New Zealand's Data Future: A View From the Privacy Commissioner

---

Submission by the Privacy Commissioner

to the New Zealand Data Futures Forum

---

4 July 2014

Privacy Commissioner
Te Mana Matapono Matatapu

Introduction

This submission responds to the New Zealand Data Futures Forum's invitation to contribute to a debate on New Zealand's data future. It responds primarily to the Forum's second discussion document, and in particular describes how our existing regulatory framework for privacy is placed to respond to the challenges we face.

The wider use and re-use of data by business and government is inevitable. Many companies have already demonstrated the commercial benefits that can be obtained from the examination of information they can collect and hold about customers and potential customers.

For the public sector, the potential to design better policies and target resources more efficiently means that the re-use of data is in some sense a responsibility as much as an opportunity – taxpayers have paid for the collection their own information, and the government should be seeking to maximise the return of value to New Zealanders from it.

I have started from the position that the values or "principles" set out in the Forum's document are sound. I believe that the goal of achieving value, inclusion, trust and control does represent a useful framework with which to consider how we as a country grapple with the opportunities and challenges offered to us by a future where large scale data collection and analysis are ubiquitous.

Privacy has an important part to play in that future. As our lives become ever more enumerated and dissected, privacy and privacy law ensure we maintain the space to take control of defining our sense of self, and our belief in our ability to make autonomous decisions.

We are fortunate in New Zealand that we already have a robust legal framework for managing data, shaped around the Statistics Act and the Privacy Act in particular. These acts may not, however, cover the range of tasks that are needed to see New Zealand prosper in a data-driven future, and the time may have come to set up an independent body specifically focussed on maximising the benefits to New Zealand from data.

The Privacy Act forms a core part of the legal framework, and one that is arguably world-leading in managing the different values and interests in play in a data driven future. A recent article by an Australian legal academic described New Zealand's regulatory approach as a "jurisdictional benchmark". It deals particularly well with the widespread desire to realise value from data from re-combination and re-use. As such it deserves to be seen as a competitive advantage.

There are areas where the Privacy Act could be strengthened. In particular, there is no explicit prohibition on the re-identification of data from which identifying information has been removed. A prohibition of this nature could potentially increase public confidence in the safe use of "de-identified" or "anonymised" data.

Similarly further work could be undertaken on strengthening individuals' rights to have information about them deleted, again increasing their confidence that information provided is not necessarily provided forever. International privacy discussions have addressed some of these issues through the idea of a "right to be forgotten", though this is not yet a fully developed concept.

I also consider that the relationship between open data and personal information needs to be explored more fully, with the aim of developing a concept of "degrees of openness". Government efforts to provide open data have sought to exclude personal information, although what constitutes personal information is not necessarily well understood. This is not a sustainable approach.

Finally, there is a need to consider the regulation of public registers in New Zealand, and specifically, to implement the Law Commission's recommendations on the topic. Public registers play an important role in New Zealand's data landscape, but the current regulatory environment does not provide for effective use of public registers, nor does it effectively protect individual privacy.

The principles set out by the Forum are fundamentally sound

The Forum's second discussion paper set out four principles that it considered could form the foundation for New Zealand's data future:

- Value
- Inclusion
- Trust
- Control

I consider these principles are sound, and reflect what New Zealand and New Zealanders should aim to gain from our data future. I also agree with the Forum that these four principles are inter-dependent. From a privacy perspective, it is difficult to envisage a future where we are able to achieve the full societal and economic value of using data without inclusion and trust. These in turn cannot be achieved without providing an appropriate level of community and individual control.

The Forum's paper also acknowledges that these four values may sometimes be in tension. In making this acknowledgement the paper helpfully avoids a simple dichotomy between value and control or utility and privacy. This is an important point to recognise: a system that aims to maximise the benefits of data to individuals, society, and the economy must be flexible enough to resolve these tensions in different ways depending on the context, and to cater for a dynamic environment. We are unlikely to be successful if we seek to reduce these tensions to a simple formula that we attempt to apply for all places and all times.

New Zealand has a robust legal framework for managing personal information

New Zealand has a robust legal framework for managing personal information used for statistical and research purposes. The Statistics Act and the Privacy Act form the two major statutory components of this framework. The Official Information Act also plays an important role, as does the National Ethics Advisory Committee (NEAC) in the health sector.

The Statistics Act ensures the collection and maintenance of official statistics. The Department of Statistics is highly trusted as a custodian of statistical information, and recognises the importance of this trust for it to be able to effectively carry out its functions. This trust is reinforced by the statutory independence of the Chief Statistician, and the robust protections the Act places on statistical data.

