68/167.

15 General Assembly Resolution, Right to Privacy in the Digital Age, A/RES/69/166 (18 December 2014) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166.

16 General Assembly Resolution, Right to Privacy in the Digital Age, A/RES/71/199 (19 December 2016) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199

17 Human Rights Council Resolution, The right to privacy in the digital age, A/HRC/RES/28/16 (1 April 2015) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/28/16.

18 In July 2015, Professor Joseph Cannataci was appointed to this role. See http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

19 Human Rights Council Resolution, The right to privacy in the digital age, A/HRC/RES/34/7 (7 April 2017) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7

governments. The most relevant reports that are referenced throughout this paper include:

- OHCHR
  - » Report on the right to privacy in the digital age (30 June 2014)[20]
- Special Rapporteur on the right to privacy
  - » Report to the Human Rights Council providing an overview of the right to privacy (24 November 2016);[21]
  - » Report to the Human Rights Council outlining first approaches to a more privacy-friendly oversight of government surveillance (24 February 2017)[22] and
  - » Report to the General Assembly on Big Data and Open Data (19 October 2017).[23]
- Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism
  - » Report to the General Assembly examining the use of mass digital surveillance for counter-terrorism purposes and the implications of bulk access technology for the right to privacy (24 September 2014).[24]
  - » Report to the General Assembly examining surveillance of electronic communications data in the counter-terrorism context (11 August 2017).[25]
- Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
  - » Report to the Human Rights Council analysing the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression (17 April 2013)[26]
  - » Report to the Human Rights Council addressing the roles played by private actors engaged in the provision of Internet and telecommunications access and providing principles to guide the private sector on human rights in the digital sector and new modalities of surveillance (30 March 2017).[27]

## International legal framework to regulate surveillance in cyberspace

The Special Rapporteur on the right to privacy has collaborated with the European Union-supported Management Alternatives for Privacy, Property and Internet Government, otherwise known as the MAPPING project, on issues relating to the "protection of privacy in this age of ubiquitous surveillance."[28] The collaboration led to the development of a draft legal instrument on surveillance.[29] The document is expected to be ready for consideration by the Human Rights Council by 2021 and may compromise "soft law" in the form of recommendations or an international multilateral treaty. [30]

## D7 – Digital Rights Working Group

The New Zealand Government is to lead an international working group on digital rights, made up of New Zealand, United Kingdom, South Korea, Estonia and Israel, Uruguay and Canada.[31] The Group's aim is to enable the digital environment to meet human rights standards and protections through the creation of a multi-national framework for digital rights.[32]

20 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37 (30 June 2014) http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

21 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64 (24 November 2016) https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf?OpenElement.

22 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/34/60 (24 February 2017) para 25 http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

23 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/72/34103 (19 October 2017) http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

24 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, A/69/397 (23 September 2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.

25 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, A/72/316 (11 August 2017) http://undocs.org/A/72/316.

26 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40 (17 April 2013)

27 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/35/22 (30 March 2017). http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22.

28 https://mappingtheinternet.eu/about.

29 http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22762&LangID=E

30 See Statement by Mr. Joseph Cannataci, Special Rapporteur on the right to privacy, 6 March 2018, Human Rights Council 37th session, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22858&LangID=E

31 The group originally comprised of five countries, including New Zealand, known as the Digital 5. However, Uruguay and Canada joined in 2018. For more information see https://www.digital.govt.nz/digital-government/international-partnerships/d7-group-of-digital-nations/

32 See https://www.beehive.govt.nz/release/leading-digital-nations-put-digital-rights-heart-their-agenda

## 1.3 Data Privacy Guidelines and Principles

Essential to the right to privacy is the right to protection of personal data. The Organisation for Economic Co-operation and Development (OECD), European Union (EU) and Asia-Pacific Economic Forum (APEC) have developed guidelines and regulations on this issue which influence domestic privacy laws in New Zealand.

### OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The OECD Guidelines were developed by OECD Member countries in 1980 and were revised in 2013.[33] The Guidelines were formed to help harmonise national privacy legislation and, while upholding human rights, at the same time prevent interruptions in international flows of data. The Guidelines set out eight core principles that apply to the processing of personal data. They form the basis of the information privacy principles in New Zealand's Privacy Act 1993 and consist of the follow key principles:

- Collection Limitation Principle: Personal data should only be collected lawfully and fairly and where appropriate with knowledge and consent of the individual concerned.[34]
- Purpose Specification Principle: The purposes for which personal data are collected should be specified at the time of or before data collection. Subsequent use of such data is limited to the purpose of collection or a compatible purpose and that these should be specified whenever there is a change of purpose.[35]
- Use Limitation Principle: Restricts the disclosure of personal information for reasons other than the specified purpose except with the individual's consent or by legal authority.[36]

Other principles in the Guidelines include:

- personal data should be protected by reasonable security safeguards; governments should be open about policy developments and practices with respect to personal data; individuals should be able to request data about themselves and receive reasons for denial of such requests; and that data controllers should be accountable for complying with the principles.[37]

### European Union

*Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*

The Council of Europe Convention was the first binding international instrument to protect individuals against abuses resulting from the collection and processing of personal data and to regulate the trans-border flow of personal data.[38] Many of the principles reflect those of the OECD Guidelines. Countries from outside Europe can sign up to the Convention, but only Uruguay has done so to date.

*General Data Protection Regulation (GDPR)*

The EU also has its own internal law regarding data protection. On 8 April 2016, the EU adopted the GDPR which takes effect on 25 May 2018.[39] The GDPR applies to the public sector, EU-based entities and non-EU based entities processing data of individuals within the EU. As noted by New Zealand's Privacy Commissioner, the GDPR's "standards lift the baseline internationally in response to challenges to consumers and data protection in today's global digital economy."[40]

Some of the key aspects of the GDPR are set out below:[41]

- Increased territorial scope: Applies to all companies (data controllers or processors) whose processing activities relate to offering goods or services or monitoring behaviour

33 New Zealand has been an OECD Member since 1973. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacy-andtransborderflowsofpersonaldata.htm

34 OECD Guidelines, Article 7

35 Ibid. Article 9

36 Ibid. Article 10

37 Ibid. Articles 10-14

38 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

39 GDPR will replace the current EU Directive and will be directly applicable on all Member States without the need for implementing national legislation. See Regulation at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

40 Privacy Commissioner, Office of the Privacy Commissioner Briefing for the Incoming Minister of Justice: Hon Andrew Little, October 2017, para 2.1 https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf

41 See https://www.eugdpr.org/key-changes.html.

of individuals residing in the EU, regardless of the company's location.

- Data Protection Officers: In some circumstances data controllers or processors must designate a Data Protection Officer as part of their accountability programme. This covers processing carried out by a public authority, where core activities are involved, monitoring data subjects on a large scale; and where core activities consist of processing on a large scale of special categories of data.

- Consent: Restrictive approach to consent requiring that it must be "freely given, specific, informed and unambiguous."

- Penalties: A tiered approach to penalties is established with fines for some infringements of up to the higher of 4% of annual worldwide turnover and EUR20 million (e.g. breach of requirements relating to international transfers or the basic principles for processing, such as conditions for consent). Civil liability is also possible with a right to compensation.

- Data breach notification: Data controllers must notify most data breaches to the Data Protection Authorities within 72 hours of awareness.

- Data subject rights: Rights of individuals are bolstered including rights to: require information about data being processed about themselves; be forgotten entitling individuals to have personal data about them erased; correction of data which is wrong; a right to restrict certain processing; object to their personal data being processed for direct marketing purposes; and to an explanation about information based on algorithms.

The GDPR may impact on New Zealand in two ways. First, any public agency or business in New Zealand that handles personal data of individuals residing in the EU will need to ensure that their internal data processing procedures comply. Second, it is possible that the EU may find that New Zealand's data protection laws are no longer 'adequate' for the transfer of European-originated data for processing.[42] The Office of the Privacy Commissioner has indicated that they are in regular communication with the European Commission on this issue.[43]

## Asia-Pacific Region

*APEC Privacy Framework*

The APEC Privacy Framework was developed in light of the 1980 OECD Guidelines and applies to all 27-member countries.[44] The Framework sets out principles and implementation guidance for the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information. Key principles include:

- Preventing harm: Preventing misuse of personal information and consequent harm to individuals.
- Notice: Individuals should know that information is collected about them and the purpose for which it is used.
- Collection limitation: Limited collection of information to the purposes for which it is collected.
- Use limitation: Limits the use of personal information to fulfilling the purposes of the collection.

Also included in the framework are the principles of choice and consent, data integrity, security safeguards, access and correction and accountability. Progress on the implementation of the Framework includes the application of Information Privacy Individual Action Plans by 14 economies. New Zealand last updated its Data Privacy Individual Action Plan, in 2011.[45]

*Comprehensive and Progressive Agreement for the Trans-Pacific Partnership Agreement (TPP)*

42 Privacy Commissioner, Office of the Privacy Commissioner Briefing for the Incoming Minister of Justice: Hon Andrew Little, October 2017, para 4.14 https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf Ibid para 4.14.

43 Ibid

44 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

45 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx

In March 2018, New Zealand signed the Comprehensive and Progressive Agreement for the Trans-Pacific Partnership (CPTPP) and is currently considering its ratification. Chapter 14 of the TPP on electronic communications includes several provisions that affect data and privacy obligations with respect to New Zealand's activities with the ten other member countries.[46] Relevant provisions include:

- Personal Information Protection: Each Party is called on to adopt or maintain a legal framework that protects users of electronic communications personal information. It recommends looking toward existing privacy principles when doing so.
- Cross Border Transfer of Information by Electronic Means: Allows for the cross-border transfer of personal information when the activity is for the "conduct of the business of the covered person.
- Data localisation: Parties cannot require companies to locate computing facilities in another Party's territory as a condition for conducting business in that territory. This ensures that businesses who want to conduct business in a Party's territory will have the freedom to choose where to store the data.
- Source Code: Prevents a country from requiring access to source code as a condition for conducting business. However, this does not extend to software used for critical infrastructure.

