

NEW ZEALAND
DATA FUTURES FORUM

DISCUSSION DOCUMENT TWO



NAVIGATING THE DATA FUTURE

FOUR GUIDING PRINCIPLES

@nzdatafutures
#NZDFF



www.nzdatafutures.org.nz

Contents

Summary	3
---------	---



Introduction	5
---------------------	---

The data revolution will challenge our current institutions	5
-------------------------------------------------------------	---

Navigating the way forward	6
----------------------------	---



An alternative approach: shifting the focus to data use and data users	8
-----------------------------------------------------------------------------------	---

A simple focus on data ownership is becoming less helpful	8
-----------------------------------------------------------	---

We need a solution that is adaptive to new social values and norms, and can change along with technology	9
-------------------------------------------------------------------------------------------------------------	---

How data is used in specific contexts is what matters most	10
------------------------------------------------------------	----



Four principles to guide New Zealand's data future	12
-----------------------------------------------------------	----

Principle 1: Value – New Zealand should use data to drive economic and social value and create a competitive advantage	13
---------------------------------------------------------------------------------------------------------------------------	----

Principle 2: Inclusion – all parts of New Zealand society should have the opportunity to benefit from data use	17
-------------------------------------------------------------------------------------------------------------------	----

Principle 3: Trust – data management in New Zealand should build trust and confidence in our data institutions	19
-------------------------------------------------------------------------------------------------------------------	----

Principle 4: Control – individuals should have greater control over the use of their data	24
----------------------------------------------------------------------------------------------	----

Putting the principles into practice	27
--------------------------------------	----



How can you be involved?	28
---------------------------------	----

Summary

The New Zealand Data Futures Forum is exploring the future of data sharing in New Zealand. This paper presents some principles to both guide our own thinking and to guide New Zealand in developing an environment where the benefits of data use and sharing can be realised safely.

The rapidly developing data environment will challenge our current institutions. The New Zealand Data Futures Forum is of the view that an approach that emphasises data use rather than data *ownership* will be better suited to dealing with these new, innovative developments and meeting some of the challenges.

The Forum proposes four principles for safely managing and optimising data use in New Zealand in the future – these are intended to guide solution development and ensure we are achieving the best outcomes in terms of harnessing the benefits and maintaining trust and protection.

1 VALUE 2 INCLUSION 3 TRUST 4 CONTROL

We seek feedback from New Zealanders on whether these principles will help us to navigate our data future. Your feedback will help the Forum to develop its thinking on what approaches New Zealand should take to support safe data use and sharing in the future. Are these the right principles to guide New Zealand? You can provide your comments via the Forum's website, www.nzdatafutures.org.nz.

FOUR GUIDING PRINCIPLES

Value:

New Zealand should use data to drive economic and social value and create a competitive advantage.

To achieve this we should

- encourage collaboration and sharing
- support creativity and innovation
- promote a data environment that, as far as possible, retains New Zealand control over the use and protection of New Zealand data.

Inclusion:

All parts of New Zealand society should have the opportunity to benefit from data use.

- We should support all New Zealanders, communities and businesses to adapt and thrive in the new data environment.

Trust:

Data management in New Zealand should build trust and confidence in our institutions.

- Transparency and openness should form the foundations on which we build trust and enhance understanding about what data is held, and how data is managed and used.
- Privacy and security are fundamental values that should be built into data frameworks and the full data life cycle.
- Data collectors, custodians and users should be accountable for responsible stewardship and should exercise a duty of care.

Control:

Individuals should have greater control over the use of their personal data.

- Individuals should be better able to determine the level of privacy they desire on the basis of improved insight into how their personal data is processed and used.
- Informed consent should be simple and easy to understand.
- Individuals should have the right to be forgotten and the right to opt out.

Introduction

The New Zealand Data Futures Forum is exploring how New Zealand businesses, government, researchers and the public can safely share data and use it to build a prosperous New Zealand. Harnessing the benefits of data sharing and use requires a trusted, transparent and balanced environment – one where privacy is paramount and trust is maintained. The Forum has been set up by the ministers of Finance and Statistics to help us shape a future where New Zealand reaps the benefits of enhanced data use safely.

Our first discussion document, *New Zealand's Data Future*, set out the opportunities and the challenges for New Zealand on our journey towards this new future. This second paper turns to how we might navigate towards our desired future.

The data revolution will challenge our current institutions


We are in the midst of a data revolution. In our digital future, data will be abundant and ubiquitous; it will be connected and linked to people, things and places; it will be used and re-used, processed and reconfigured. Around every major invention (think of the printing press, electricity or the automobile), new practices emerge that create huge and often innovative opportunities, but also tensions with existing practices, habits and regulatory frameworks. In the data revolution we will need to learn how to do things differently, while protecting the values that are, and continue to be, of importance to us.

Experts expect that the widespread use of 'big data' will challenge fundamental concepts in legislative frameworks around privacy and information in countries around the world, such as the definition of 'personal information', the role of individual control, and the principles of data minimisation and purpose limitation ([Information Integrity Solutions 2013: 15](#)). New Zealand's existing privacy legislation requires, for example, that people be told that their data will be collected and how their data will be used (notification), and that data must then be used only for the purpose for which it was collected (purpose limitation) (www.privacy.org.nz). However, informing people about data collection may not always be possible in the new environment, as sensors become more widely used for example. And, as we cannot foresee the future, it is impossible to ask for consent for unanticipated innovative data uses at the time data is collected.

Privacy is, and continues to be, a critically important value for us as New Zealanders. Our existing regulatory settings to protect privacy and information may not always be sufficient to do this. While there is presently more flexibility under privacy and related information legislation than people commonly think, it is our expectation that the legislation will come under increasing pressure over time as technology, preferences and uses change. We need to develop new ways to achieve trust and privacy.



