

VICKY NOBLE

PRIVATE DATA AND THE PUBLIC GOOD

Submitted for LAWS 542: HEALTH LAW

Faculty of Law

Victoria University of Wellington

2017

CONTENTS

I	INTRODUCTION.....	3
II	PRIVACY AND THE PUBLIC GOOD: SOME INITIAL CONSIDERATIONS.....	4
III	THE GOVERNMENT’S SOCIAL INVESTMENT STRATEGY.....	4
IV	PRIVACY LAW INCLUDING PRIVACY PRINCIPLES AND THE HEALTH INFORMATION PRIVACY CODE.....	9
	A THE PRIVACY ACT 1993.....	9
	B THE HEALTH INFORMATION PRIVACY CODE 1994 (HIPC).....	11
V	PROPOSALS FOR REFORM OF THE PRIVACY ACT 1993.....	12
VI	CASE STUDY.....	13
VII	STAKEHOLDERS’ PERSPECTIVES.....	16
	A PERSPECTIVE 1.....	16
	B PERSPECTIVE 2.....	18
	C PERSPECTIVE 3.....	18
	D PERSPECTIVE 4.....	20
VIII	THE PRIVACY COMMISSIONER’S INQUIRY INTO MSD’S COLLECTION OF INDIVIDUAL CLIENT-LEVEL DATA FROM NGOS....	21
IX	CONCLUSION.....	23
X	BIBLIOGRAPHY.....	25

I Introduction

Internationally, and across many jurisdictions, there is a tension between the rights of individuals to have their privacy respected and the roles and responsibilities of Government in relation to how it protects these rights on the one hand and how it conducts itself as the governor and protector of this information on the other.

Most recently an issue has arisen in the New Zealand context (hereafter ‘the Case Study’) relating to privacy and a perceived conflict between the rights of individuals together with the non-governmental organizations (NGOs) working with them and the Ministry of Social Development (MSD). This has captured the attention of many, including the media, and triggered a Privacy Commission inquiry.¹

Whilst some may not view this issue as being all that significant when considering the myriad of political and cyber security events currently threatening the security and protection of information globally, it has touched a chord amongst many.

This paper will explore the Case Study from the perspectives of four key stakeholders, referring to a range of legislation that is primarily concerned with health, privacy and the rights of the individual. In so doing, it aims to describe and highlight how in one instance the government reconciles, or fails to reconcile, its responsibility to protect individual privacy with the need to uphold the public good. It will discuss more generally how modern political and economic drivers are challenging current legal requirements governing the collection, use, retention, storage, disclosure and dissemination of individual citizens’ data (with a backdrop of exponential growth in information technology developments) and directly challenging the rights of individuals to privacy. It will include some comments on the Privacy Commissioner’s recent report to the Minister of Justice regarding Privacy Act reform.

¹ John Edwards *Privacy Commissioner’s Inquiry into the Ministry of Social Development’s Collection of Individual Client-Level Data from NGOs*. (April 2017).

II Privacy and the Public Good: Some Initial Considerations

Privacy can be variously defined. One definition of privacy is that it ‘is probably best understood as an individual human right, one that may be breached by someone with no relationship with the individual concerned’.² Distinctions are frequently drawn between the right to privacy and confidentiality. Within the New Zealand context individuals can expect to enjoy the right to privacy by having control over the ‘collection and use’³ of information that is considered sensitive to them. Any such material that is considered sensitive and is then published without that person’s permission is considered by law to be a breach of privacy.

The public good, a concept that dates back to the Greek philosophers, is variously defined, but is usually conceived of as a good that benefits society as a whole, and that government has a responsibility to uphold. Depending on how it is defined it can also be construed as providing benefits to individuals, groups or communities within society as well to society as a whole.

In the context of this Case Study it is important to consider two key factors relating to the proper balance between privacy and the public good. These are: the New Zealand Government’s social investment strategy; the New Zealand laws, principles and codes relating to privacy.

III The Government’s Social Investment Strategy

The current New Zealand government is taking a social investment approach to purchasing health and social services so as to improve the health and wellbeing of all members of society. This approach endeavors to use evidence-based policy-making and big data to ensure that health and social services are provided more efficiently and with more effective results. There are many ways of achieving this: applied research; monitoring and evaluation built into any given programme design; the use of new

² Peter Skegg and Ron Paterson, (eds) *Health Law In New Zealand* (Thomson Reuters, Wellington, 2015) at 321.

³ Peter Skegg and Ron Paterson, (eds) *Health Law In New Zealand* (Thomson Reuters, Wellington, 2015) at 321.

methodologies and new ways of managing and manipulating big data. A key issue, one that is central to this Case Study, is the level of detail of the data needed to achieve this, and in particular to what extent it justifies accessing detailed identifiable client-level information.