46 Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, Peru, Singapore, Vietnam.

# PART II: NEW ZEALAND'S LEGAL AND POLICY FRAMEWORK

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

## 2.1 Application of International Human Rights Framework to New Zealand

While Parliament holds the ultimate power to legislate in New Zealand, the Government must take into account the impact of international law on domestic legislation as a result of its international treaty obligations and the principles of customary international law.[47] The Vienna Convention on the Law of Treaties[48] provides that treaty obligations are binding on a State party and its territory and that domestic law may not be used as a justification for its failure to perform a treaty obligation.[49]

Accordingly, the Cabinet Office Manual and the ancillary Legislation Design and Advisory Committee Guidelines[50] direct the Government and public servants to ensure that proposed legislation and policy conforms with international obligations.[51]

The Government's approach to applying human rights treaty obligations to legislation and policy development has been somewhat uneven to date. However, it is notable that the recent reforms to New Zealand's intelligence and security jurisdiction, which had considerable implications for the right to privacy, gave careful scrutiny to international human rights standards. This resulted in human rights considerations being elevated amongst the new legislative principles and decision-making criteria that the reforms have introduced.

This focus on international human rights obligations has been further reflected in related policy developments in the sector. In 2017, a Ministerial Policy Statement (MPS) regarding functions of the intelligence and security agencies when cooperating with overseas public authorities listed 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."[52]

Furthermore, the New Zealand Courts have affirmed that they can be expected to interpret legislation in a manner consistent with international treaty obligations[53] and that it is not to be assumed that Parliament intentionally passed legislation contrary to those treaty obligations.[54] In addition, the reference to the ICCPR in the Long Title of The New Zealand Bill of Rights Act 1990 indicates a legislative desire to achieve compliance with international rights obligations.[55]

The Courts have also applied non-binding international human rights documents, such as UN Minimum Standards passed by the General Assembly, as persuasive interpretative aides when considering the application of a human rights obligation under an international treaty.[56] The High Court has stated that "subject to express or implied contrary provisions in domestic legislation, New Zealand Courts will pay regard to internationally accepted human rights norms in the exercise of judicial discretion"[57].

Jurisprudence arising from the judgments of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union on the application of the right to privacy under the European Convention on Human Rights (ECHR)

47 Philip A Joseph, Constitutional and Administrative Law in New Zealand, 4th ed., pg 563

48 Ratified by New Zealand on 4 August 1971

49 Articles 26, 27 & 29.

50 http://www.ldac.org.nz/guidelines/lac-revised-guidelines/chapter-8/.

51 Cabinet Office, Cabinet Manual 2017, [7.65 (d)-7.66].

52 Hon Christopher Finlayson, Ministerial Policy Statement: Cooperation of New Zealand intelligence and security agencies (GCSB and NZIS) with overseas public authorities, Appendix One, p 15, September 2017 available: https://www.nzic.govt.nz/assets/MPSs/Ministerial-Policy-Statement-Cooperation-with-overseas-public-authorities.pdf.

53 Ye v Minister of Immigration [2009] NZSC 76, [2010] 1 NZLR 104 at [24]; DP v R [2015] NZCA 476, [2016] 2 NZLR 306 at [11], citing New Zealand Airline Pilots Association Inc v Attorney-General [1997] 2 NZLR 269 (CA) at 289 and Yuen Kwok-Fung v Hong Kong Special Administrative Region of the People's Republic of China [2001] 3 NZLR 463 (CA) at [16].

54 DP v R, at [11], citing inter alia Terranova Homes and Care Ltd v Service and Food Workers Union Nga Ringa Tota Inc [2014] NZCA 516, [2015] 2 NZLR 437 at [227]; Ye v Minister of Immigration [2009] NZSC 76, [2010] 1 NZLR 104 at [24] and [32]; and Zaoui v Attorney-General (No 2) [2005] NZSC 38, [2006] 1 NZLR 289.

55 Although not referred to in the Long Title of BORA, international conventions other than the ICCPR have been referred to on a number of occasions and can inform the analysis. See for example, Ministry of Health v Atkinson [2012] 3 NZLR 456 (CA) at [42].

56 See para 11 of Winkelmann J's judgment in TV3 v N (name suppression) (unreported, HC Auckland, 7 July 2006) where she finds at paras 10 and 11 that public interest factors as to reporting of evidence must be balanced with "the State's particular obligations to young offenders, and in particular Article 8 of the United Nations Standard Minimum Rules for the administration of juvenile justice ("the Beijing Rules").

57 R v Rawiri & Ors (Unreported, HC Auckland 19 June 2002), Fisher J.

may also be considered by the New Zealand Courts. While judgments of the European Courts are not binding upon them, New Zealand Courts have displayed a willingness to consider and refer to decisions of the ECtHR, and to decisions of the UK courts made under its Human Rights Act 1998 which incorporates much of the ECHR into UK law.[58]

### 2.2 New Zealand Bill of Rights Act 1990

The preamble of the New Zealand Bill of Rights Act 1990 (BORA) provides that it is an Act to:

a. affirm, protect, and promote human rights and fundamental freedoms in New Zealand; and

b. affirm New Zealand's commitment to the International Covenant on Civil and Political Rights.

The preamble enunciates the purpose of the BORA as a legislative instrument that affirms New Zealand's human rights obligations under the ICCPR. Notably, BORA does not contain a free-standing right to privacy equivalent to Article 17 of the ICCPR.

The challenges brought about by contemporary and future electronic surveillance and data interception technology raise the question of whether the BORA should be updated to include a free-standing right to privacy. The Human Rights Commission,[59] the Office of the Privacy Commissioner,[60] and human rights advocates and academics[61] have called for the inclusion of the right to privacy in the BORA or a written constitution for New Zealand. To do so would not only bring the BORA into greater substantive alignment with the ICCPR. It would also 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.[62] Furthermore, it would allow the Courts to issue a declaration of inconsistency if they believe that legislation is inconsistent with the right to privacy.[63]

***The challenges brought about by contemporary and future electronic surveillance and data interception technology raise the question of whether the BORA should be updated to include a free-standing right to privacy.***

BORA does, however, provide for the right to protection from unreasonable search and seizure,[64] a right that is engaged when considering the surveillance and interception of personal data. There is a corollary between the civil right to protection from unreasonable search and seizure and the common law recognition of the privacy of the home.[65] The New Zealand Courts have affirmed that private property rights, in this context, have "special significance" in that they "enable individuals to maintain their right to privacy and their civil liberties in general and…underline the value attached to personal independence and freedom from official harassment."[66]

58 Butler & Butler, The New Zealand Bill of Rights Act, A Commentary, 2nd ed., pg 95.

59 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/.

60 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

61 http://constitutionaotearoa.org.nz/the-conversation/rights-privacy/.

62 Section 7, BORA.

63 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.

64 BORA, s 21

65 Butler, pg 65, 3.3.15 citing Morris v Beardmore [1981] AC 446 (HL).

66 Transport Ministry v Payn [1977] 2 NZLR 50 (CA) at 64

## 2.3 Privacy Act 1993

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 businesses (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.[67]

The Act itself does not provide for, or affirm, a free-standing right to privacy. However, the information privacy principles are fundamentally congruent with the right to privacy and provide presumptive rights for a person to access their personal information and have their personal information protected from unauthorised use or disclosure to third parties. The information privacy principles are designed as operational safeguards and thus are subject to exceptions in certain circumstances (for example where non-consented disclosure of personal information may be required to avert a likelihood of serious harm).

Compliance with the Privacy Act is overseen by the Privacy Commissioner, who may investigate and instigate proceedings against agencies that may be in breach. In addition, the Privacy Commissioner may produce sector-specific codes of practice, such as the Health Information Privacy Code and the Telecommunications Information Privacy Code, that derive from the foundational information privacy principles in the Act.

Among other things, the Privacy Act regulates information matching practices between specified public-sector agencies and information sharing practices among agencies that would otherwise breach one or more of the information privacy principles. Agencies that wish to share personal information in such a manner are required by the Privacy Act to enter into Approved Information Sharing Agreements.

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,[68] as well as calls by the Privacy Commissioner to modernise the Act.[69]

The new Bill proposes modernising the 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.[70] 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.[71]

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."

The most significant reforms to the law are the increased accountability mechanisms supporting the early identification of systematic privacy risks. These changes include:

- Mandatory reporting of data breaches: One of the major changes under the Bill is the introduction of a mandatory requirement

67 Part 2 of the Privacy Act 1993, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

68 See http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf

69 See https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf

70 Privacy Bill, Clause 19, http://www.legislation.govt.nz/bill/government/2018/0034/latest/whole.html#LMS23342

71 Ibid.

for agencies to report privacy breaches to the Privacy Commissioner and affected individuals if the breach has caused or risks causing harm.[72] This is consistent with mandatory reporting regimes that are increasingly required in privacy legislation overseas, 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[73] 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.[74]

- 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.[75] The Human Rights Review Tribunal will be able to enforce compliance notices and hear appeals.[76]

- 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.[77]

- 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.[78]

## 2.4 Approved Information Sharing Agreements

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.[79] The Privacy Act provides for procedural safeguards in the formation of AISAs as well as continued oversight, including:

- Agencies must consult the Privacy Commissioner, any person or organisation representing the interests of the people whose information will be affected and any other person that the agencies consider should be consulted.[80]

- 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.[81]

- The Privacy Commissioner also has the power to prepare a report on any privacy matters relating to the AISA.[82]

72 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.