Sensor lighting at airports – how personal is it?



At Newark Liberty International Airport, the lights are watching you. The airport is piloting new lights outfitted with special chips and connected to sensors, cameras and one another over a wireless network. The data can be used to identify long queues and identify suspicious activity. The airport will hold and maintain the data, with other agencies requiring a subpoena or written request to obtain it.

Privacy advocates worry that the technology has been adopted without enough thought about whether the data was useful and what it would be used for. Others are asking about transparency (do people know this is happening?) and value (is this simply for security and safety?). Can people consent to this data being collected? And do people need to give their informed consent: is this ‘personal’ data, or do we expect and want comprehensive security systems at airports?



- www.nytimes.com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you.html
- nakedsecurity.sophos.com/2014/02/19/the-led-lights-are-watching-you-at-newark-airport/

Navigating the way forward

There are some important design choices we, as New Zealanders, need to make about our digital future. This paper sets out how we might approach those choices.

The paper begins with an exploration of an alternative approach that we suggest will be more workable and effective in the new environment. We propose that our institutions manage for data use rather than simply focusing on data *ownership*.

In this paper we also wish to test with you four principles for safely managing and optimising the use of data. The four principles we are initially proposing are

- 1 Value** – New Zealand should use data to drive economic and social value and create a competitive advantage for New Zealand
- 2 Inclusion** – all parts of New Zealand society should have the opportunity to benefit from data use
- 3 Trust** – data management in New Zealand should build trust and confidence in our institutions
- 4 Control** – individuals should have greater control over the use of their personal data.

These principles are intended to work together in tension to support an environment where there is trusted data use, delivering prosperity and well-being. Each principle is described in further detail in the sections that follow, with some short case studies and examples that raise important questions or present ways in which the principles could be or are put into practice.

These principles provide us with a test for any proposed approach – how well does any particular initiative meet these principles? As specific initiatives and solutions for data management are developed in a complex, fast-moving world, these principles should ensure we are achieving the best outcomes in terms of harnessing the benefits and maintaining trust and protection. We expect to explore how to make sure these principles are applied to best effect in our next paper. The aim of this paper is to seek feedback from you to see if we have adequately covered the important values and considerations.

WHEN WE HAVE



WE CAN

Harness the benefits of data use... **safely**



An alternative approach: shifting the focus to data use and data users

A simple focus on data ownership is becoming less helpful

Our current frameworks for information and privacy protection are based on a 'data ownership model'. We tend to treat data as a property belonging to a particular person (in the case of personal data) or an organisation (a business, a government agency or a non-government organisation). This was easy to do in the past, when there was not much data around and we weren't using the digital tools and capabilities we have today. Our regulatory frameworks have been constructed and developed on the assumption that data can be categorised into 'natural' homes and, within each of these data homes, linked to a data owner who has control over the data.

However, in the future, many types of raw data will be less like properties of people or organisations and more like a natural resource, similar to water. Data will flow in all sorts of directions. Like water, large volumes of data will not only have much more value than individual pieces of data, but will also generate enormous new opportunities. Think about an ocean generating marine life, fertilising soil, carrying boats and swimmers and regulating weather patterns, compared with what individual water drops can do.

The water analogy is also useful when thinking about interests in data. Multiple people in New Zealand have interests in water: iwi and hap, canoeists, dam builders, farmers, fishermen, conservationists. Ownership is contested, and there are different views about acceptable uses of our water. Collaborative approaches where all parties contribute and the various use interests are considered, such as the Land and Water Forum, have tended to prove most effective.

Similarly there are multiple interests in data: the person whose data it is about, the data collector, multiple data re-users, privacy experts, government, etc. But unlike water, in our digital future data will be abundant, and it will increasingly be merged, transformed and re-used. New types of data will be introduced in our society. Think, for instance, about recent introductions of sensor data, smart phone data or tweets. These developments will make it, in many cases, difficult if not impossible to identify the owner of the data involved in the data flow at a particular stage. An approach based principally on data ownership will become increasingly unworkable.

We need a solution that is adaptive to new social values and norms and can change along with technology

It is important to recognise that people's attitudes towards personal information, data ownership and privacy change over time, usually in response to the introduction of new technologies in our society. We need to develop responses that are adaptive and able to cater for changing norms and expectations and unanticipated uses.

Which personal data is considered as more private is different for people from various backgrounds and will depend on the context in which the information is used. Our values and norms about personal information sharing are continuing to change as our behaviours change: we increasingly interact with each other on the basis of information flows rather than through face-to-face or paper-based forms of communication. In order to do this, we have an increasing variety of personal data at our disposal, which supports us in the varying activities we do online nowadays, such as online shopping, reading a book, transacting with government, or communicating with friends and family via social networking sites.

From research, we know that many people knowingly or unknowingly use personal data as a 'commodity' in these online relationships nowadays. For example, they provide their email address, mobile phone number or their Facebook login details in order to get access to a particular online product or service. These people see the added value to themselves of trading off their personal information and, with that, their right to privacy, for a particular benefit in a certain context or relationship. For example, at Singapore Airport you can access free Wi-Fi by providing either your Facebook login or your mobile phone number.

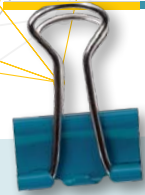
These trade-offs will be increasingly common in the digital future when we become more and more dependent on informational transactions via digital channels. Moreover, the changes that are likely to occur in our practices and attitudes signal that we may want to revisit how we commonly define 'personal' data in the digital future.



Obvious bounds of propriety and decency?

Consider the fact that a person's right to privacy was introduced at the end of the 19th century, after a public debate about the publication of people's photographs in newspapers. According to the two lawyers who suggested this right to privacy, the newspaper industry had "invaded the sacred precincts of private and domestic life" through publication of these "instantaneous photographs" and the "unauthorized circulation of portraits of private persons". As a result, the newspaper industry had violated people's "right to be left alone".