New Zealand's social investment policy has its origin in the current National Party's focus on a more evidence- and results-based approach to the commissioning of social services. It is regarded as the brainchild of former Minister of Finance Minister (and now Prime Minister) Hon Bill English and former Minister of State Services and Social Development Hon Paula Bennett. Starting in 2011 policy development in this field was located in the New Zealand Treasury. In April this year (2017) the Minister of Social Investment, the Hon Amy Adams, announced the creation of a Social Investment Agency (SIA), replacing an earlier Social Investment Unit. This new agency is to be launched on 1 July 2017, consolidating the New Zealand Treasury's and other government ministries' policy development and work programmes over the last six years.⁴

Since 2015, the Government has increasingly moved to restructure its approach to social investment policy. It has done so by getting various government agencies (including the Ministries of Health, Education, Social Development and Justice) to collaborate and cooperate, partly by pooling data so as to minimise duplication and overlap. Statistics New Zealand has provided the warehouse for this data through its Integrated Data Infrastructure.⁵ Data has been collected, stored and shared in accordance with privacy, security and confidentiality provisions of the Statistics Act 1975 and the Privacy Act 1993. No security breaches are known to have ever occurred.

A range of papers relating to social investment policy development dating back to early 2015 and through to 2017 are readily available on the New Zealand Treasury's website.⁶ A series of Analytical Papers focused on the role of data in support of the social investment strategy, in relation to children, youth and young adults at risk of

⁴ <https://www.beehive.govt.nz/release/changing-lives-through-social-investment>.

⁵ www.stats.govt.nz.

⁶ <http://www.treasury.govt.nz/publications/research-policy/ap>.

poor outcomes.⁷ These Analytical Papers sourced their data from Statistics New Zealand's Integrated Data Infrastructure and utilised a range of predictive modelling methodologies. It should be noted that a number of the findings have been scrutinised and subsequently criticized for having a number of shortcomings, ethical and cultural.⁸

The long-term goal of the Government's social investment strategy is twofold: firstly, to improve the lives of New Zealanders, particularly the most vulnerable; and secondly, to secure overall financial efficiency by eliminating the unnecessary waste caused by individual government agencies engaging in variable, uncoordinated, and disaggregated strategies and work programmes.

The social investment strategy is described in a New Zealand Treasury policy paper⁹ as being 'about improving the lives of New Zealanders by applying rigorous and evidence-based investment practices to social services. By gaining a clearer understanding of the indicators that are associated with poor outcomes, social sector and community organisations can identify where to invest early rather than deal with problems after they have emerged.'

The New Zealand Cabinet's definition of social investment is more detailed. As provided by the Social Investment Unit, this is as follows:

“Social investment puts the needs of people who rely on public services at the centre of decisions on planning, programmes and resourcing, by:

Setting clear, measurable goals for helping those people;

Using information and technology to better understand the needs of people who rely on social services and what services they are currently receiving;

Systematically measuring the effectiveness of services, so we know what works well and for whom, and then feeding these learnings back into the decision-

⁷ Insights – informing policies and services for at-risk children and youth (AP 17/02) (June 2017).

Christopher Ball Sarah Crichton Robert Templeton and Sarah Tumen – The Treasury. Rissa Ota and Conrad MacCormick – Ministry of Social Development. *Characteristics of Children at Greater Risk of Poor Outcomes as Adults* (The Treasury, Analytical Paper 16/01, February 2016).

⁸ Tim Dare. *Predictive Risk Modelling and Child Maltreatment. An Ethical Review*. (University of Auckland, 2013).

⁹ <http://www.treasury.govt.nz/statesector/socialinvestment>.

making process Purchasing outcomes rather than specific inputs, and moving funding to the most effective services irrespective of whether they are provided by government or non-government organisations.”¹⁰

A number of questions have been asked about the Government’s current social investment strategy. Some of these have been critical or negative. They include such concerns as to whether the social investment approach enables us to learn anything that is not already known; whether by singling out individuals or families/whanau the data will not further stigmatize an already vulnerable sector of our society; and importantly, whether policies are in place to provide effective support to vulnerable groups if indeed the data does in fact identify them correctly. They also include ethical concerns as to whether the strategy is culturally appropriate, given that a high proportion of those identified have been shown to be Maori.

Even more critical analysis has cast doubt on the whole concept of social investment as a policy or strategy, arguing that it really represents a misuse of agency time and resources, since the numbers of vulnerable people in New Zealand are proportionately quite small and can be readily identified, without the putative benefits of sophisticated methods of big data analysis. The issue, such an argument suggests, is not to apply big data analysis, but rather to work with such people in a person-centered way that avoids stigma or incorrect analytically-based conclusions, and can ensure instead, that existing social service resources are used in a less impersonal, more responsive way.

Other comments and commentaries have been more positive. Professor Rhema Vaithianathan, co-director of the Centre for Social Data Analytics in the School of Economics at Auckland University of Technology, has written widely on the subject of the Big Data revolution¹¹ and the likely long term benefits of having accurate data readily available to help support improved policy-making, specifically with regard to government-funded health and social services. Vaithianathan applauds the

¹⁰ <https://siu.govt.nz/assets/Uploads/Cabinet-Paper-Implementing-Social-Investment-Dec-2015.pdf>.