73 Privacy Bill, Clause 122.

74 Ibid. Clause 123.

75 Ibid. Clause 124.

76 Ibid. Clause 130.

77 Ibid. Clause 92.

78 Ibid. Clause 96.

79 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.

80 Privacy Act 1993, s 96O.

81 Ibid. s 96N.

82 Privacy Act 1993, s 96P.

## 2.5 Predictive Risk Modelling

In New Zealand, the development of a proposed predictive risk modelling (PRM) programme in the child protection sector may have 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. As a PRM initiative requires agencies to share identifiable personal information without consent, it requires either an AISA[83] or enabling provisions in primary legislation to legally override standard Privacy Act protections.

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.[84]

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. 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 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.

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 to consideration the potentially discriminatory impacts of this practice, is made public and is referenced in all relevant legislation."[85]

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 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.[86] 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.[87]

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.[88] Other PRM initiatives, such as one that was directed at identifying young people at risk of long-term benefit dependency,[89] have relied upon AISAs.

More generally, New Zealand academics at the University of Otago have commented on the use

83 See, for example, the 2015 Draft Youth Services AISA between MSD, the Ministry of Education and the Department of Corrections which proposed to enable personal data to be shared between those agencies for the purpose of identifying youth beneficiaries eligible to enrol in the MSDs Youth Service programme. The draft AISA is accessible at: https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/policy-development/youth-service-information-sharing-agreement-consultation/public-consultation-on-new-youth-service-information-sharing-agreement.html

84 See Keddell E, "The ethics of predictive risk modelling in Aotearoa/New Zealand child welfare context: child abuse prevention or neo-liberal tool?", 28 July 2014, available at https://ourarchive.otago.ac.nz/bitstream/handle/10523/5666/PRMfinal3.pdf?sequence=1&isAllowed=y

85 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

86 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).

87 Clause 41, new s 66(2).

88 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

89 https://www.hrc.co.nz/files/7914/6483/4019/16g_Human_Rights_Commission_feedback_on_draft_Youth_Service_AISA.pdf.

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.[90] These questions include whether:

- The PRM tool is accurate – this requires both transparent evaluation processes and a thorough description of the data set on which it was assessed
- The responsible agency can explain how the PRM tool works so that clients can appeal a decision made by it
- The PRM tool distorts the way the agency pursues its policy objectives
- The PRM tool enables the agency to 'duck' its responsibility to make fair and humane decisions
- The PRM tool implicitly discriminates against individuals – evaluative processes should be used to identify whether this is the case
- The responsible agency is effectively training employees in the use of the PRM tool and associated decision-making system

## 2.6 Citizen Based Analytics

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, an approach described as "social investment" in New Zealand.[91] The research was the result of a collaboration with European data statisticians via the European Commission.

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.[92] 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.[93] The IDI has been subject to privacy impact assessments and is subject to the privacy protocols of Statistics NZ.

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.[94] 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 Partnership[95] are working together to recommend an assurance and governance system for data access and use.

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.[96] 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

90 http://www.otago.ac.nz/humanities/news/otago664403.html.

91 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

92 http://archive.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure.aspx

93 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

94 Ibid.

95 The Data Futures Partnership 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/.

96 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

person, family or whanau focus.[97] The coercive nature of the policy was of considerable concern to many NGO service providers working in those sectors.

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.[98] 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."[99] 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."[100] The Privacy Commissioner accordingly recommended that the policy be amended to conform with the IPPs under the Privacy Act.[101] Subsequently, the policy appears to have discontinued.

## 2.7 Intelligence and Security Act 2017

In March 2016, a major independent review of the intelligence and security legislation was presented to parliament.[102] The review itself was conducted following calls by the Human Rights Commission[103] in a report to the Prime Minister and 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, 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 regarding access to information from other government agencies, and set out a proposed authorisation framework for intelligence and security activities.

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.[104] 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.

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 to issue Ministerial Policy Statements (MPS) which set out policy and practice standards concerning the operational activities of the intelligence and security services.[105]

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,[106] including the requirement under IPP 4(a) that personal information is collected by lawful means. Prior to the amendment, the agencies

97 Ibid., para. 3.3.4.

98 Ibid, Executive Summary at point

99 Ibid., para 4.2.

100 Ibid, Executive Summary, at point 5

101 Ibid, point 8.

102 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 .

103 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.

104 http://www.legislation.govt.nz/act/public/2017/0010/37.0/DLM6920823.html .

105 http://www.legislation.govt.nz/act/public/2017/0010/37.0/DLM6920823.html .

106 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)).

were exempt from this requirement, as well as most of the other IPPs.[107] 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.

In March 2016, Sir Michael Cullen and Dame Patsy Reddy presented the First Independent Review of Intelligence and Security to parliament (Cullen/Reddy Report).[108] The review focused on the legislative framework governing the Government Communications Security Bureau (GCSB) and NZ Security and Intelligence Service (NZSIS) and their oversight regime. They concluded that there should be a single, integrated and comprehensive Act clearly setting out how and why the agencies are constituted; how their intelligence and security activities are authorised; and their oversight.

## 2.8 Legislative Advisory Committee Guidelines, the Chief Privacy Officer and the Government Chief Data Steward

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:

> *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 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.*[109]

The LAC Guidelines provide that if proposed legislation affects the privacy of individuals, the Privacy Commissioner and the Government Chief Privacy Officer (GCPO)[110] 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 set out the following five-part set of questions that officials must apply to proposed legislation:

- Is the legislation consistent with the requirements of the Privacy Act 1993 and its 12 Information Privacy Principles?
- Have you complied with any relevant Code of Practice issued by the Privacy Commissioner?
- Have you consulted the Privacy Commissioner, the Ministry of Justice and the GCPO?
- Does the legislation require a complaints process?
- Have you considered the consequences of non-compliance with the Privacy Act 1993?

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.[111]

The LAC Guidelines can be seen, in this respect, as establishing a legislative due diligence procedure on privacy. The GCPO is also an integral component of the Government's internal due diligence processes on privacy. Unlike the Privacy Commissioner, who as the Privacy Act 'watchdog' agency, is an Independent Crown Entity and therefore legally independent of the Government, the GCPO is a government official tasked with developing standards, issuing guidance and providing assurance to Government

107 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)

108 https://www.parliament.nz/resource/en-nz/51DBHOH_PA-P68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe e.

109 http://www.ldac.org.nz/guidelines/lac-revised-guidelines/chapter-7/.

110 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/.

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

agencies to help build their privacy and security capabilities.[112] The GCPO accordingly has no role in investigating non-compliance with the Privacy Act.

In 2017, the State Services Commissioner designated the Chief Executive of Statistics New Zealand (Stats NZ) as the Government Chief Data Steward. Stats NZ has a key role in supporting government agencies to build their capabilities as regards their use and management of data. This includes the development and implementation of data standards. The principles of transparency, trust and integrity around the use of government data are described by Stats NZ as being "at the heart of this work."[113]

## 2.9 Common law

As described earlier in the paper, the common law has long recognised that personal property rights enable "individuals to maintain their right to privacy and their civil liberties in general."[114] The New Zealand Courts have extended these principles to include informational privacy, such as in the Duffield and Moulton cases which regarded the statutory power of police to compulsorily acquire information from arrestees to confirm identity.[115] In *Moulton*, the Court of Appeal held that the statutory power should be confined to recording details necessary to identify the arrestee, and may not be used to compile a personal history or dossier of information on the persons employment record, schooling, friendships, financial circumstances and the like under pain of legal penalty.[116]

The existence of a tort for breach of privacy in New Zealand law was also inferred by the Court of Appeal in the case of *Hosking v Runting*.[117] In that case, the Court held that the omission in the BORA and the Privacy Act of a free-standing privacy right did not preclude the existence of a common law remedy for breach of privacy. The Court considered that the legislative intent instead indicated that privacy law would be left for "incremental development" in the absence of a statutory right to privacy.[118] The Court also held that the New Zealand's international human rights obligations under the ICCPR also provide a basis for the New Zealand common law recognising the tort of breach of privacy.[119]

112 https://www.ict.govt.nz/governance-and-leadership/the-gcio-team/government-chief-privacy-officer/.

113 https://www.stats.govt.nz/about-us/data-leadership/

114 Transport Ministry v Payn [1977] 2 NZLR 50 (CA) per Woodhouse J

115 See Butler at 3.3.21 p 58; Duffield v Police (No 2) [1971] NZLR 710, Moulton v Police [1980] 1 NZLR 443.

116 Moulton v Police [1980] 1 NZLR 443 at 446

117 Hosking v Runting [2004] 1 NZLR 1.

118 Ibid at 26.

119 Ibid at 38.

# PART III: PERMISSIBLE LIMITATIONS ON THE RIGHT TO PRIVACY

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

The right to privacy is not absolute. At times governments will need to protect the interests of its citizens and to do so may gather intelligence to assist with the detection, investigation and prosecution of crime, as well as for national security.[120] Personal information may also be collected about individuals for research and policy purposes. In such cases limits may be placed on the right to privacy.

Unlike other provisions of the ICCPR, the right to privacy does not explicitly set out what limits are permissible.[121] However, authoritative international sources have established principles against which rights limiting measures can be assessed. These are the principles of legality, necessity and proportionality.[122] Any rights-limiting measure that does not accord with these principles is likely to be unlawful or arbitrary and in breach of Article 17 of the ICCPR.