It was clear to them that “the press is overstepping in every direction the obvious bounds of propriety and of decency” (Warren & Brandeis 1890).

Compare this with our current practices of sharing, using and re-using digital photographs in the press, magazines and via social media. Do we still consider the unauthorised circulation of people’s photographs, which are abundant nowadays, as a violation of people’s right to be left alone under all circumstances? Do people own their own photographs when photographs are disseminated via social media sites? And is legal enforcement of this ‘right to privacy’ actually feasible nowadays? Answers to these questions are primarily negative, with potential legal action depending on the actual picture and the context in which a person’s photograph has been used. There are formal controls and social norms around the publication of images of individuals which have developed in response to media use.



• en.wikipedia.org/wiki/Right_to_privacy

How data is used in specific contexts is what matters most

In the new and changing data environment, a greater focus on the rights and responsibilities of all players and all along the data life cycle will enable us to harness benefits safely. Data subjects, collectors of data, stewards and users of data all have rights and responsibilities, working together to ensure that we collect, manage, use and share data in acceptable ways.

However the proof of the pudding will be in the eating – the actual use of the data in a particular context is what ultimately matters. It is through use that we collectively and individually realise the benefits and potentially cause harm. Shifting our focus away from data ownership and on to the rights and obligations around data use may help us to make some progress in how we might effectively regulate these new developments.

Data users could be any organisation or individual using the data and would include various stakeholders in data sharing. We would like to think that large companies, research institutions, iwi, government agencies, SMEs, start-ups, non-government organisations and individuals will all be data users in our digital future.

Returning to the example of the publication of people’s photographs in newspapers in the late 19th century, our focus would be on the newspaper as the data user, instead of the specific person in the photograph. And if this photograph were re-used via a public website, the focus would be on that website. Making users of this data accountable for safe use will be easier than trying to trace back to the person in the picture or the photographer to see what consents or stipulations were originally agreed. Of course, that may be required in some situations, but in a world with significant data re-use, we consider an emphasis on safe data use a much more workable approach.

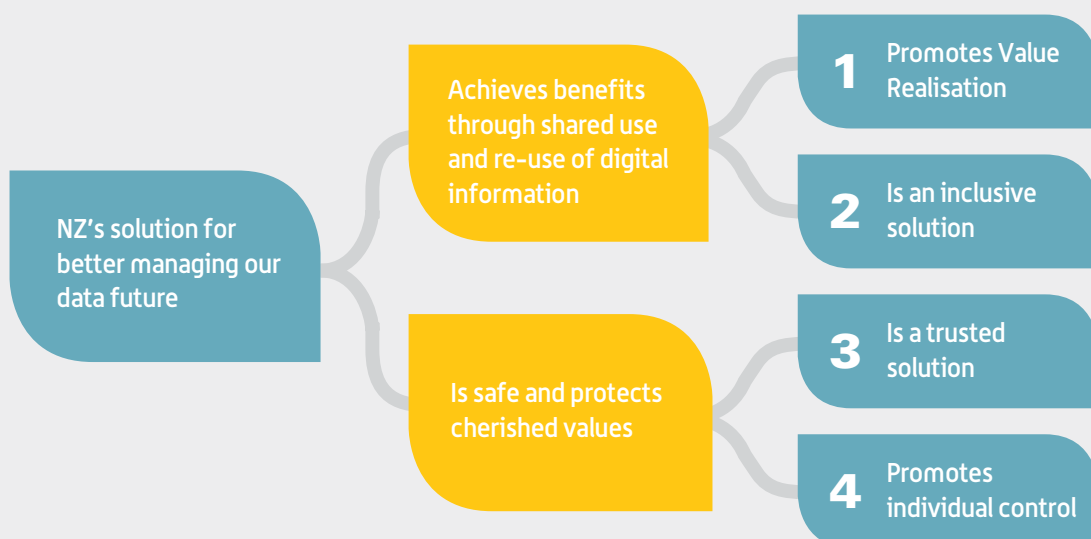
A focus on data use instead of data ownership would also have the advantage of focusing on data (re-)use in a particular context, and being able to take this context into account when data use is being assessed. For example, a photograph of a naked person would be considered inappropriate to use in newspapers, but would be less problematic to use in a medical context. In our digital future, assessments about the contextual integrity of data will remain of importance even when we are dealing with large data sets.

We intend to further explore a data use framework in our third discussion document. However we raise these ideas now so that they can be tested and benefit from robust discussion. We look forward to hearing your views.

Four principles to guide New Zealand's data future

In our digital future, innovative developments will have a fundamental impact on our daily lives. While a lot of the changes are international in nature, we can shape our digital future to a certain extent by implementing guiding principles for New Zealand. These principles are put forward to start a conversation about the values a data management system in New Zealand needs to support. While some people favour a 'data bill of rights', as Sandy Pentland and others have discussed at the World Economic Forum, this is not the purpose of the principles presented here.

We stated in the first paper that there were benefits to increasing access to shared data and through re-use. We also emphasised that there is no free lunch. We need to meet many challenges that arise. Our four principles in this paper are designed to build on that thinking – that we must design a system to lever value and do so safely. The four principles we talk about here are designed to harness the benefits of data sharing and use in a safe way. We see these principles as working together in tension to achieve our overall objective: to maximise the opportunities for all New Zealanders, while minimising the risks and protecting values of importance to us.