¹¹ <http://www.stuff.co.nz/national/politics/opinion/85416929/rhema-vaithianathan-big-data-should-shrink-bureaucracy-big-time>.

government's investment in the Integrated Data Infrastructure¹², arguing that access to this information enables greater transparency in decision-making. In her view, taking the politics out of the equation when government determines what services to purchase ensures that there is a greater likelihood of improved continuity of policy across election cycles.

Questions have also been raised about how much individual client-level data is really needed, how it should be collected, and how it should be protected and secured. If personal data has to be given, one recourse that is currently being more fully explored is 'de-identifying' or anonymising critical aspects of the data on a stringently controlled basis.¹³ (Interestingly, de-identifying data and the need for greater protections is included in the Privacy Commissioner's current recommendations for Privacy Law reform, which will be considered briefly later). This data is identifiable client-level data that has been effectively and securely made anonymous, or anonymised. Vaiathanathan has argued that such data, which she calls 'confidentialised data', can provide a significant amount of analysable data that can be protected with appropriate levels of control and security – indeed enough data for all practical purposes when it comes to social investment policy development. Her confidence in the ability of government to control and secure such data seems to be borne out by the fact that, as mentioned earlier, Statistics New Zealand has for many years been the third party holder of New Zealand's data and has managed to keep this data secure and unbreached. Examples of data effectively collected and safely stored include the New Zealand census and the New Zealand Health Survey.

Despite Vaiathanathan's optimism, there are concerns that 'de-identifiable' or 'confidentialised' data may, in the end, be less confidential or 'de-identified' than its proponents hope. A number of issues relating to controls on re-identification and the problems and risks associated with it are highlighted in the proposals and recommendations for Privacy Act reform that the Privacy Commissioner recently

¹² http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure.aspx.

¹³ Kirsten Lovelock, Robin Gauld, Greg Martin and Jayden MacRae. *Exploring the Ethics of the Use and Commercialisation of New Zealand Public Health System Data*. Policy Quarterly vol 11, Issue 4, November 2015. At 77-84.

submitted¹⁴. The Privacy Commissioner, John Edwards, cited six examples of failures to successfully anonymise data. The most notable (and relevant for the purposes of this paper) refers to a case where the Massachusetts Group Insurance Commission ‘released anonymised health data on state employees.....to help health researchers to improve health care’.¹⁵ Despite identifiers such as names, addresses and social security numbers being removed, a research student used the electoral rolls for the area to identify de-identified datasets and to derive identifiable client-level data.

All the examples cited by the Privacy Commissioner highlight the fact that despite assurances that the privacy of individual information contained in datasets is well protected through high levels of security, flaws and vulnerabilities often become evident after the fact. Public confidence and trust are undermined, budgets are compromised, and legal cases ensue.

IV Privacy Law including Privacy Principles & the Health Information Privacy Code

Privacy in New Zealand is protected by law. In the health sector it is also regulated by a privacy code.

A The Privacy Act 1993

The Privacy Act 1993 (hereafter ‘the Act’) is primarily concerned with the promotion and protection of the privacy of the individual.¹⁶ Its publication established two important fundamentals. Firstly, it set clear guidelines for the collection, use and disclosure of information relating to individuals by public and private sector agencies.¹⁷ And secondly, it established the rights of individuals to access information

¹⁴ John Edwards *Privacy Commissioner’s Report to the Minister of Justice under Section 26 of the Privacy Act. Six Recommendations for Privacy Act Reform.* (February 2017).

¹⁵ Above n13.

¹⁶ Privacy Act 1993 133.

¹⁷ Privacy Act 1993 133 (a)[1].

held about them by public and private agencies.¹⁸ Twelve privacy principles¹⁹ are set out in the introduction to the Act and form the foundation of the law.

A significant part of the Act is concerned with information sharing and matching and lists the agreements that exist between government and other international and domestic agencies.²⁰

The Act also created the role of the Privacy Commissioner (the Commissioner) and provided for powers within that role to “investigate complaints about interferences with individual privacy”.²¹ The Commissioner is defined as a ‘corporation sole’ and is recognized as a Crown Entity.²² The Commissioner’s function, powers and duties are significant, far-reaching and comprehensive.

One of the most important responsibilities of the Commissioner is a statutory requirement to report to parliament on the functioning and application of the Act in relation to new legislation. The Office of the Privacy Commissioner responds regularly via the submission process to achieve this aim. Its submissions and reports are made available to the public via its website.²³

Section 26(1) of the Act provides for a review of the Act at intervals of no more than 5 years and no less than 3 years. Sections 26(1)(b) and (c) refers to the consideration of amendments. Part 6, s 46 provides for the Commissioner to issue a code of practice.

The Act does not apply to the media and its news gathering activities. “A new tort of unreasonable interference with personal privacy”²⁴ is based on common law principles and enforced by the courts, rather than by the Privacy Commissioner.

¹⁸ Privacy Act 1993 133 (a)[2].

¹⁹ Privacy Act 1993 Part 2 section 6.

²⁰ Privacy Act 1993 Part 9A and Part 10.

²¹ Part 8.

²² Part 3 ss (2)[a] and (2)[b].