***Personal information may also be collected about individuals for research and policy purposes. In such cases limits may be placed on the right to privacy.***

120 Report of Special Rapporteur on the right to privacy (19 October 2017) para 7.

121 Note that the European Convention on Human Rights right to privacy under section 8 provides for the permissible limitations on the right at section 8 (2): it must be in accordance with the law, necessary in pursuit of a legitimate and, and proportionate.

122 OHCHR Report, The Right to Privacy in the Digital Age, para 22, ("Guidance on the meaning of the qualifying words "arbitrary or unlawful" nonetheless can be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, the practice of the Human Rights Committee as reflected in its general comments, including Nos. 16, 27, 29, 34, and 31, findings on individual communications and concluding observations, regional and national case law; and the views of independent experts.").

## 3.1 Legality

The UNHRC has explained that "unlawful interference" with the right to privacy means that no interference can take place unless it is envisaged by the law.[123] This means that States are required to have in place legislation that specifies in detail the precise circumstances in which interferences with the right to privacy may be permitted.[124] The law must be publicly accessible, clear and precise,[125] and individuals must be put on notice and foresee the application of the law that limits their right to privacy.[126]

## 3.2 Necessity

The principle of necessity requires that any interference with the right to privacy must be limited to that which is strictly and demonstrably necessary to achieve a legitimate aim and the lest intrusive option available.[127]

## 3.3 Proportionality

Any measures that intrude on the right to privacy must be proportionate to the objective. This involves a balancing exercise of the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests.[128]

## 3.4 Principles in New Zealand Law and Policy

New Zealand legislation and policy instruments broadly reflect the principles of legality, necessity and proportionality. For example, the information privacy principles set out in the Privacy Act 1993

123 UNHRC, General Comment No. 16 (right to privacy), para 3

124 Ibid, para 8

125 UNHRC, General Comment No. 16 (right to privacy), paras 3, 8; OHCHR Report, The Right to Privacy in the Digital Age, para 23; GA Resolution on the Right to Privacy in the Digital Age (18 December 2014); Report of Special Rapporteur on freedom of expression, Frank La Rue (17 April 2013) para 83, Report of SR countering terrorism, Martin Scheinin (23 September 2014) paras 35-36; Report of the Special Rapporteur on freedom expression, (11 May 2016) para 85, Human Rights Council Resolution, Protection of human rights and fundamental freedoms while countering terrorism, A/HRC/RES/35/34 (23 June 2017) repeating wording of A/HRC/RES/29/9; SR on countering terrorism (2 July 2016); Special Rapporteur on countering terrorism, (11 August 2017).

126 Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006).

127 Report of the SR on countering terrorism, Martin Scheinin (23 September 2014) para 51; OHCHR Report, The Right to Privacy in the Digital Age, para 23.

128 bid.

provide that personal information shall not be:

- Collected unless for a lawful purpose connected with a function or activity of the collecting agency[129] (reflecting the legality principle).
- Collected unless collection of the information is necessary for that lawful purposes[130] (reflecting the necessity principle).
- Used or disclosed without consent unless certain prescribed grounds are met e.g. to avoid prejudice to maintenance of the law, to prevent of lessen serious harm[131] (reflecting the proportionality principle).

The limiting principles are more explicitly referenced in Ministerial Policy Statements issued under the Intelligence and Security Act 2017[132] by the Ministers Responsible for the GCSB and the NZSIS.[133] These will be discussed further below.

129 Privacy Act 1993, Information Privacy Principle 1.

130 Ibid.

131 Ibid, Information Privacy Principles 10 and 11.

132 Intelligence and Security Act 2017, ss 206-208.

133 Ministerial Policy Statements issued to date are publicly available at www.nzic.govt.nz

# PART IV: ADEQUATE SAFEGUARDS

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

## 4.1 Oversight and Authorization

Even if a limitation on the right to privacy is permitted by law, any measures must be subject to procedural and legal safeguards, via a sufficiently independent and robust oversight and authorisation mechanism. This ensures:

- Public trust and confidence in the work of government agencies empowered with privacy-limiting functions, such as intelligence agencies.[134]
- Information concerning a person's private life does not fall into the hands of those who are not authorised by law to receive it.[135]
- Government agencies and their delegates are held accountable for activities that result in arbitrary or unlawful interference with privacy.[136]

Safeguards are accordingly a central requirement in the relevant international frameworks. For example, the OECD has specified that:

> *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*[137]

The UN General Assembly has called on States:

> *To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.*[138]

In the intelligence and security sector, adequate authorisation and oversight may occur at three stages of surveillance activities:

- when the activity is ordered,
- while the activity is carried out, or
- after the activity has been terminated.[139]

All three branches of government should be involved in the oversight of surveillance. Mixed models whereby layers of oversight are provided by the administrative (executive), judicial and parliamentary branches of government are considered desirable.[140]

Targeted surveillance, which usually involves traditional methods such as the interception of phone calls, is usually subject to prior judicial or executive authorisation before the measure is carried out and subsequent review of legality by reference to the particular circumstances and the individual whose communications were intercepted.[141]

However, mass surveillance and the collection of metadata are usually subject to much weaker safeguards[142] because there is no opportunity for prior authorization (for a brief explanation of metadata see below). Metadata can reveal much information about an individual's personal life. Therefore, UN experts have recommended strong independent oversight mechanisms should be in place to scrutinise such surveillance.[143]

The importance of independent intelligence oversight in the New Zealand context was highlighted in the report of the First Independent Review of Intelligence and Security in New Zealand:

> *Independent external oversight is . . . essential to ensure that by working to secure populations*

134 Report of Special Rapporteur on countering terrorism, Martin Scheinin (17 May 2010) para. 13 http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf ("Intelligence oversight institutions serve to foster public trust and confidence in the work of intelligence services by ensuring they perform their statutory functions in accordance with respect for the rule of law and human rights.").

135 UNHRC, General Comment No. 16, Article 17 (right to privacy) para. 10 ("Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.").

136 Report of Special Rapporteur on countering terrorism, A/69/397 (23 September 2014) para. 45, citing OHCHR Report, The Right to Privacy in the Digital Age, para. 23

137 OECD Guidelines, Security Safeguards Principle 11

138 General Assembly Resolution on the Right to Privacy in the Digital Age (19 December 2016).

139 Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015) para. 233, http://hudoc.echr.coe.int/eng?i=001-159324

140 OHCHR Report, The Right to Privacy in the Digital Age, para 37; Report of Special rapporteur on countering terrorism, Ben Emmerson (23 September 2014) para 45; Human Rights Resolution A/HRC/27/37.

141 Report of SR on countering terrorism, Ben Emmerson (23 September 2014) paras 46-48; Report of SR on privacy, Joseph Cannataci, A/HRC/34/60 (24 February 2017) para 25

142 Report of SR privacy, Joseph Cannataci (24 February 2017) para 25.

143 Report of SR countering terrorism, A/69/397 (23 September 2014) paras 46-48; Report of SR privacy, Joseph Cannataci (24 February 2017) para 25

*against internal and external threats and advance the interests of the nation as a whole, intelligence and security agencies do not undermine democracy or the rights of individuals in the process. As publicly funded agencies, they must also be held accountable for how they use public money. Oversight must ensure the Agencies are operating efficiently and effectively in the interests of the country and in accordance with the values of its citizens.*[144]

New Zealand has several intelligence and security oversight mechanisms in place.[145] The Inspector General of Intelligence and Security (IGIS) is provided with powers under the Intelligence and Security Act 2017 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.[146] During an inquiry the IGIS may compel the 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 provide redress including remedies that involve the payment of compensation.[147] 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 of lack of jurisdiction.[148]

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. The Intelligence and Security Committee is 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 an inquiry into any matter relating to compliance with NZ law, including human rights law and propriety of activities.

Within New Zealand, there has been an oversight group established that includes the IGIS, Privacy Commissioner, Auditor-General and the Chief Ombudsman.[149] The NZ Intelligence Community is also subject to oversight of the independent authorities such as the Auditor-General, Privacy Commissioner, Ombudsman and the judiciary.

In terms of oversight of the use of personal data in the social sector, as discussed earlier, the Ministry of Social Development is currently developing a Privacy, Human Rights and Ethics Framework. The original intention of the framework is that it would apply to predictive risk modelling initiatives in the social sector (specifically the child protection and social security sectors). However, the framework potentially could be expanded to apply more generally to all information sharing initiatives within the social sector.

## 4.2 Transparency

States should be transparent about the use and scope of techniques and powers that potentially infringe the right to privacy.[150] This includes administrative processes related to the gathering of personal information and data.[151]

David Anderson, the UK's Independent Reviewer of Terrorism legislation, helpfully summed up the need for transparency in his review of surveillance legislation in the UK stating:

*The fact that the subject-matter is technical is no excuse for obscurity. It should be possible to set out a series of limited powers, safeguards and review mechanisms with a high degree of clarity and . . . without technical jargon: the place for the*

144 Sir Michael Cullen and Dame Patsy Reddy, First Independent Review of Intelligence and Security to parliament, p.52, para 4.4.