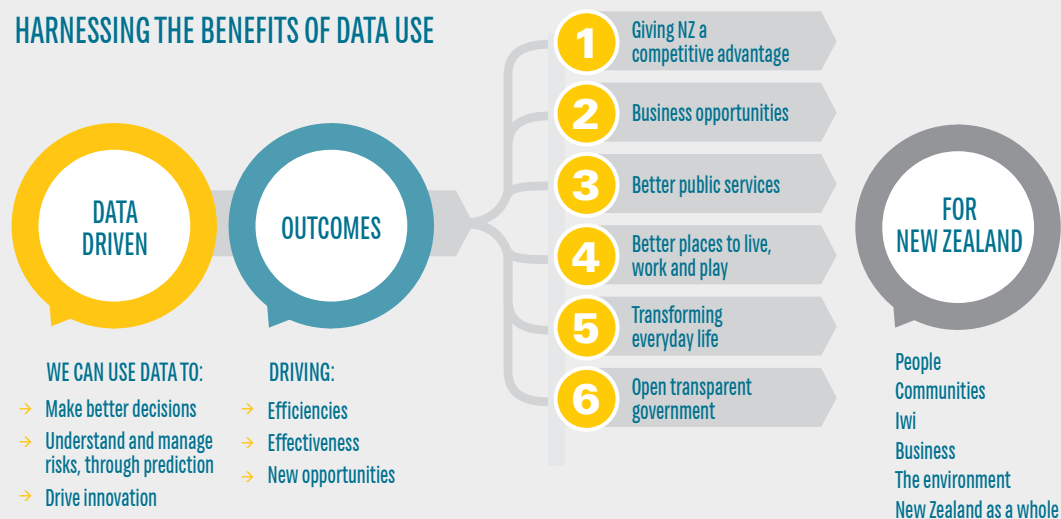
Principle 1: Value

– New Zealand should use data to drive economic and social value and create a competitive advantage

In our first paper we talked about the significant benefits that could be gained from data sharing and use, creating new opportunities to support prosperity, well-being, efficiency and sustainability. We can create a competitive advantage for New Zealand by establishing a trusted environment that attracts investment.

There are important risks around issues of control and misuse; however we believe that one of the biggest risks to New Zealand is failing to adapt and take advantage of the enormous opportunities the data future holds for us as a country.

HARNESSING THE BENEFITS OF DATA USE



Data is most valuable and most able to create value when it is *shared*. In order to realise the benefits, we need to encourage collaboration, sharing, creativity and innovation, as these components are vital to achieve benefits for all New Zealanders.



Encouraging collaboration and sharing

Large, valuable data sets are often dispersed, sit in siloes and come from multiple sources. Creating technology-enabled collaborative platforms for data-driven innovation initiatives, the development of data standards, and strengthening communities of data users would help to facilitate the sharing, use and re-use of data across academia, government and the private sector.

Moreover, industry, government and academia already have experience and expertise in the analysis of large data sets. Bringing this knowledge, experience and expertise together, as well as having producers of valuable data sets sitting around the same table, will further enable the collaborative creation of effective, data-driven solutions.

Optum Labs: data growth through partnership – how partnership and collaboration supports value realisation in United States health care

Optum Labs's goal is to bring together data, technology and expertise to support research projects that will lead to improved patient care and lowered costs of care, in a way that protects personal data and is transparent to all its partners. It is not-for-profit, so its value proposition is about the benefits it supplies to its partners. Its projects will

- focus on delivering real benefits to patients when they are sick, and helping populations stay healthy
- improve the productivity of the health care system, including delivery of higher quality care to more people, more efficiently
- simplify the complexity of the health care system, between and within sectors
- deliver translational innovations with real-world application.

Although the Optum Labs were only recently established (2013), partnerships with a range of United States-based groups – such as data providers, academics, professional and consumer organisations, funding groups, and pharmaceutical and life science companies – have already been arranged. Each stakeholder brings something that supports data-driven health care innovation – such as data, expertise, funding or clinical environments to test solutions. Studies underway are focusing on issues such as employee absenteeism, the diagnosis of Hepatitis C and the pancreatic cancer risk associated with diabetes treatments.



- [www.ecri.org/Documents/2013_TA_Conf/Presentations/Optum_Labs_Overview\(Wallace\)S6.pdf](http://www.ecri.org/Documents/2013_TA_Conf/Presentations/Optum_Labs_Overview(Wallace)S6.pdf)
- strataconf.com/rx2013/public/schedule/detail/29813
- medcitynews.com/2014/02/optums-collaboration-center-harnesses-big-data-answer-vexing-healthcare-questions/
- www.optum.com/optumlabs.html



Supporting creativity and innovation

In order to realise value from the new data environment, it will be critically important for New Zealanders to be able to experiment and learn fast how to do things differently and to be creative. Doing this will require safe spaces to play, experiment, learn and innovate with digital data.

A particular group in our society is already 'learning-by-using' in a very natural way. Young people, who are growing up with new digital technologies and not held back by practices, habits or frameworks from the offline past, are already using digital data sets in new ways. They are mashing up digital data from various sources in new, creative ways.

These practices are occurring, sometimes without any consideration of existing regulatory frameworks, such as those around copyright. Do we want to raise a generation of criminals? Or would we rather prefer people to play safely and creatively and, in so doing, show us new ways, perhaps, in which we can use and re-use digital data collaboratively?

Ironically, innovation requires certainty, about what is and is not acceptable, and that valuable innovation will be rewarded. Part of providing certainty in the context of innovation will be ensuring the intellectual property of innovators can be protected at the same time as enabling re-use of data. Business, government and academia are asking for more certainty so that they can experiment within well understood and navigable boundaries.



Free culture – supporting creativity and innovation

Beginning a decade ago now, the American academic Lawrence Lessig argued existing laws on copyright were choking creativity and “raising a generation of criminals”. Lessig is an advocate for ‘free culture’. He saw many people ignoring copyright law to create mash-ups and remixes, repurposing copyrighted content, and so acting illegally. Key to Lessig’s argument was the concept of fair use and how this applies in the digital age. Fair use allows limited use of copyrighted material without requiring permission from the rights holders, and is essential for reporting, remixing, research and teaching. Lessig argued that fair use in the digital world was not supported by existing laws, and the laws needed to be changed to allow a free and creative culture.