Statistics New Zealand has recently provided greater and more flexible access to integrated microdata in Statistics' integrated data infrastructure, with a primary focus on achieving public benefit. This represents an appropriately cautious and stepwise approach to opening up Statistics New Zealand's data, and a robust case would need to be made if there was any desire to accelerate this process.

There may be a case for a 'Data Council'

The time may have come for an independent body to promote the ethical and safe use of data. While I play a role in setting limits on what can be done with personal information, my role is limited to personal information, and does not include a mandate to promote the wider use of data. Promotion of the more effective use of data raises a range of questions about infrastructure and capability that are not as yet part of any organisation's mandate. There is also an important distinction between privacy and ethics in data use, and there is no body charged with providing advice on what constitutes ethical practice outside of NEAC's role in the health sector.

The Privacy Act is already a competitive advantage

New Zealand's Privacy Act as it currently stands provides New Zealand with a competitive advantage in a data-driven future that seeks to adhere to the four values proposed by the Forum's paper.

- It already addresses effectively some of the major issues other countries are struggling with in regulating a data future
- It is not based on a model of ownership
- It is recognised as "adequate" by the EU, therefore freeing up the movement of information between the EU and New Zealand

The Privacy Act has already addressed some of the major challenges others are struggling with

There is a great deal of angst internationally about whether privacy frameworks in place in most OECD countries are fit for purpose in the new data environment. Most of the difficulties encountered overseas, however, are not a feature of New Zealand's privacy legislation.

There are two key features of New Zealand's privacy law that make it a potential model for managing privacy in a data-driven future:

- Its definition of personal information is broad enough to encompass de-identified and pseudonymous information
- It provides broad exceptions to principles on collection, use and disclosure where information will be used in a form in which individuals will not be identified

If agencies have a lawful purpose for collecting personal information and do not intend to use it in a form in which individuals will be identified, they can use and re-use it without having to obtain detailed consents that apply to all those future uses. In many jurisdictions this has been seen as a particular barrier to a more dynamic environment for data re-use. On the trust side, however, agencies still have responsibilities to collect only data they have a use for, to store it securely, and to delete it when they no longer have a use for it.

These exceptions encompass the majority of demand for re-use of data, which tends not to require individuals to be identified.

The Privacy Act is not based on a model of ownership

The Forum's second discussion paper emphasised the need to move away from concepts of ownership when considering the appropriate use of personal information. One of the reasons the Privacy Act can effectively regulate the innovative use of personal information is because it has never been based on a legal concept of ownership. Instead the Act, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data on which it is based, seek to codify a commonly held set of societal norms about how personal information should be used. In this respect, privacy law in New Zealand has always been based around the creation of a standalone bundle of rights that do not rely on establishing who might "own" information.

This feature of privacy law is often overlooked by those who collect and use personal information day to day. Agency structures and processes around data, and personal information specifically, are still often shaped around a model of ownership. This can prevent agencies from using personal information in ways that are allowed for by the Privacy Act. Ownership is also still commonly used by consumers as a starting point for discussions about privacy in everyday conversation. It is therefore understandable that the forum's paper talks about a need to "move away from a model based on ownership".

Care needs to be taken to ensure that this idea of "moving away" from an ownership model is not used as an excuse to weaken the existing legal rights of data subjects, which have their own independent basis. It remains critical to maintain a clear idea of who is responsible for data. The Privacy Act focusses this question on who holds or controls the data, the rights of data subjects, and the actions of agencies in those circumstances, rather than on the data itself.

The EU has recognised the Privacy Act as 'adequate'

In December 2012 the European Union recognised the Privacy Act as providing an adequate standard of data protection for the purposes of European Law. Only a handful of other countries have achieved this standard, and this represents a significant commercial advantage for New Zealand companies wanting to provide data processing services on a global scale.

Since 1995 European businesses have been prohibited by law from transferring personal information to countries outside the EU for data processing unless special contractual provisions are put in place. Providing these safeguards can be expensive and difficult. The finding of adequacy establishes that information can be transferred to New Zealand companies without the requirement for special contractual provisions.

There are some areas where steps could be taken to improve the environment for data

There are five areas where steps could be taken to better support the four values set out by the Forum:

- The Privacy Act should have stronger protections against re-identification of de-identified or pseudonymous data

- The Act could provide stronger rights to have information to be deleted
- A more nuanced approach to open data is required, based around an idea of 'degrees of openness'
- Work needs to continue on cross-border enforcement of privacy rights
- The government should implement the Law Commission's recommendations on regulation of public registers

The Act's protections against re-identification of data are insufficient, and an explicit prohibition on re-identifying data should be considered

Individuals' confidence in the use of de-identified data is in part determined by their belief that they will not be able to be re-identified. In order to achieve this, consideration should be given to whether the Privacy Act should contain an explicit prohibition on re-identifying previously de-identified data. An explicit prohibition could usefully reassure people that they have a means of redress if they suffered harm due to them being successfully re-identified from supposedly anonymous data.