145 See NZ Intelligence Community, Oversight https://www.nzic.govt.nz/oversight/.

146 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/

147 Intelligence and Security Act 2017, s 185.

148 Ibid. s 190.

149 Privacy Commissioner, Office of the Privacy Commissioner Briefing for the Incoming Minister of Justice: Hon Andrew Little, October 2017, para 4.2 https://privacy.org.nz/assets/Uploads/Briefing-for-Incoming-Minister-October-2017.pdf

150 Report of Special Rapporteur for freedom of expression, Frank La Rue, (17 April 2013) para 91.

151 Ibid.

*latter is in regularly updated Codes of Practice*[152]

The First Independent Review of Intelligence and Security in New Zealand similarly placed greater transparency as a central objective of reform to the intelligence and security sector, providing that one of its key purposes was:

> *to provide transparency and accountability through its recommendations for a "single, integrated and comprehensive Act of Parliament that lays out in plain English how the agencies are constituted what their purposes are; how all their intelligence and security activities are authorised; and how they are overseen so as to protect those freedoms and liberties that are part of what we are as a nation.*[153]

It is notable that the Privacy Act 1993 requires procedural transparency and consultation in the development of Approved Information Sharing Agreements (AISAs), as well as publication and public access following the passage of an AISA into law.[154]

Transparency requirements also extend to private sector actors. For example, the Special Rapporteur on the right to freedom of expression has recommended that telecommunications companies should be transparent in how they communicate the impact of their activities on human rights externally, including the number of government requests they have received for things such as customer data, and the availability of remedies for persons whose rights have been breached as a result of their activities.[155]

## 4.3 Purpose Specification

The Special Rapporteur on the right to privacy has affirmed the principle of "purpose specification" as fundamental to ensuring that data collection and use adheres with the right to privacy. He notes:

> *Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose. Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.*[156]

Against this context, it is notable that the OHCHR has expressed concern that "personal data ends up in the same 'bucket' of data which can be used and re-used for all kinds of known and unknown purposes."[157] In addition, the Special Rapporteur on countering terrorism has noted that many States lack "purpose specification" provisions that restrict information gathered for one purpose from being used for other unrelated governmental objectives, leading to "purpose creep".[158] The Special Rapporteur observed:

> *This means that data for national security purposes may be shared between intelligence agencies, law enforcement agencies and other State entities, including tax authorities, local councils and licensing bodies. National security and law enforcement agencies are typically excluded from provisions of data protection legislation that limit the sharing of personal data. As a result, it may be difficult for individuals to foresee when and by which State agency they might be subjected to surveillance. This "purpose creep" risks violating article 17 of the Covenant, not only because relevant laws lack foreseeability, but also because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.*[159]

In New Zealand, the Privacy Act places limits on the use of personal information that was obtained in connection with one purpose from being used for another purpose, unless specific criteria are met.[160] One of these criteria relates to the activities of New Zealand's intelligence and security agencies and was introduced by the enactment of the Intelligence and Security Act 2017. It provides that:

> *An intelligence and security agency that holds personal information that was obtained in*

152 David Andersen Q.C. Independent Reviewer of Terrorism Legislation, A Question of Trust Report of the Investigatory Powers Review (June 2015) p 253.

153 Cullen/Reddy Report, p 1.

154 Privacy Act 1993, ss 96O, 96S.

155 Report of Special Rapporteur for freedom of expression (11 May 2016) para 13

156 Report of the Special Rapporteur on privacy, Joseph A. Cannataci (24 November 2016).

157 OHCHR Report, The right to privacy in the digital age, para. 20

158 Report of Special Rapporteur on countering terrorism, para. 56

159 Ibid

160 Privacy Act 1993, Principle 10

*connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.*[161]

However, any use of information by those agencies would have to be consistent with the policy principles set down in Ministerial Policy Statements by the Ministers responsible for the GCSB and the NZSIS and accordingly meet legality, necessity and proportionality requirements, minimise impact on third parties and facilitate effective oversight by the oversight entities.[162]

## 4.4 International Intelligence Sharing and Data Transfers

The OECD Guidelines provide member countries with a framework for managing the flow of data across their borders. The Guidelines require member countries to:

- Take steps to ensure that trans-border flows of personal data are uninterrupted and secure.[163]
- Restrict the sharing of personal data with other member countries that do not substantially observe the OECD Guidelines or that do not have in place equivalent privacy protections in domestic legislation.[164]
- Ensure that procedures for trans-border flows of personal data, including those that protect of privacy and individual liberties, are simple and compatible with those of other member countries.[165]
- Establish procedures to facilitate information exchange and mutual assistance in procedural and investigative matters.[166]

The OECD Guidelines are reflected in the Privacy Act 1993. The Act gives the Privacy Commissioner power to prohibit a transfer of personal information from New Zealand to another State by issuing a transfer prohibition notice.[167] Such a notice may be issued if the Commissioner is not satisfied that:

- Information has been received in New Zealand from another State and it is likely to be transferred to a third State which does not provide comparable safeguards to the Privacy Act; and
- Transfer would be likely to lead to a contravention of the basic principles of national application set out in part two of the OECD Guidelines.[168]

When considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans-border data flows.[169]

As noted above, the new Privacy Bill strengthens the requirements relating to the disclosure of information to an overseas person. Among the new requirements under privacy principle 11 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.[170]

In December 2012, the European Council issued a formal decision recognising that New Zealand law provides an adequate level of data protection for the purposes of EU law.[171] This decision means that personal data can flow from the EU member states to New Zealand for processing

161 Privacy Act 1993, Principle 10(2).

162 Section 206 of the Intelligence and Security Act 2017. See, for example, the MPS on Collecting Information Lawfully paragraphs 18-31, https://www.nzic.govt.nz/assets/MPSs/Ministerial-Policy-Statement-Collecting-information-lawfully.pdf

163 OECD Guidelines, Article 16.

164 Ibid. art. 17.

165 Ibid. art. 20.

166 Ibid. art. 21.

167 Privacy Act 1993, s 114B.

168 Ibid.

169 Ibid s 114B(2).

170 Privacy Bill, Clause 19, http://www.legislation.govt.nz/bill/government/2018/0034/latest/whole.html#LMS23342

171 See Commission Implementing Decision of 19 December 2012 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415703506367&uri=CELEX:32013D0065

without other safeguards being necessary.[172] The decision does not cover data exchanges in the law enforcement sector. The European Commission has only recognised eleven other countries as providing adequate protection, including Canada and the United States.[173] As noted above, New Zealand may no longer meet the EU's data protection standards in light of the new European data protection regulation that goes into effect in May 2018. This may also be relevant to the current negotiations between the New Zealand Government and the EU for a free trade agreement of which negotiations are expected to begin in 2018.

The Intelligence and Security Act 2017 requires that the Minister responsible for intelligence and security agencies issue Ministerial Policy Statements in relation to lawful activities of the Agencies and sets out guiding principles. 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." The following key principles must be applied by the Agencies when cooperating with overseas public authorities:

- Legality: Cooperation must be conducted in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.[174]

- Human rights obligations: 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 duty of due diligence and applies to requests to share intelligence on a case-by-case basis or within the context of a broader standing authorisation.[175]

- Necessity: Cooperation with overseas public authorities should only occur for the purposes necessary to support the Agencies to perform their statutory functions.[176]

- Reasonableness and proportionality: The Impact of cooperation with overseas public authorities should be reasonable and proportionate to the purpose for carrying out the cooperation, the benefit gained and the reputational risk to the Agencies and the New Zealand Government. The MPS includes a range of factors in determining reasonableness.[177]

- Protections for New Zealanders: When cooperating with overseas public authorities, the Agencies must continue to apply the same protections for New Zealand citizens and permanent residents that would normally apply, including adherence to the information privacy principles in the Privacy Act.[178]

- Information Management: Steps must be taken to ensure that information obtained by the Agencies and subsequently shared with overseas public authorities is managed in accordance with all information management requirements, standards and guidelines that relate to that information in New Zealand.[179] The Agencies are also required to specify the protection, storage and use (including the passing on of that information to any third parties) to be adhered to in respect of personal information about New Zealanders, shared with an overseas public authority.[180]

172 See https://www.privacy.org.nz/blog/providing-an-adequate-level-of-data-protection/

173 See http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

174 Ibid. paras. 30-34.

175 Ibid. paras. 35-46.

176 Ibid. para. 47.

177 Ibid. paras. 48-52.

178 Ibid. paras. 53-54.

179 Ibid. para. 55.

180 Ibid. para. 56.

- Oversight: All cooperation must be carried out in a manner that facilitates effective accountability, transparency and oversight, including the use of clear authorisation procedures, the keeping of appropriate records, maintaining up-to-date internal policies and procedures and guidance for staff, and reporting to the responsible Minister on the nature and outcomes of cooperation with overseas public authorities.[181]

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 where information has been obtained as a result of, human rights breaches in that country. This includes a 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.

181 Ibid. para. 57.

# PART V: REMEDIES

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

Article 2 of the ICCPR provides that individuals whose rights have been violated must be provided with access to an effective remedy. This requires a process where individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review and providing a rights-vindicating outcome (for example through an injunction, reparation, declaration or restitution) in the event a breach is found to have occurred.

International human rights law requires States "to provide individuals whose right to privacy has been violated by unlawful and arbitrary surveillance with access to an effective remedy."[182] Furthermore, the UN Guiding Principles on Business and Human Rights provide that States should ensure access to an effective remedy for violations of human rights by private entities.[183]

Remedies can come in a variety of judicial, legislative or administrative forms. According to the OHCHR, effective remedies will:

- be known and accessible to anyone with an arguable claim;
- involve "prompt, thorough and impartial" investigation of the alleged violations, often by an independent oversight body;
- be capable of ending ongoing violations i.e. through deletion of data or other forms of reparation; and
- in cases of gross violations, may require criminal prosecution.[184]

In New Zealand, the following remedies are available to individuals in the context of surveillance and informational privacy.

## 5.1 Domestic

*Privacy Act*

Under the Privacy Act, the Privacy Commissioner has the power to investigate a matter that is or may constitute interference with privacy.