²³ www.privacy.org.nz.

²⁴ Peter Skegg and Ron Paterson, (eds) *Health Law In New Zealand* (Thomson Reuters, Wellington, 2015) at 322 highlighting *Hosking v Runting* (2005) 1 NZLR 1 (CA).

There are New Zealand examples of this tort in relation to the disclosure of health and other personal information.²⁵

B The Health Information Privacy Code 1994 (HIPC)

The HIPC was issued in 1994 by Bruce Slane, the then Privacy Commissioner, under s 46 and in accordance with s 48(1) of the Privacy Act 1993.

The HIPC is recognized as a code of practice. It clearly describes what classes of information it applies to and to which services. The focus is on all publicly and privately funded health and disability services as well as agencies engaged in the training, registration and discipline of health professionals. It also applies to agencies providing health, disability, accident and/or medical insurance.²⁶

The HIPC includes twelve Rules that are based on the twelve privacy principles established by the Privacy Act 1993. They are explicitly designed to address privacy issues and practice, particularly those relating to the health information held by public and private health agencies. They are intended to provide assurance to people accessing services from any health care provider (hospital, doctor or other health provider) that the information about them needed to provide their care is collected and used properly.²⁷

The HIPC Rules are clearly described. Exceptions to these rules are relevant, appropriate and able to be applied. They are presented in such a way that health providers and health care professionals alike should be in no doubt as to their obligations.

The HIPC provides a valuable and important framework for health care providers and health care professionals.

²⁵ Peter Skegg and Ron Paterson, (eds) *Health Law In New Zealand* (Thomson Reuters, Wellington, 2015) at 322 *P v D* (2000) 2 NZLR 591 (HC).

²⁶ Health Information Privacy Code, 1994 s 4(2)(1).

²⁷ Healthpoint Health Information Privacy Code <https://www.healthpoint.co.nz/useful-information/patient-rights/privacy-code/> accessed 10 May 2017.

There have been a number of breaches of the HIPC involving health practitioners. Some of these have been high profile and have aroused a great deal of media interest. They have highlighted how slow some of New Zealand's larger health care organizations (for example District Health Boards) have been in not only developing policy to protect patient information but also in providing education to their employees.

V Proposals for Reform of the Privacy Act 1993

Privacy Act law reform has been on the agenda for a number of years. As mentioned earlier, the Privacy Commissioner has a statutory obligation²⁸ to undertake periodic reviews of the Privacy Act and seek feedback on their views of it from a broad range of stakeholders. The New Zealand Law Commission also undertook a comprehensive review of the Privacy Act, a review that took it five years, and was finally completed in 2016. This was a significant undertaking with some impact, though some of its findings have apparently been superseded. Addressing their content and implications is beyond the scope of this paper.

The most recent of the Privacy Commissioner's periodic reviews, which was submitted to the Minister of Justice, the Hon Amy Adams, in 2017, recommends six ways of modernising the Privacy Act. These six recommendations all seek to significantly strengthen the Privacy Act through its more strict and stringent application, and through ensuring greater compliance with its key provisions. This would partly be done by providing the Privacy Commissioner himself with much greater powers. These would enable the Commissioner to secure the use of civil penalties including fines, and otherwise enforce charges relating to criminal offences. A key consideration in the recommendations is the need to improve government agency compliance with the Privacy Act, and to take the Act more seriously, steps that would take into account the new challenges of the digital age and that would be in line with emergent international practice. Of particular relevance are the Privacy Commissioner's comments on privacy law as it relates to emergent trends in information technologies that allow for data to be exploited and misused

²⁸ Privacy Act 1993, s 26.

uncontrollably. This is not, of course, a trend peculiar to New Zealand, nor is New Zealand alone in starting address the need for more stringent and enforceable regulation of information technology usages to address gaps and weaknesses in current legislation. It is part of a growing global trend in which governments and others are coming to recognise the very significant challenges caused by the fast-moving developments in information technology that are occurring within what is essentially a borderless context.

In more detail, the Privacy Commissioner's recommendations are as follows. The first two focus on strengthening current legislation by highlighting a key privacy principle that an individual retains the right to ownership and control of her or his information, and that if an individual's information is indeed going to be 'anonymised' as part of big data analysis there should be firm processes in place to ensure that it remains so. The third recommendation focuses on strengthening agency compliance with the Privacy Act, particularly in relation to system management of data protection. Agencies will be required to provide greater assurances as to how data is safely managed and will be held to a far greater account by the Privacy Commission when issues occur than they are at present. The fourth recommendation seeks enhanced authority for the Privacy Commissioner so that significant civil penalties can be imposed for repeated breaches of the Privacy Act. The fifth recommendation relates to increasing the scope of prospective criminal convictions under the Act. And the sixth and final recommendation is for reform of public register privacy principles.

VI Case Study

The Case Study consists of an issue comprising a series of recent events. It concerns the question of whether the government is entitled to demand individual client-level data as part of contracts awarded to NGOs for social services ('NGOs').