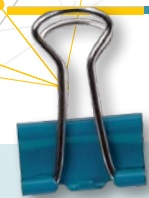
Creative Commons was a solution that Lessig and others advocated and implemented. Creative Commons allows content creators to apply a licence to their work that allows others to re-use it in specific ways. It balances control over content with sharing.

Creative Commons has been very successful, and is implemented all over the world. Many New Zealand government agencies use NZGOAL (New Zealand Government Open Access Licensing), a New Zealand version, to license re-use of their material. For example, Statistics New Zealand licenses all the statistics it releases under ‘CC By’ (Creative Commons Attribution 3 New Zealand Licence). This means that anyone is free to use and re-use the data in any way, as long as they acknowledge Statistics New Zealand as the source of the data.

What Creative Commons allows is both individual control and increased trust as individuals and institutions are able to remix and mash-up within law, by using licensed content. Some might argue that further work is needed on issues of digital copyright, but Creative Commons is a great example of how solutions can be found to enable good practice.



Lessig giving his 2007 TED Talk on Laws that Strangle Creativity.



What is fair use in the new data environment? Can we learn from Creative Commons to support creativity, trust and control?



- governancexborders.com/2012/12/18/10-years-of-creative-commons-an-interview-with-co-founder-lawrence-lessig/
- www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity
- creativecommons.org/
- creativecommons.org.nz/



We should promote a data environment that, as far as possible, retains New Zealand control over the use and protection of New Zealand data ...

... in order to harness the benefits of data for New Zealanders, to use these New Zealand data sets safely in accordance with New Zealand data rules, standards and public expectations, and create a competitive advantage for New Zealand internationally. New Zealand should aspire to maintain sovereignty over the use and protection of data collected in New Zealand. This will enable us both to protect against misuses by foreign players and to ensure that we realise benefits for New Zealand and New Zealanders.

Principle 2: Inclusion

– all parts of New Zealand society should have the opportunity to benefit from data use

Although we don't know what will happen in the future, we do know that increased data sharing can lead to good and bad things in our society, depending on how the data is used. As we indicated in our first discussion paper, the New Zealand Data Futures Forum believes that the objective of the sharing, use or re-use of data should aim to create value for all New Zealanders – saving lives, increasing well-being, driving innovation, supporting learning. In the digital future, each individual would desirably benefit from the increased sharing and use of data facilitated in this country. We should also consider ways to minimise any harms.



We should support all New Zealanders, communities and businesses to adapt and thrive in the new data environment

Supporting New Zealanders, communities and businesses to adapt and thrive in the new data environment means that communities, iwi, non-government organisations, small businesses, start-ups and individuals are all able to reap the benefits of data sharing and use, not just larger scale organisations such as government and big business.

Enabling everyone to adapt and thrive will require

- educating citizens and communities about what data is available, and how to access and explore the data
- making data sharing and use accessible for all stakeholders – the data infrastructure would need to allow for low barriers to entry; ease of data access, sharing and use; user-friendliness; and equal access for all
- making sure that data is re-used in ways that benefit a wide cross-section of the community or the country as a whole.



Global Pulse – realising value for communities



The mission of Global Pulse is to enable the use of data to promote well-being and better outcomes for people and communities.

Global Pulse was set up by the United Nations Secretary-General specifically to provide timely information to track and monitor the impacts of global and local socio-economic crises. Their work supports development priorities for vulnerable communities, like access to food and health services. While traditional statistics are great at tracking medium- to long-term developments and changes, new data – such as online news stories, social media and telecommunications data – provide a new opportunity to gain real-time insights, and thus agile responses to crises.

The Pulse Lab in Jakarta is one of the initiatives of the Global Pulse, established in 2012. The lab brings together United Nations agencies, the Indonesian government, non-government organisations and the private sector to research and use new digital data sources and real-time analysis techniques for social development in Indonesia.

The Pulse Lab has access to rich data because Indonesians' use of mobile technology and internet penetration has skyrocketed in recent years, with Indonesians considered the most active Twitter users in 2013. The research agenda is set in consultation with the Government of Indonesia and the United Nations Country Team, based on national development priorities such as changes in food prices, fuel prices, employment and urban poverty.

Projects undertaken by the Jakarta Pulse Lab include the following.

- An investigation of attitudes to immunisation.

Tweets were analysed for occurrences of nearly 1,000 keywords and phrases related to immunisation and vaccination in Bahasa Indonesia. The four primary topics of discussion found were (a) new vaccines, (b) debates about the ethical and religious dimensions of immunisation, (c) discussion when there is news of outbreaks and (d) discussion of side effects of immunisation. The team is preparing the summary and findings report.

- Understanding attitudes to women's employment in Indonesia.

Online news articles, blogs and social media are being mined to gain insight into people's views on women's role in the workplace, their conditions of employment and obstacles to equality and equal opportunities in the workforce. The intention is to support the government and International Labour Organization Indonesia to find ways to improve women's access to employment, and to monitor the impact of programmes and interventions.



• www.unglobalpulse.org/sites/default/files/GP%20Annual%20Report_2013.pdf



Principle 3: Trust

– data management in New Zealand should build trust and confidence in our data institutions

Without trust, people will stop (or resist) freely sharing their data – there would be fewer data assets for businesses, government, non-government organisations, researchers and citizens to use. Trust is crucial to would-be data users and to would-be providers of personal or commercially sensitive data. It is of mutual benefit to build a high trust environment within which data sharing and re-use can take place. Without trust, everybody loses.

Trust is built upon many factors: transparency, openness, privacy, security, real accountability. In a trusted environment, these values work together to provide balance and to support each other.