182 General Assembly Resolution on the Right to Privacy in the Digital Age (18 December 2014).

183 UN Guiding Principles on Business and Human Rights, Pillar 3.

184 OHCHR Report, The Right to Privacy in the Digital Age, paras. 40-41.

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.

***International human rights law requires States "to provide individuals whose right to privacy has been violated by unlawful and arbitrary surveillance with access to an effective remedy."***

The Commissioner will then investigate whether the public or private sector agency has breached the Act.[185] If the complainant does not obtain a satisfactory outcome, they can take their case to the Human Rights Review Tribunal (HRRT) 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.[186]

*Human Rights Commission*

The Human Rights Act 1993 (HRA) sets out a complaints mechanism for people who believe they have been discriminated against. In the context of the collection of Big Data and the application of algorithms to that data to generate risk outcomes to inform for social policy, an individual could potentially complain to the Commission if they believe that they have been discriminated against, for example on the

185 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/.

186 See Privacy Act 1993, s 85

grounds of race or ethnicity.[187] The Commission will try to resolve the issue through informal methods such as mediation. However, if it is not resolved, individuals can take their complaint to the HRRT, where remedies may be granted if it is found that there has been a breach of the HRA.[188]

*Civil*

Individuals may bring a civil case in the New Zealand courts for a breach of BORA. Such a claim may represent elements of a person's private life and autonomy, including the right to be secure against unreasonable search and seizure, the right to freedom of association, and the right to freedom of expression. The Court of Appeal in Baigent's Case established that the remedy of monetary compensation was available to grant relief for a breach of the BORA, notwithstanding the absence of a specific remedies section in the Act. As noted in section 2, the Court of Appeal in the case of Hosking v Runting found that there is a tort for invasion of privacy in New Zealand, which provides a direct remedy against the disclosure of private facts about a person.

*Criminal*

There is an array of criminal offences in New Zealand which impose penalties for various sorts of conduct that might be categorised as invasions of privacy. Privacy of communications, especially via mail and telephone, receives fairly extensive protection. There are also offences relating to the disclosure of private or confidential information[189] and offences relating to computers.[190]

187 See s 6.4 describing concerns in the US where the use of algorithmic techniques has exacerbated racially biased procedures and outcomes in the law enforcement sector.

188 Human Rights Act 1993, s 92I.

189 Part 9A of the Crimes Act 1961, entitled "Crimes against personal privacy" protects private communications through regulating the use of interception devices. It is an offence, punishable by up to two years' imprisonment, to intercept any private communication using an interception device, unless the person intercepting the communication is a party to that communication or it was carried out in pursuance to the Search and Surveillance Act 2012, Part 4 of the Intelligence and Security Act 2017 or the International Terrorism (Emergency Powers) Act 1987). Where a private communication has been intercepted contrary to the Act, it is prohibited to intentionally disclose the communication or its substance or meaning, or to intentionally disclose the existence of the communication, if the discloser knows that the communication has come to his or her knowledge as a direct or indirect result of contravening the Act (Crimes Act 1961, s 216C).

190 A person who intentionally access a computer system, directly or indirectly, without authorisation, knowing that they are not authorised to access the computer system or being reckless as to whether they are authorised, commit an offence (Crimes Act 1961, s 252).

*Harmful Digital Communications*

The Harmful Digital Communications Act sets out ten communication principles, including that a digital communication should not disclose sensitive personal facts about an individual. An individual can make a complaint to Netsafe, the approved agency under the Act, if they believe that one of the principles has been breached. Netsafe will 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.[191] 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.

*Inspector General of Intelligence and Security*

The IGIS can 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.[192] 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 provide redress including remedies that involve the payment of compensation.[193] 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 of lack of jurisdiction.[194]

*Judicial review*

An individual can apply to the High Court for a review of actions or decisions of a public or

191 For more information see https://www.consumerprotection.govt.nz/consumer-law-and-your-rights/online-safety/harmful-digital-communications-act/

192 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/

193 Ibid., s 185.

194 Ibid., s 190.

private administrative body to see whether they acted within the powers given to them by the law. Generally, a person needs to be affected by a decision to apply for judicial review, but the Court increasingly allows applications from people when the decision relates to a matter of public interest. The Court can grant interim relief preventing a decision being made or given effect to.

## 5.2 International

*Optional Protocol to the ICCPR*

While the right to privacy is not included in the BORA, individuals may still seek a remedy under the individual complaints procedure of the Optional Protocol to the ICCPR. New Zealand has been a party to the Optional Protocol since 1989, which allows individuals to make complaints to the UNHRC if they believe their rights under the ICCPR have been violated. Complaints are only accepted if all domestic remedies have been exhausted. The UNHRC examines the admissibility and merits of the complaint and if it decides that the individual's rights have been violated will make recommendations to the State party concerned.

# PART VI: EMERGING ISSUES

NZ Human Rights.
Human Rights Commission
Te Kāhui Tika Tangata

## 6.1 Meta Data and Data Retention

Data retention in the context of communications surveillance relates to laws or policies that require telecommunications companies to store content data and metadata in case such data is required at a future date. Content data is the actual substance or subject of communications that individuals send to each other using modern communications. Meta data, on the other hand, is data about the communication. This includes information about:

- the location that it was sent and received from;
- the devices that it was sent and received on;
- the times at which the message was sent and received; and
- information relating to the sender and recipients such as email address, ISPs and IP addresses.[195]

Technological advancements mean that metadata can be analysed, mined and combined in ways that make it even more revealing about individuals than content data. Certain types of metadata, when aggregated "may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication."[196] Through such information, individuals leave a digital trail which can be used by governments and commercial private sector entities to generate a profile about an individual's private life and interactions.

The OHCHR has noted that mandatory data retention laws are neither a necessary or proportionate limitation on the right to privacy.[197] The Special Rapporteur on freedom of expression has also criticised that they limit an individual's ability to remain anonymous, commenting that:

> *A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.*[198]

***Technological advancements mean that metadata can be analysed, mined and combined in ways that make it even more revealing about individuals than content data.***

The issue of retention of metadata was addressed recently by the European Court of Human Rights (ECtHR). In a December 2016 judgment concerning legislation that requires the mandatory retention of data in bulk by telecommunication providers, the ECtHR held:

> *The interference entailed by such legislation in the fundamental rights guaranteed in the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered used being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance […]*[199]

In that case, the ECtHR concluded that national legislation allowing for the general and indiscriminate retention of all traffic and location data cannot be considered necessary, even in the fight against serious crime.[200]

The ECtHR also held that retention of traffic data

195 See Privacy International, What is Metadata?, https://www.privacy-international.org/node/53.

196 Human Rights Council Resolution 34/7, The right to privacy in the digital age (7 April 2017).

197 OHCHR Report, The right to privacy in the digital age, para 26

198 Report of Special Rapporteur on freedom of expression, (22 May 2015) para 55

199 ECtHR, Tele2 Sverige AB Grand Chamber, Joined cases C-203/15 and C-698/15 (21 December 2016) para 103 http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

200 Ibid. para. 103.

must be the exception not the rule.[201] The Court noted that it would be legitimate for States to adopt data retention laws for the purpose of fighting terrorism or serious crime if the retention of data is limited to what is strictly necessary for that purpose. [202] However, such laws must have safeguards, effective oversight and remedies mechanisms in place.[203]

The outcome of this case was questioned by David Anderson, UK's independent reviewer of terrorism legislation, who described the decision as "genuinely radical." Anderson stated that:

> *A more rigorous analysis of proportionality would have focussed on any actual harm that this useful power might be shown to have caused over its years of operations, and sought to avoid assertions based on theory or on informal predictions of popular feeling.*[204]

The Special Rapporteur on the right to privacy welcomed the ECtHR's judgment. However, he shared Anderson's desire for a more rigorous analysis of proportionality when it comes to mass surveillance. In doing so, he noted that he has not been granted, in the UK at least, access to any information which would confirm that the utility of bulk acquisition of data is both necessary and proportional to the risk.[205]

Addressing, in part, concerns about data retention, the EU's General Data Protection Regulation, which comes into force in May 2018, provides for the right of data erasure. That is the right to be forgotten which entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure under the regulation include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.[206]

In the context of storage of personal data that is not necessarily gathered through surveillance, the OECD Guidelines provide that:

> *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*[207]

In New Zealand, the Privacy Act requires, in unequivocal terms, that agencies should not hold information for longer than what is required for the purposes for which the information may lawfully be used.[208] Furthermore, the Privacy Act and the sector specific codes that sit beneath it (the Health Information Privacy Code, the Telecommunications Information Privacy Code and the Credit Reporting Privacy Code) require relevant agencies to ensure security safeguards are in place to protect against loss, access, use, modification or disclosure or any other misuse of the information.[209] Notably, credit agencies under the Credit Reporting Privacy Code have a particularly detailed and specific set of prescribed storage safeguards that they are required to have in place.[210]

## 6.2 Mass Surveillance

Mass surveillance involves the indiscriminate monitoring of the population or a significant component of a group of persons.[211] The technology revolution has meant that governments can now use mass surveillance to capture data about virtually all aspects of our lives. Traditionally such surveillance was conducted through CCTV and national databases, but the focus now is around the monitoring of individual's communications on phones and computers.

Mass surveillance of meta data and intercepted material is particularly problematic because it interferes with the privacy of a large number

201 bid. para. 108.