In early March 2017, Brenda Pilott, chairperson of the NGO community group collective ComVoices, was interviewed on the Radio New Zealand programme *Nine to Noon* by interviewer Kathryn Ryan, to convey a concern about the work she is involved in. She spoke on behalf of ComVoices, which represents more than 800

NGOs and social service agencies. The kinds of services provided by these NGOs and social service agencies are diverse and include “budgetary advice, counselling in response to sexual violence or trauma, respite care for children whose families are in distress, settlement support services for refugees and migrants, elder abuse and neglect services, support for people living with HIV, anti-bullying programmes and others”.²⁹

In the interview, Pilott described how in order to be considered for a renewal of an existing contract with the Ministry of Social Development (MSD), NGOs would now have to provide MSD with comprehensive and identifiable information about the people receiving services. She noted that this was a new condition that would come into force on 1 July 2017. Previous contracts had required the reporting of non-identifiable information, a requirement that had not been contested and had been complied with.

Under the terms of the new conditions, NGOs would require every person accessing their services to consent to the sharing of their personal details – including their name, address, gender, date of birth, primary ethnicity, iwi, as well as dependents’ names, date of birth and relationships to the client. In her opinion, the new requirement would breach the privacy of those receiving services. Previously, people accessing services had been assured of anonymity. She was concerned that people who had previously considered accessing a service did so knowing that their privacy was assured, but might no longer wish to access the service if their data was no longer confidential. In her opinion vulnerable people would most likely be deterred from seeking help.

Pilott said ComVoices was concerned people would “walk out the door” instead of giving up their personal details. “There have been quite a substantial number of people who are saying ‘No, I do not want my information passed on’”, she went on.

“People who have been dealing with sexual abuse or mental health issues or drug and alcohol addictions, those who have been offending, but have not been arrested, or been violent – those are the very people you want most to get into the system, and they are the very people who are most likely to actually not access the service...We

²⁹ Above n 1.

would have thought that voluntary help seeking behavior is something that you would want to encourage before things get to the point where there's an arrest or a charge or a violent occasion or a child is hammered".³⁰

A deputy chief executive of MSD, Mr Murray Edridge, was interviewed the next day on the same Radio New Zealand programme *Nine to Noon*, again by interviewer Kathryn Ryan³¹. In the interview Mr Edridge was challenged to justify the new requirement. A focus of the interview - and the main substance of the discussion - was the extent to which the new contractual demand was a breach of privacy. Mr Edridge insisted that MSD was well within its rights to make this new demand. He described the criteria for this justification. MSD needed to have assurance that the significant investment made in regard to services contracted out represented value for money. In a related point, MSD needed to know and understand the number of different social services that an individual and/or their family or whanau was receiving. In his opinion, MSD could only get this information by having identifiable client data. Mr Edridge concluded that MSD would benefit overall from the data gathered, and that the proposed data-sharing process was in line with MSD's new approach to contracts for NGOs providing social services, as well as with the Government's social investment approach to targeting services.

Subsequent to these two radio interviews a number of other social service agencies, voluntary groups and other non-profit groups raised concerns similar to those raised by Pilott. Salvation Army spokesperson Major Pam Waugh, for example, said that the charity was disappointed by the new requirement, which had created "some unrest. We need to protect our client's trust in us as an agency," she said, "and this may be eroded if clients feel that we are collaborating with Government".³²

In the meantime, the Privacy Commissioner was undertaking an inquiry into the government's personal-data collection practice as proposed by MSD – in other words, into the circumstances of the Case Study just described. The inquiry, was carried out under s13 of the Privacy Act 1993, and took as its basic terms of reference the Act's

³⁰ stuff.co.nz *Government demands non-profit clients' personal data* 2 March 2017.

³¹ radionz.co.nz *Nine to Noon* programme 3 March 2017.

³² Above n 30.

twelve privacy principles.³³ S13 includes a wide range of provisions regarding the Privacy Commissioner's mandate, including his ability to inquire into any matter where privacy may be infringed; his ability to provide advice to a Minister; his ability to make suggestions in the interests of privacy, and his ability to make public statements.

The Privacy Commissioner released his report, entitled 'Inquiry into MSD Collection of Client-Level Data from NGOs', on 4 April 2017. The report found that the MSD's proposed new data collection process was inadmissible under the terms of the law, and specifically the Privacy Act 1993. A summary of his findings is provided below.

VII Stakeholders' Perspectives

In contrast to the Privacy Commissioner, who investigated the Case Study under the terms of the twelve privacy principles laid down by the Privacy Act 1993, this paper explores the multiple and intersecting perspectives of the key stakeholders in the Case Study, highlighting the differing concerns and expectations they had with respect to the protection of private data and the public good. These key stakeholders consist of: (A) the NGOs; (B) the practitioner(s), i.e. the person or people delivering these services to clients; (C) the clients receiving the services; (D) MSD.

As mentioned at the outset, by considering these varying perspectives individually and as a whole the aim is to assess the extent to which individual privacy concerns have been reconciled with the public good, and the extent to which they clash.