Transparency and openness should form the foundations on which we build trust and enhance understanding about what data is held, and how data is managed and used

Increased transparency around data use empowers stakeholders in a data-driven society. People usually do not oppose large datasets as such, but they are concerned about hidden or unwanted data uses. Increased transparency about what data is held and what it is being used for is one way of meeting people's concerns. When organisations involved in a data use initiative decide to publicly offer insight into the flow of data – who has access and who uses certain types of data at a particular moment in time – people's trust and understanding of data use (and non-use) will usually be improved.

Another possibility for achieving data use transparency and enhance trust and public understanding is to provide insights to stakeholders into the methodologies, algorithms or criteria used in the decision-making process with respect to the data analysis. Again, an exception would need to be made for organisations that need to protect their commercial interests (including intellectual property) in this respect. Algorithm transparency or being 'open' about the decision criteria or methodology used for data analysis would discourage inaccurate, unfair or unethical classifications and inferences and give stakeholders the 'democratic' means to challenge decisions made about them.

In some cases, we can go beyond transparency about data holdings, use and methods, to making data fully open. This supports transparency and trust by making it clear what data is held, as well as allowing others to re-use the data. Fully open data sets have the following characteristics (McKinsey 2013:3).

- Accessible for a wide range of users.
- Machine-readable, so that data can be processed automatically.
- Free or negligible costs to access the data.
- Minimal limitations on the use, re-use, transformation and distribution of data.

Government agencies are already releasing and using open, non-personal data under the Declaration on Open and Transparent Government and the NZGOAL framework. However, there are certain types of data which cannot be made open, and in these cases, being transparent about why is important to maintain trust.



ClearButton.net – a way of making data use transparent

At the MIT Media Lab in Massachusetts, Dazza Greenwood, Ray Campbell and the legal systems research team have been doing some thinking on rights around data responsibilities and how to protect privacy in an era where non-disclosure may not be an option.

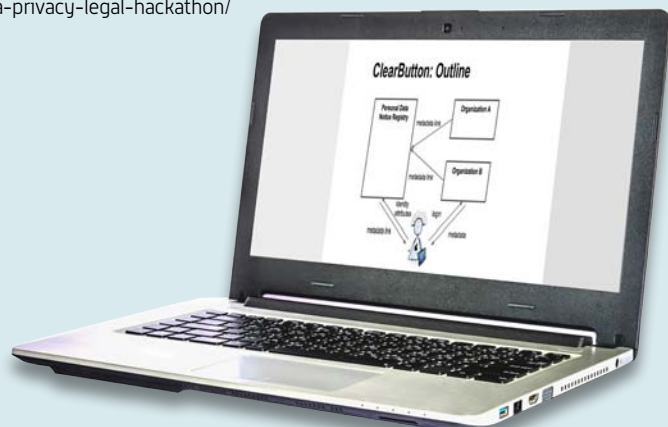
“Whether, or the extent to which, people can and should be capable of exercising meaningful control over personal data about them is a key public policy decision point of our time. The ClearButton initiative reflects a definite view that it is in the interests of all major stakeholders for individuals to maintain and exercise robust means of control over and transparency of their own personal data.”

The idea is that ClearButton would increase transparency by giving individuals the ability to find out which institutions held data about them, what they are using it for, and even to request download of the data. At the moment, there is no way for people in the United States, or any country, to reliably and comprehensively find out who has information about them.

ClearButton is in its early stages, being developed via various Legal Hackathons in 2014. It is envisaged as an open standards, open source and open architecture approach to a Personal Data Notice Registry that will provide value to both the data holder and the individual. The developers hope that ClearButton would be attractive enough to all parties to be voluntary and self-propelling. “In short, we believe all key stakeholders stand to increase value, reduce risk and enable significant innovation by using the ClearButton approach.”



- www.ecitizen.tv/2014/01/clearbutton-personal-data-notice.html
- www.hackerleague.org/hackathons/data-privacy-legal-hackathon/hacks/clearbutton-personal-data-notice-registry





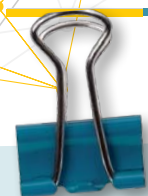
Privacy and security are fundamental values that should be built into data frameworks and the full data life cycle

Certain data sets, such as personal data, will continue to require a higher standard of care and greater consent before they can be made publicly available. Privacy is a choice and needs to be supported by the data infrastructure, policies and processes around data management and use.

- Privacy and security are important in any initiative that involves the sharing and use of personal data.
- Privacy and security are also important to protect some national interests or public good. For instance, from a national interest point of view, foreign policy data may not be made widely available or police data may not be widely available publicly – to protect the business and activity of policing from criminal interests.
- Finally, commercial interests such as business confidentiality need to be protected to allow economic benefits from data (re-)use, such as the creation of jobs through the development and delivery of new products and services.

If we want to maximise both the value creation through increased data use and the privacy protection of individuals and businesses, it is clear that we need to continue to build in privacy and security arrangements through all stages in the collection, storage, sharing, use and re-use of data.

- For example, privacy-by-design involves protecting personal data in each phase of a data-use initiative. Current techniques include requiring data users to de-identify data when possible, implementing security measures and limiting uses of personal data to those that are acceptable from an individual and a public good perspective ([Tene & Polonetsky 2013](#)).
- Data also needs to be managed securely, appropriate to the level of harm arising from its misuse. Security-by-design solutions include the use of encryption, two-way authentication and secure channels, minimising data access points, and restricting the access and use of protected data, such as personal data and classified data, for authorised purposes only.



Statistics New Zealand – building privacy and security into systems and processes to protect people and businesses

Trust is vital to the collection of official statistics, as without trust, people and businesses will not supply their information, resulting in distorted or biased statistics that are much less useful. To maintain trust, statistical data has always been subject to very strong protections to safeguard the privacy and confidentiality of the people and businesses who provide information.