202 Ibid.

203 Ibid. paras. 103-111.

204 Report of Special Rapporteur on the right to privacy (24 February 2017) para. 16.

205 Ibid. para. 17.

206 http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

207 OECD Guidelines, art. 9.

208 Privacy Act 1993, Principle 9

209 Ibid. Principle 5.

210 Credit Reporting Privacy Code, Rule 5(2).

211 Privacy International, What is mass surveillance? https://www.privacyinternational.org/node/52.

of individuals.[212] This type of indiscriminate approach also has potentially discriminatory implications. Privacy International have observed that:

> *By starting from a position where everyone is a suspect, mass surveillance encourages the establishment of erroneous correlations and unfair suppositions.*[213]

The General Assembly's resolution on the right to privacy in the digital age has raised deep concern about the negative impact surveillance carried out on a mass scale may have on the enjoyment of human rights.[214] The Special Rapporteur on countering terrorism, Ben Emmerson, has gone as far as to say that the practice of mass surveillance impinges on the very essence of the right to privacy:

> *It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights; it excludes any individualized proportionality assessment; and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult.*[215]

The European courts have found that laws permitting mass surveillance breach the right to privacy.[216] However, where such activity has accorded with the privacy limitation principles (i.e. legality, necessity and proportionality) and is subject to effective oversight, the courts have ruled in favour of it. In a case brought against Germany,[217] the ECtHR dismissed an application that complained that the German state was monitoring communications in the absence of any "concrete suspicion" and relying on "catchwords" in order to analyse the data.[218] The Court found that "strategic monitoring" was not in itself a disproportionate interference with the right to privacy. In so concluding, it had regard to the narrow and closely defined justifications for such collection, the safeguards that governed the authorisation of the collection, the safeguards concerning use of that material and the data protection systems in place.[219]The Court found that there existed adequate and effective guarantees against abuses of the state's strategic monitoring powers.[220]

In New Zealand, the report into intelligence and security legislation noted the practical limitations of mass surveillance and describes the context in which GCSB uses mass surveillance:

> *The reality of modern communications is that it is often not possible to identify and copy a specific communication of interest in isolation. If a particular satellite might carry a relevant communication, the GCSB cannot search for that communication before interception occurs. First it needs to intercept a set of communications, most of which will be of no relevance and will be discarded without ever being examined by an analyst. This is the haystack in which the needle must be found.*[221]

In addition, case law of the ECtHR and the UNHRC have made clear that UN human rights treaty obligations may extend extraterritorially

212 David Andersen Q.C. Independent Reviewer of Terrorism Legislation, A Question of Trust Report of the Investigatory Powers Review (June 2015) pg. 78.

213 Privacy International, What is mass surveillance? https://www.privacyinternational.org/node/52

214 General Assembly Resolution on the Right to Privacy in the Digital Age (18 December 2014).

215 Report of Special Rapporteur on countering terrorism, Ben Emmerson (23 September 2014) para. 18.

216 See Roman Zakharov v. Russia, App. No. 47143/06, ECtHR, Judgment (4 December 2015) at paras. 302-304. http://hudoc.echr.coe.int/eng?i=001-159324. In a case against Russia in 2015, the Court found that a law providing for secret interception of mobile telephone communications violated the right to privacy. The Court noted that a number of shortcomings in the law relating to: circumstances in which they could resort to secret surveillance measures and circumstance in which they could be discontinued; procedures for authorising interception as well as for storing and destroying the intercepted data; supervision of the interception; and effectiveness of remedies; Szabo and Vissy v. Hungary App No. para. 89. In a subsequent case regarding 2016 Hungarian legislation on secret anti-terrorist surveillance that allowed for mass surveillance, the Court found that the law did not provide sufficient safeguards to avoid abuse. The Court reached this conclusion based on the fact that the: scope of the measures could include virtually anyone in Hungary; that the ordering of such measures was taking place entirely within the executive and without an assessment of whether interception of communications was strictly necessary; and lack of effective remedial measures being in place.

217 Weber and Saravia v. Germany, App. no. 54934/00, European Court of Human Rights, Decision as to Admissibility (29 June 2006).

218 Ibid. para 9.

219 Ibid. paras. 114-117.

220 bid. para. 137.

221 Cullen/Reddy Report, para. 3.37. The report went on to note that to find the "needle" (the communications that are of intelligence value), the GCSB filters intercepted material for relevance using search terms. At para. 3.38 the report notes that "only those communications that meet the selection criteria are ever seen by an analyst. The GCSB has internal processes in place to ensure analysts justify their use of each search term and record all searches for the purpose of internal audits and review by the Inspector-General of Intelligence and Security."

in respect of cross-border surveillance.[222] [223] The Special Rapporteur for the right to privacy has accordingly held that:

> *any international agreements that permit surveillance activities directed at foreigners or citizens must be carried out in compliance with fundamental human rights such as privacy and non-discrimination. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age.*[224]

## 6.3 Big Data

"Big Data" is a term that is becoming increasingly prevalent alongside the rapid development of technology that allows for the collection of data. The UN Special Rapporteur on the right to privacy, in his October 2017 report on "Big Data, Open Data" characterised Big Data 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.*[225]

There is no agreed definition to Big Data. However, various experts in the field have defined it as:

- huge in volume, consisting of terabytes or petabytes of data;
- high in velocity, being created in or near real-time;
- diverse in variety, being structured and unstructured in nature;
- exhaustive in scope, striving to capture entire populations or systems;
- fine-grained in resolution and uniquely indexical in identification;
- relational in nature, with common fields enabling the conjoining of different data sets;
- flexible, adding new fields easily and able to expand in size rapidly.[226]

The Special Rapporteur has observed that Big Data is increasingly being used to "produce social benefits, including personalised services, increased access to services, better health outcomes, technological advancements and accessibility improvements."[227] While the potential utility of Big Data is profound, the Special Rapporteur has urged caution in applying it too readily and without objective scrutiny:

> *…epistemological claims, which tend to elevate Big Data to a new form of scientific method, lie at the centre of the unease many have expressed about the limitations of, and risks posed by, Big Data.*[228]

One of the most significant developments arising from Big Data has been the introduction of new analytical techniques that allow for the detection of meaningful patterns in the data. One such technique is 'data mining' – "a process whereby data is extracted from large data sets and subsequently analysed to determine whether patterns or correlations exist."[229]

The algorithm is the "engine" which drives this technique by determining how data should be interpreted and what resulting actions should be taken.[230]

As discussed above, in New Zealand the application of algorithmic risk assessments to Big Data has been identified as having utility for social sector policy and decision-making. In particular, it is seen as underpinning the implementation and operation of the "social investment model" in which "citizen-based analytics" is used to provide empirical support for social policy

222 Report of Special Rapporteur on countering terrorism, Ben Emmerson (23 September 2014) para. 43 ("States are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction."); The UN Human Rights Committee has highlighted that any interference with the right to privacy must comply with the principles of legality, proportionality and necessity, regardless of nationality or location of individuals whose communications are under direct surveillance CCPR/C/USA/CO/4 at para. 22.

223 See David Andersen Q.C. Independent Reviewer of Terrorism Legislation, A Question of Trust Report of the Investigatory Powers Review (June 2015) citing Venice Commission of the Council of Europe, pg 80

224 Report of Special Rapporteur on the right to privacy (24 February 2017) para. 29.

225 Ibid. para. 36.

226 Report of Special Rapporteur on the right to privacy (24 November 2017) citing Rob Kitchen, Big Data, new epistemologies and paradigm shifts, Big Data & Society, April-June 2014, pg. 1

227 Ibid. para 44.

228 Ibid. para. 48

229 Ibid. para. 54.

230 Ibid. para. 55.

(including funding and service delivery).[231] The proposed predictive risk modelling programme for the child protection and welfare sector is an example of a specific policy initiative which uses algorithmic techniques to identify risk and target service interventions accordingly.

The use of Big Data in this way has significant implications for not only the right to privacy, but also the right to freedom from discrimination due to the inherent nature of the algorithmic approach. The Special Rapporteur on the right to privacy has highlighted a number of well documented risks associated with algorithmic techniques, including that they:

- are value laden,
- may be based on imperfect or selective data,
- may be used for profiling, and
- are opaque and unaccountable – it is difficult to attribute responsibility or accountability for harm caused by algorithmic processing.[232]

The Special Rapporteur further observes that:

> *Recommendations and decisions that result from algorithmic processing appear to spring from an inscrutable and unknowable black box, a kind of twenty-first century Delphic oracle that seemingly makes unchallengeable and authoritative pronouncements divorced from human agency.*[233]

As with surveillance activities by intelligence and security agencies, operational and procedural safeguards in the social sector are an essential bulwark against the risk of human rights breaches occurring and becoming normalised in relation to personal data. The New Zealand Government's proposed Privacy, Human Rights and Ethics Framework therefore will be a critical front-end procedural safeguard for ensuring that the deployment of algorithmic Big Data techniques in the social sector conform with human rights obligations and accordingly are carried out with the necessary "social licence" identified by Sir Peter Gluckman.

## 6.4 Artificial Intelligence

The development of Big Data and Artificial Intelligence (AI) technologies has occurred hand in hand in recent years. While AI has existed for over sixty years, its development and application over the last ten years has rapidly accelerated due to "better algorithms, increases in networked computer power, and the tech industry's ability to capture and store massive amounts of data."[234]

A recent report by AI Now, a US research institute which examines the social implications of AI, describes how AI has infiltrated every aspect of our lives:

> *AI systems are already integrated in everyday technologies like smartphones and personal assistants, making predictions and determinations that help personalize experiences and advertise products. Beyond the familiar, these systems are also being introduced in critical areas like law, finance, policing and the workplace, where they are increasingly used to predict everything from our taste in music to our likelihood of committing a crime to our fitness for a job or an educational opportunity.*[235]

As discussed earlier in the paper, AI is increasingly used in the criminal justice system. For example, by the police to target resources or high-risk individuals, by the courts to predict the likelihood of re-offending and prisons in targeting restorative justice.