At the end of the review of the different stakeholders' perspectives, a brief review is included of the findings of the Privacy Commissioner's inquiry and recommendations.

A Perspective 1

The NGO under contract to MSD that is responsible for delivering a service to clients

³³ Privacy Act 1993, Part 6.

In the case of the NGOs, the Case Study highlights how they have found themselves facing a Hobson's choice. Many NGOs depend on MSD to sustain their business. If they decline to follow the directive of MSD to include identifiable client level data then their sustainability is threatened. If they accept the directive then as they see it, they compromise their relationship with their clients. Currently, this relationship is based on trust. By requiring their clients to agree to confidential information being passed on to the government, they risk undermining this trust.

NGOs see themselves as having responsibilities as well as legal obligations.

As far as their responsibilities are concerned, they see themselves as having three main responsibilities. The first is to their clients; the second is to MSD, the purchasing agency with which they have a contract; and the third is to the people they employ.

Taking each of these in turn:

a) With respect to clients, NGOs seek to provide the service(s) contracted for to the best of their ability within available resources. By undertaking this work they are committed to a number of privacy principles. These are embedded in various documents, but mainly provider/client relationship agreements, consent forms and individual NGO codes of conduct. If an NGO is a provider of a health and/or disability service, it is required to apply both the Code of Health and Disability Services Consumers' Rights³⁴ and the Privacy Act's privacy principles.³⁵

b) With respect to MSD, the NGO seeks primarily to meet the service specifications of the contract as agreed and to provide reports on an as agreed basis.

c) With respect to its responsibility to the people it employs, the NGO primarily relates to its employment agreement, which includes reference to its health and safety obligations.

³⁴ Code of Health and Disability Services Consumers' Rights - Health and Disability Commissioner, 1994.

³⁵ Privacy Act 1993 Part 2.

As far as their legal obligations are concerned, NGOs are aware that they have to meet their contractual obligations under contract law. They have to ensure that an appropriate standard of care is provided³⁶ and that they employ appropriately skilled and competent practitioners.

B Perspective 2

The practitioner(s) delivering services to clients.

When considering the perspective of the practitioner(s) providing the services referred to, it is important to note the diverse range of practitioners likely to be employed. They may include social workers and clinical psychologists, as well as a range of other practitioners and support workers who may or not be regulated by the Health Practitioners Competency Assurance Act.³⁷

Practitioners delivering a health and/or social service have both an ethical and a professional duty to maintain the privacy and confidentiality of a client's information.³⁸ Individual professional ethical professional codes of conduct apply.

As already mentioned, many of the services highlighted in the Case Study are engaged in the delivery of sensitive services to vulnerable people. Because of this, practitioners will be concerned to maintain a high level of mutual trust and confidentiality, one that lies at the heart of their relationships with clients. For the relationship to be therapeutic the client needs to be able to trust the practitioner and be confident that anything shared as part of an interaction is not disclosed. A loss of mutual trust and/or confidence can have a serious impact on a client's willingness to engage.

C Perspective 3

A client accessing and receiving a service

³⁶ Code of Health and Disability Services Consumers' Rights - Health and Disability Commissioner, 1994.

³⁷ Health Practitioners Competence Assurance Act, 2003.

³⁸ Health Practitioners Competence Assurance Act, 2003.

A client accessing a service from an NGO can and should have the same expectations as any other person accessing services across the health and social care sector. The Health and Disability Code of Consumers' Rights³⁹ provides for a number of rights to be upheld, among them rights to informed consent; to be fully informed; to be treated with respect; to receive skilled care; to privacy; to fair and equitable access; to a culturally appropriate experience; and to be able to complain.⁴⁰

A review of the Health and Disability Commissioner Act 1994 and the Code of Health and Disability Services Consumers' Rights⁴¹ received submissions as to whether or not health information privacy issues should be dealt with by the Health and Disability Commissioner. The Ministry of Health was concerned that an 'overlapping jurisdiction between the Health and Disability Commissioners and the Privacy Commissioner could lead to inconsistency in the application of the law and confusion for the public about the two roles'⁴² and was not persuaded that an amendment of the Act was necessary.

When receiving a service, therefore, a client can expect that the privacy principles of the Privacy Act 1993 as well as the Code of Health and Disability Services Consumers' Rights will be followed. According to these, information must be accurate and stored securely, must not be shared without permission and must be made available when requested. Permission must be sought when gathering it in the first place and the client needs to know what it will be used for. When information about a client is no longer needed it must be destroyed.

As the Privacy Commissioner has pointed out, examples of when a client's privacy is breached include when information is given to someone the client didn't authorise, when incorrect or wrong information about the client is held, when information is

³⁹ Code of Health and Disability Services Consumers' Rights – Health and Disability Commissioner, 1994.

⁴⁰ Above n 38.

⁴¹ Report to the Minister of Health. *Review of the Health and Disability Commissioner Act 1994 and the Code of Health and Disability Services Consumers' Rights* (June 2014).