Focusing on protection alone would prevent New Zealand from realising the full value from statistical information: it is through the sharing and use of statistics to support good decision-making that New Zealand gets value from its official statistics.

Policies and procedures are designed to protect privacy and confidentiality during the collection, use, storage and distribution of statistical information.

- Privacy is ensured by collecting only the information that is needed to create statistics, and using it only for that purpose.
- Security is ensured by keeping data safe from unauthorised access.
- Confidentiality is ensured by not releasing any information that could identify a person, household or business.

Key to the maintenance of trust is the distinction between published statistics, which are open and freely available, and individual-level data, which is protected.

- Open, publicly released statistics are prepared in such a way to ensure they do not identify individuals, households or businesses. Published statistics only describe groups, and have had confidentiality rules applied. Confidentiality techniques include random rounding, suppression of cells and collapsing of categories.
- Individual-level data can only be accessed by external researchers under very restricted circumstances, with a variety of protections applied. For example, there is a rigorous application process and eligibility criteria. Access can only be for bona fide research or statistical purposes in relation to a matter of public interest and must take place in approved, secure environments. Data is anonymised and results are checked to ensure confidentiality. Work that involves identifying or targeting individual people or businesses is not permitted.

Recent changes to access rules mean that individual-level statistical data remains protected, but is more available for use, and thus value realisation. For example, changes to the Statistics Act allow non-government researchers to apply for restricted access to individual-level data. Inland Revenue has also allowed non-government researchers to access tax data held by Statistics New Zealand in the Integrated Data Infrastructure (IDI), an increasingly important source for research. Recent projects include work by the Ministry of Education to understand pathways from tertiary education to employment, and Ministry of Business, Innovation and Employment research on migration and labour market dynamics.



• www.stats.govt.nz/tools_and_services/microdata-access.aspx

• www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure.aspx



Data collectors, custodians and users should be accountable for responsible stewardship and should exercise a duty of care

In the digital future, data will not be collected and used just once – we can expect more and more re-uses of existing data sets and also re-use for other purposes. This may create uncertainty about who is responsible for any future data uses and data management, and who can be held to account when things go wrong. Making data users accountable could provide clarity around this issue of possible data re-use and would ensure that there are consequences for any possible misuse in the future. User accountability would help to generate and maintain trust between various stakeholders and to identify misuse early. In addition, making data users accountable would stimulate responsible data use and data management behaviours, including data stewardship.



Shared Care Records – a system to support accountability

District health boards are beginning to introduce electronic Shared Care Records to allow authorised health care providers, like hospitals, to access summary information from your GP – information such as your test results, medical conditions, allergies and prescribed medications.

Sharing the information means that in an emergency, or after hours, health professionals can quickly access the information and prescribe treatments and medications.

The Canterbury Shared Care Record system is built in such a way to enable data user accountability and protect patient privacy. Canterbury introduced its electronic Shared Care Record View (eSCRv) system in September 2013, with systems in place to identify inappropriate access. Clinicians have to log on in order to access any records and can only access information relevant to their part of a patient's care. If there is any indication of inappropriate access, this is investigated and a clinician may have access rights removed or face disciplinary action. Patients can choose to opt out of the system by talking to their GP.

The Canterbury system was developed jointly by the district health board, Orion Health and Pegasus Health, with input from GPs, pharmacists and Nurse Maude community nurses. It has proved so successful that it is being rolled out to other parts of the South Island. Similar systems are being rolled out in Wellington and the Wairarapa.

The Health Information Governance Expert Advisory Group is currently developing a framework that will guide the sharing of health information across the New Zealand health sector. The framework will consider issues to do with the collection, storage, access, use, security and privacy of health information.



- ithealthboard.health.nz/our-programmes/common-clinical-information/summary-view-primary-health-information/case-study-%E2%80%93-93
- tvnz.co.nz/national-news/privacy-questions-raised-over-medical-record-database-5790303
- www.stuff.co.nz/the-press/news/8549885/Sharing-medical-files-saves-lives
- www.compasshealth.org.nz/HealthServices/SharedCareRecord.aspx

Principle 4: Control

– individuals should have greater control over the use of their data



Individuals should be better able to determine the level of privacy they desire on the basis of improved insight into how their personal data is processed and used

In order to enable each individual to make better decisions about the personal data they are willing to provide to others in return for a personal benefit or a particular public good, we believe that strengthening individuals' control over the use of their personal data is of critical importance. While informed consent about future data use at the time of data collection may not always be possible any longer in the emerging digital future, improved insight into how people's personal data are processed and used will enhance transparency about data collection and management in the new data environment, including data accuracy, and build trust amongst the stakeholders involved. This then can lead to greater individual control over the provision and use of personal data. Strengthened individual control over personal data also supports having decisions made about an individual's privacy at the level where the possible benefits and costs are felt.

Giving individuals greater control is likely to provide some additional benefits. We may also see better security and protection of personal data and the improved organisation of traditionally fragmented personal data, such as all sorts of usernames, passwords, pin codes and shared secrets. Control should also support higher quality and accuracy of personal data, including the option for people to see their own data and suggest any corrections if needed.

Examples of how individuals' control over their personal data can be strengthened for each person include:

- using a digital vault service through which they can manage their personal data online
- the use of federated identity management systems so that the exchange of personal data can be organised separately for each online relationship
- personal data minimisation through the restricted or anonymised use of personal identifiers, the use of pseudonyms or the use of confidential personal data.



Informed consent should be simple and easy to understand

Control should be genuine. This means that strengthening individuals' control over their personal data and improving their understanding about how personal data will be processed and used include making it easy to understand and manage consent.