Protection against re-identification is important because it can be surprisingly easy to identify individuals in supposedly de-identified data. Often the key link in a chain that allows an individual to be identified can be provided by seemingly innocuous pieces of information. For instance, in a seminal piece of research, Latanya Sweeney demonstrated that 87% of US citizens could be identified by date of birth, gender and zip code alone[1]. The typical US zip code contains 7,500 people. By way of comparison, the population of the average Statistics New Zealand mesh block is around 90.

The Privacy Act could provide stronger rights to have information deleted

Drawing on European debate the Forum's discussion paper raises the question as to whether there should be a "right to be forgotten". At this stage there is still debate as to what a "right to be forgotten" actually requires, let alone how it might be implemented. Nevertheless, the Privacy Act could provide individuals with stronger rights to have information about them deleted.

Granting individuals stronger rights to have information deleted has the potential to improve our ability to obtain value from data, because it could give individuals greater confidence that when they provide information, they have not necessarily given it away forever.

Individuals have existing rights under Principle 7 to have information corrected. That right includes the possibility that information should be deleted. But principle 7 generally only applies to information that is inaccurate, out of date, incomplete or misleading.

Principle 7 also has other important limitations. Agencies are not required to delete or correct incorrect information if they do not wish to, although they must note that the information is disputed. An argument could be made that they should at least have reason to believe that the information is correct despite the subject's claims to the contrary.

---

[1] L. Sweeney *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. (PDF).

There are also situations where individuals might expect information to be deleted where the information is accurate. For instance where an individual ceases their relationship with an organisation – for instance a customer loyalty scheme – they ought to be able to ask for historical information to be deleted or at least de-identified.

Any right to have information destroyed could never be absolute. Removing data from backups can be notoriously difficult. Many organisations – in both the public and private sector – have legitimate reasons for holding on to information that individuals would prefer to have deleted. These include public sector organisations' legal obligations to create and maintain records under the Public Records Act. Similarly an agency that had deleted information in good faith couldn't reasonably be held accountable for it being discoverable elsewhere.

Open data initiatives should begin moving towards an idea of "degrees of openness"

To date, government's approach to open data has been to attempt to exclude personal information. Yet this excludes some of the most interesting and useful information from the open data environment. It also assumes that all participants know what personal information is, and in particular how the definition of information is or is not affected by de-identification or aggregation.

Consideration needs to be given to whether we need to start thinking about "degrees of openness". Statistics New Zealand has already begun moving towards this type of model by providing highly controlled access to micro-data for accredited researchers. This represents an important first step.

There may also be opportunities to use intellectual property rights to manage privacy risk in de-identified or aggregated data sets. For instance some low-risk data sets could be released under open access licenses that included provisions to protect privacy and prevent re-identification. Licenses might also limit access to certain types of organisations.

An explicit prohibition of re-identification might also provide part of a solution, particularly if it applied equally to published and unpublished data.

Cross-border enforcement of privacy rights remains a challenge we need to invest effort in

The Forum's second discussion paper also argued for promoting a data environment that, as far as possible, retains New Zealand control over the use and protection of New Zealand data, and to "aspire to maintain sovereignty over the use and protection of data collected in New Zealand". A defensive attempt to maintain sovereignty over data seems unlikely to succeed, and may unnecessarily curtail the ability of New Zealand agencies to take advantage of the global data environment.

Challenging cross-border enforcement issues are already arising in the globalised data processing environment. Privacy regulators are working together closely to improve cooperation on cross-border privacy issues, and privacy laws are gradually changing to facilitate joint enforcement efforts. It will take time before we are able to evaluate the ultimate success of these measures, but this is important work that needs to continue.

Some changes are likely to be made to reinforce agency accountability when transferring data internationally as part of planned reforms to the Privacy Act, in response to recommendations made by the Law Commission. If the Law Commission's recommendations are taken up as proposed, these would not undermine the ability of New Zealand organisations to share information, but would reinforce their obligations to do so responsibly.

The government should implement the Law Commission's recommendations on public registers

Public registers provide the backbone to many critical processes in local and central government, and therefore it is important that they are efficiently and effectively regulated. The Privacy Act's public register privacy principles foresaw the development of a more digitised environment and attempted to recast the balance for an unknown future. In practice they have not been successful in achieving that balance; they constrain some activities they arguably should not, while not preventing other activities they should.

In its stage 2 report on the Privacy Act, the Law Commission recommended repealing the public register privacy principles in conjunction with a review of the statutes that set up the registers themselves, with the aim of developing an appropriate regulatory structure for each register on a case by case basis. The government should implement this recommendation.