⁴² Above n 40. At 10.

collected without the client's consent; or when the client asks for information about themselves and it is refused.⁴³

What other perspectives can clients be expected to have, or bring to bear? A key factor, mentioned already, is trust. NGOs and others, including the Privacy Commissioner, are concerned about the vital importance of maintaining clients' trust. If a client's privacy is breached, for example through the indirect effects of social investment policy being misapplied, trust will quickly erode. Vulnerable people accessing or seeking to access social services often already suffer from a sense of being stigmatised (for example because of being subject to intrusive scrutiny by Work and Income when applying for benefits), and so are suspicious about what might happen if they divulge too much personal information. For such people the protection of personal data is critical or even fundamental. Only if they are absolutely convinced that it is reliably protected will they readily agree to sharing it, and even come to accept that doing so may benefit future generations, thus contributing not only to the welfare of themselves and their families/whanau, but also to the public good.

D Perspective 4

MSD

MSD's perspective is encapsulated in the comments Senior MSD manager Mr Murray Edridge made during the Radio New Zealand interview mentioned earlier.⁴⁴ In it he noted that what he called the Ministry's community investment strategy (which supports and aligns with the Government's social investment approach) wanted to ensure that decision-making on the spending of \$320 million of taxpayers' money each year was based on fact and not "intuition". MSD's website describes MSD as moving the social sector to "a results-focused and evidence-based purchasing strategy".⁴⁵ He also argued that "collecting client data helped MSD understand who is using the programmes and services it funded and what impacts they are having".⁴⁶

⁴³ Your Personal Information. Know your Privacy Rights. Privacy Commissioner. <https://www.privacy.org.nz/your-rights/privacy-introduction/>.

⁴⁴ radionz.co.nz *Nine to Noon* programme 3 March 2017.

⁴⁵ msd.govt.nz.

⁴⁶ radionz.co.nz *Nine to Noon* programme 3 March 2017.

VIII The Privacy Commissioner’s Inquiry into MSD’s Collection of Individual Client-Level Data from NGOs⁴⁷

The Privacy Commissioner (‘the Commissioner’) released his report on MSD and the collection of individual client-level data in April 2017. This report was much anticipated for a number of reasons. Firstly, it was based on a wide range of sources, including email exchanges, policy documents, advice to ministers and sought feedback from many of the NGOs involved in the issues addressed in this Case Study. Secondly, while it was being undertaken, contract negotiations between MSD and affected NGOs were continuing apace against the backdrop of ongoing argument and debate in the public arena. Thirdly, a serious security breach occurred with the database where MSD proposed to store – and indeed was already storing NGO data. This breach resulted in the Minister of Social Development, the Hon Anne Tolley, shutting down the database and declaring that the proposal for NGOs to provide identifiable client-level data would be put on hold subject to an internal MSD review. She also ordered an employment investigation, that is, an investigation into who might have been directly responsible for the breach, to be undertaken by MSD. Subsequently the MSD deputy chief executive, Mr Edridge, resigned.

The Commissioner elected to undertake the inquiry under s13 of the Privacy Act 1993.⁴⁸ This provides for the Commissioner to make statements, receive recommendations and consult the public, makes suggestions, provide advice and otherwise “inquire generally into any matter if it appears that the privacy of the individual is being, or may be infringed thereby”.⁴⁹ In explaining this decision in the introduction to the report, the Commissioner referred to two other sections that he gave consideration to. The first of these was s 66, but he noted that this section was concerned with a breach of an information privacy principle, and that “It is not a simple matter to determine in advance if a policy amounts to a breach”.⁵⁰ The Commissioner also noted that under s14(a) he was to have “due regard for the protection of human rights and social interests that compete with privacy, including

⁴⁷ Above n 1.

⁴⁸ Above n 46.

⁴⁹ Above n 1. At 4.

⁵⁰ Above n 1. At 7.

the general desirability of a free flow of information and the recognition of the right of government to achieve its objectives in an efficient way.” In doing so, he noted, “I acknowledge the legitimacy of the Government’s intention to assess the effectiveness of social services and prioritise its investment decisions.”⁵¹ In other words, he acknowledged in effect at the outset that his inquiry would take fully into account not just individual privacy concerns but also considerations that could be seen to contribute to the public good.”⁵²

In summary, the Commissioner concluded after undertaking his inquiry that despite the Government (MSD) having a legitimate right to expect a necessary level of reporting for services it has commissioned, it had not taken the requisite steps to ensure that its processes were sufficiently robust. Additionally, he was concerned that given the lack of due diligence applied to the commissioning process, public trust and confidence could be potentially undermined. Moreover, vulnerable people who needed to access the services might not do so, because they feared that their privacy would not be protected. As a result these users would not access services, and so “would not feature in data being used to inform government policy” and “would effectively become invisible”.⁵³ The outcome would therefore be directly counter to the intentions of the social investment approach. The Commissioner concluded that MSD’s policy relating to the requirement for NGOs to provide identifiable client-level data as part of their contractual obligations was “inconsistent with the principles of the Privacy Act and should therefore be amended”.⁵⁴

He made four recommendations. The first (and primary) recommendation upheld the Government’s (MSD) legitimate right to information and suggested that instead of storing NGO information in its own database, MSD should use Statistics New Zealand’s Integrated Data Infrastructure (IDI), which, he said, “would provide the highest level of confidence while still meeting many of the government’s goals”.⁵⁵ The three remaining recommendations focus on how MSD might mitigate existing risks and manage the unintended consequences of its current approach should it not be

⁵¹ Above n 1. At 3.