The use of algorithmic risk assessments in sentencing was recently challenged in the United States in the case of State v. Loomis in the Wisconsin Supreme Court.[236] The Court sentenced the defendant based in part on a tool called COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) that was developed by a private company and purports to predict a defendant's risk of committing another crime. The defendant appealed the ruling on the grounds that the court's reliance on COMPAS

231 Sir Peter Gluckman, Using Evidence to Inform Social Policy: the role of citizen-based analytics. A Discussion Paper, Office of the Prime Minister's Chief Science Adviser (19 June 2017) p 10.

232 Report of SR on privacy (24 November 2017) paras 57-70.

233 Ibid para 55.

234 AI Now 2017 Report https://ainowinstitute.org/AI_Now_2017_Report.pdf.

235 AI Now 2017 Report, p 3.

236 For an overview and analysis of the decision see https://harvardlawreview.org/2017/03/state-v-loomis/

violated his due process rights because the COMPAS reports provide data relevant only to particular groups and because the methodology used to make the reports is secret. Therefore, the use of the COMPAS assessment infringed on both his right to an individualised sentence and his right to be sentenced on accurate information. The defendant also complained that it was unconstitutional because it took gender into account.

The Supreme Court ruled that a trial court's use of an algorithmic risk assessment in sentencing did not violate the defendant's due process, highlighting that the COMPAS report was not the sole basis of the sentencing decision. However, the Judge added that judges must proceed with caution and expressed scepticism when using such risk assessments. To ensure that judges weigh risk assessment appropriately, the court prescribed both how these assessments must be presented to trial courts and the extent to which judges may use them. The court explained that risk scores may not be used "to determine whether an offender is incarcerated" or "to determine the severity of the sentence."[237] Therefore, judges using risk assessments must explain the factors other than the assessment that support the sentence imposed. Five written warnings must also be provided to judges when COMPAS assessments are used.[238]

Concerns regarding the inherent risk of bias that arises from algorithmic risk assessments in the criminal justice sector were raised by U.S. Attorney General, Eric Holder in 2014.[239] Furthermore, in an investigation by ProPublica in 2016 found that COMPAS assessments for more than 7,000 arrestees in Florida was based on an algorithm that was biased against African Americans.[240]

AI systems challenge the right to privacy because they depend on ingesting as much data as possible, a methodology which is adverse to privacy.[241] AI's capacity for prediction and inference adds to these concerns.

This has led to calls for professional and legal ethical codes to be developed that govern the design and application of AI technologies and apply to the activities of both governments and private sector organisations and entities.[242]

The European Union has introduced the first piece of legislation to address algorithmic discrimination in the European General Data Protection Regulation. This recognises the effect of algorithmic decision making on fundamental rights and addresses algorithmic discrimination, which occurs when an individual or group receives unfair treatment as a result of algorithmic decision-making. The ERDP addresses three principles:

- Data sanitisation – removal of specific categories from data sets; prohibition against "processing of data revealing racial or ethnic origin" and other "special categories" (Article 9); and prohibits decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significant effects against him or her" that is "based on the special categories of information referred to in Article 9" (Article 22)
- Data transparency – right to an explanation where entitled to information about logic involved and envisaged consequences (Article 13, 14)

237 State v. Loomis 881 N.W.2d 749 (Wis. 2016) at 769.

238 Ibid.

239 In 2014, then U.S. Attorney General Eric Holder raised concern about algorithms that produce risk assessments that seek to assign the probability of individual's likelihood of committing future crimes: "Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice… they may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society. See https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-national-association-criminal-defense-lawyers-57th.

240 The report by Pro Publica, a non-profit newsroom based in the US, investigated whether the use of algorithms by courts and law enforcement to predict the likelihood of a defendant re-offending were bias against African Americans. It obtained the risk scores assigned to more than 7,000 people arrested in Florida in 2013 and 2014 and checked to see how may were charged with new crimes over the next two years. They found that only 20 percent of the people predicted to commit violent crimes actually went on to do so. Significant racial disparities were found to exist, with the formula more likely to falsely flag black defendants as future criminals, wrongly labelling them this way at almost twice the rate as white defendants. See https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

241 Ibid p 28.

242 Ibid pp 32-34.

- Third party audit of algorithms – anticipated by data impact assessments under Article 24 requiring data controllers to evaluate "the risks of varying likelihood and severity for the right and freedoms of natural persons."

In New Zealand, concerns have been raised about the use of computer-based risk prediction models by the Accident Compensation Corporation (ACC) to profile and target clients. University of Otago researchers have warned against the dangers of such tools.[243] While final decisions appear to come down to the case manager, the researchers raised concerns that "their decisions are guided by advice generated automatically by a machine, based on a large set of data extending far beyond their own experience." The researchers recommend that Governments and companies consider the following when using such tools:

- Accuracy of the tool, including a thorough description of the data set on which it was assessed
- Ability to explain how the tool works so that clients can appeal decision
- Distortion in the way the agency pursues its policy objectives
- Responsibility to make fair and humane decisions
- Whether the tool implicitly discriminates against individuals
- Training employees in the use of the system

## 6.5 Role of Business

While Governments are primarily responsible for protecting human rights, the United Nations Guiding Principles on Business and Human Rights (UNGPs) make clear that all businesses have a responsibility to respect human rights.[244] The UNGPs are the authoritative global standard on business and human rights, endorsed by the United Nations Human Rights Council in 2011. They consist of 31 principles that set out the expectations of states and businesses human rights.

Under the UNGPs, States must protect against human rights abuses within their territory by third parties, including businesses, and should set clear expectations that businesses respect human rights. Businesses are also required to respect human rights. The foundation principle of the corporate responsibility to respect human rights is that businesses should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. The three key components of the corporate responsibility to respect human rights can be summarised as:

- A public commitment to respect human rights: The responsibility to respect human rights refers to internationally recognised human rights, including the International Bill of Human Rights, International Labour Organization's (ILO) Declaration on Fundamental Principles and Rights at Work.
- An ongoing process of human rights due diligence: This includes an assessment of risks to human rights; integrating findings of human rights impact assessments across relevant internal functions and processes; and tracking the effectiveness of response to human rights impacts.
- Having processes in place to enable a remedy when companies identify that they have caused or contributed to adverse human rights impacts

The UNGPs are increasingly important as businesses gather vast amounts of personal data about individuals and use it for purposes that it was not originally intended for, placing individual data privacy at risk. These issues were recently brought to light after Facebook admitted that Cambridge Analytica, a data mining and targeting company, used the personal data of 87 million of its users to create psychographic profiles. The international human rights framework and importantly the UNGPs are becoming more relevant as individuals are becoming increasingly concerned about the use of personal data by

243 http://www.otago.ac.nz/humanities/news/otago664403.html

244 http://www.ohchr.org/Documents/Publications/GuidingPrinciples-BusinessHR_EN.pdf

private companies.[245]

New Zealand businesses also have responsibilities under the OECD Guidelines on the Protection of Privacy and Trans border Flows of Information. They key principles under these Guidelines are set out in Part I. They play a major role in guiding governments and businesses in their efforts to protect privacy and personal data, and regulate transborder data flows.

In New Zealand, the Data Futures Partnership (DFP), an independent group funded by the Government, was set up to identify challenges in the data-use system and to develop guidelines for public and private organisations. The purpose of the guidelines was to encourage organisations to utilise a "social licence" approach to data use. According to the DFP "the Guidelines focus on eight key questions that organisations can answer to explain how they collect and use data, to better build trust with clients and the wider community. The DFP explains:

> *When people trust that their data will be used as they have agreed, and accept that enough value will be created, they are likely to be more comfortable with its use. This acceptance is referred to as a social licence.*[246]

Businesses in New Zealand also have legal human rights obligations and human rights responsibilities in the context of surveillance and interception, particularly if they are required to supply data or user information to the government in response to a request that contravenes the right to privacy. Furthermore, businesses may be at risk of being complicit in human rights abuses if they provide mass surveillance technology or equipment to States without adequate safeguards in place.[247] The UN Special Rapporteurs for freedom of expression and counter-terrorism, and the OHCHR have raised concerns about the increasing reliance by States on the private sector to facilitate digital surveillance.[248]

In light of such risks, the UN General Assembly and UN Human Rights Council resolutions on the right to privacy in the digital age has called for Governments to:

- Refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way;
- Consider appropriate measures that would enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;
- Develop or maintain legislation, preventive measures and remedies addressing harm from the sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit and informed consent."
- Respect human rights in accordance with the UN Guiding Principles on Business and Human Rights; and
- Inform users of the collection, use, sharing and retention of data about them.[249]

245 International reports have found that the public is concerned about the use of personal data by private companies as much as they are government agencies. See Independent Surveillance Review: A Democratic License to Operate, Report of the Independent Surveillance Review, Royal United Services Institute for Defence and Security Studies (July 2015) p 35, para 2.24, p 44, para 2.53 https://www.rusi.org/downloads/assets/ISR-Report-press.pdf

246 http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/

247 See OHCHR Report, The Right to Privacy in the Digital Age, para 43

248 Report of SR on countering terrorism, Ben Emmerson (23 September 2014) paras 43, 57; Report SR on freedom of expression (30 March 2017).

249 General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/71/199 (19 December 2016); Resolution 34/7

NZ Human Rights.

Human Rights Commission
Te Kāhui Tika Tangata