⁵² Above n 1. At 5.

⁵³ Above n 1. At 4.

⁵⁴ Above n 1. At 4.

⁵⁵ Above n 1. At 5.

possible to utilise Statistics New Zealand's IDI.⁵⁶ Of particular note is the emphasis he placed the need for a range of measures by MSD to limit the likelihood of vulnerable people being deterred from accessing services.

IX Conclusion

When considering privacy issues, the Case Study and the information on social investment policy and on privacy law provided as background to the Case Study, show that a line needs to be drawn between what individuals have a right to, and what the government needs to do when providing services that address the public good. The critical question raised by the Case Study is: what is the right balance between an individual's right to control her or his information and the government's need to access the information for the public good? When it comes to an individual's right to a service that protects her or his privacy on the one hand, and the government's need to provide social services that can be shown to be effective on the other, whose needs outweigh whose? With respect to privacy it is clear that ideally there should be a convergence or as close a convergence as possible between what individuals and government want and need.

As far as the differing perspectives of the stakeholders in the Case Study are concerned, ComVoice was justified in its grievance, a grievance that also affected health and social service professionals' relations with their clients. On the other hand MSD was not justified in demanding identifiable data without sufficient safeguards to process that data. As the Privacy Commissioner showed in his inquiry, the rights of individual clients and their family/whanau were in danger of being breached by a poorly devised policy – use by MSD of contracts requiring identifiable client-level data without appropriate protective measures. It is clear that if MSD had succeeded in imposing its new contracts on NGOs, these NGOs would have to tell prospective clients that their personal and identifiable details would have to be provided to MSD without enough safeguards, something that would potentially undermine trust and

⁵⁶ Above n 1. At 5.

worse, cause vulnerable groups of people to disengage entirely. These groups would be unlikely to have legal recourse under the terms of current privacy legislation.

In the New Zealand setting, government agencies need to restore confidence and trust in how government collects, stores and utilizes individuals' information in pursuit of the public good. The highest levels of assurance need to be provided to these individuals, and for that to happen it will take time to develop robust systems in a rapidly changing domestic and international information technology environment in which respect for individuals' rights to privacy must remain paramount. One of the most important of these systems relates to legislation and regulation. Therapeutic jurisprudence has a role to play in this regard and may provide an alternative means for considering the unintended consequences of government policy. Steps will have to be taken of the kind proposed by the Privacy Commissioner. As noted earlier, these include strengthening legislation relating to ownership of personal data; ensuring that any data that is 'de-identified' remains securely de-identified; and ensuring that the security, integrity and protection of individual data are more stringently regulated.

X Bibliography

Legislation

Privacy Act 1993.

Health Practitioners Competence Assurance Act 2003.

Health Information Privacy Code 1994.

Health and Disability Commissioner Act 1994.

Code of Health and Disability Services Consumers' Rights – Health and Disability Commissioner 1994.

Crown Entities Act 2004.

New Zealand Bill of Rights 1990.

Reports

Privacy Commissioner's Inquiry into MSD Collection of Client-Level Data from NGOs Report. 6 April 2017.

Privacy Commissioner's Report to the Minister of Justice under Section 26 of the Privacy Act Six Recommendations for Privacy Act Reform. 3 February 2017.

privacy.org.nz accessed 12 May 2017.

Independent review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data. 12 May 2017 accessed 17 May 2017.

Danijela Tavich. New Zealand Productivity Commission Research Note: Social sector productivity: a task perspective. May 2017.

Review of the Health and Disability Commissioner Act 1994 and the Code of Health and Disability Services Consumers' Rights. Report to the Minister of Health 2014.

Anna Davison Jean Beetham Jared Thomas Abigail Harding Vivienne Ivory and Chris Bowie. Public attitudes to data integration: Report prepared for Statistics New Zealand. Opus International Consultants (2015) Available from www.stats.govt.nz

Texts

Peter Skegg and Ron Paterson, (eds) *Health Law In New Zealand* (Thomson Reuters, Wellington, 2015)

Journal articles

Kirsten Lovelock Robin Gauld Greg Martin and Jayden MacRae. “Exploring the Ethics of the Use and Commercialisation of New Zealand Public Health System Data” (2015) 11 Policy Quarterly 4.

Samantha Beattie “Privacy and patient rights: does New Zealand need a right to informational privacy in the Code of Health and Disability Services Consumers’ Rights” (2013) NZLawStuJl 6 (2013) 3 NZLSJ 88.

David Wexler “Therapeutic Jurisprudence: An Overview”

<http://www.law.arizona.edu/depts/upr-intj/intj-o.html> accessed 16 June 2016

Word length: the text of this paper (excluding title page, footnotes and bibliography) comprises 7,256 words.