The current common practice of asking people to read and understand complicated privacy policies or statements before they are able to access a particular online service does not, in

many cases, achieve genuine consent. From research, we know that only 25 per cent of the New Zealand population actually reads and is able to understand online privacy statements, whereas 47 per cent of the New Zealand population does not read online privacy statements at all. This current practice of obtaining people's permission via online privacy disclosures will become even more complicated in situations of data re-use on the basis of machine processing of data and data exchange with individual users. Therefore increased control and consent may also be facilitated by building solutions to make those choices more transparent.



MyInfoSafe – how giving individuals increased control over the information about them also helps efficient business practice



MyInfoSafe is a New Zealand developed tool that helps businesses to streamline identity management, and also helps individuals to control the information that is held and supplied about them.

As robust identity management becomes more important to banks and other businesses, these businesses are looking for ways to streamline the identity checking process and meet the required standards. MyInfoSafe provides a product where individuals store their information in their own secure digital vault and then provide identified businesses access to that information for particular purposes. Businesses accessing personal information this way don't have to keep it forever. Instead, they can keep a record that shows they have seen the information, checked it and verified the individual's identity. This gives the individual much greater control over their personal data and empowers them to protect their own information in the new data environment.

The company behind MyInfoSafe, Personal Information Management, has received support from Callaghan Innovation to develop its tool, and is looking for ways to grow its business in New Zealand. Its thinking is in line with an increasing number of initiatives that aim to put more control in the hands of consumers – initiatives like RealMe, a way for New Zealanders to prove their identity online, like ClearButton, or the Respect Network, which is creating a personal cloud where privacy is guaranteed.



- www.myinfosafe.co.nz
- www.realme.govt.nz
- www.respectnetwork.com/



Individuals should have the right to be forgotten and the right to opt out

In the digital future, when data may be stored for longer periods to enable data re-use opportunities, there needs to be an opportunity for people to escape their digital past, with exceptions to meet national interests. For example, if, later in life, people change their mind about the public availability of particular photographs, it should be possible to remove these pictures from the data set. The new data environment needs to cater for possible fundamental changes in people's lives, such as separating from a violent partner, a major career change or a transgender experience, which require the erasure of personal data.

A right to forget can also facilitate situations where incorrect data on the individual was used or where incorrect data inferences were made about an individual in the past, with reputational risks or damage involved.

Opt out options also strengthen people's control over their personal data. If people don't see the benefit any longer for their personal data to be used in a particular data use initiative, or have privacy concerns about the use of their personal data, they could have the right for their personal data to be removed from the data set. Opt out options should provide a necessary handbrake on practices that don't have widespread support or approval: when people are able to 'vote with their feet' then the data innovators and users will need to sell the value of their project.

Opt-out would require legally authorised exceptions for specific public good initiatives or purposes, such as birth registration, tax compliance or the protection of public safety.

This new option for an individual to opt out *after* a data use event, instead of the current situation of providing consent *before*, could also meet a need around the introduction of innovative technologies or applications in our society. It can be unclear to people what to expect from the digital innovation in terms of weighing up the benefits against the risks. A right to opt out gives people a second chance to decide once they have more information. This option can also cater for situations where it will be difficult, if not impossible, to tell people before the data use event (for example, in the case of machine-to-machine transactions or the passive collection of individuals' personal data such as through sensing lights).

Collecting information about dementia patients – who consents?

Increasingly, countries around the world are using GPS trackers to monitor dementia patients. The data-driven technology supports both patients' and caregivers' well-being and reduces costs to the community. While the benefits are clear, countries are still debating how best to ensure appropriate consents are given. Is this a situation where the community, rather than the individual can give consent?

Dementia patients can get very distressed if they forget where they are, and it helps reduce distress if families and caregivers use the trackers to locate people or alert them to risks. Bernard Stoneham, a United Kingdom man who cares for his wife who suffered from vascular dementia, noticed his wife had not moved for 11 minutes. He tracked her down to a muddy field where she had fallen while walking the dog. Another caregiver installed motion sensors in his home so that he can be certain he will be woken if his wife falls or walks outside during the night.

Advocates of the devices emphasise the increased safety and quality of life for patients, reduced anxiety for caregivers, as well as the reduced costs of care. On the other hand, critics worry that such devices will replace quality care and are being used without patient consent.

In Norway, tracking devices can only be used if the patient is lucid enough to agree, but after a recent study indicated that patients were happy to have the devices, lawmakers have suggested allowing health care workers to equip patients with the devices.



- sciencenordic.com/dementia-patients-embrace-gps-surveillance
- www.bbc.com/news/technology-22984876
- www.icenews.is/2013/02/04/norway-ponders-tags-for-dementia-sufferers/
- www.bloomberg.com/news/2013-10-10/gps-for-wandering-dog-walker-shows-dementia-challenge.html



Putting the principles into practice

These principles will not always cover everything. From time to time they will be in tension and sometimes judgement will be required. In particular, there may be times when public good, or significant net social benefit, may override some principles. Think of using data without consent to fight a flu pandemic, or for policing or national security. Any overrides should have rigorous justification, and it will be important to develop robust ways of making these kinds of decisions. Governance and decision-making processes will need to be transparent and democratic, and might, in some cases, include parliamentary approval for example.

How can you be involved?

The New Zealand Data Futures Forum exists to stimulate an informed conversation about the future of data use in New Zealand. We want you to participate in this discussion. By providing your ideas, you will help us to develop solutions and suggestions for what is needed to support New Zealand to be a world leader in the trusted use of shared data to deliver a prosperous, inclusive society.

The Forum would like to hear your thoughts on the following questions

The principles we have identified are designed to balance benefits and risks of data use and sharing. Are the principles we have identified right? If not, why not?

Do you think a shift in focus from data ownership to data use is viable and fair?

In your view, will the principles work in practice in a range of situations? If no, what do you think needs to be in place to make them practicable?

Can you foresee situations where the principles would need to be overridden? Who should the ultimate decision-maker be?

There are a number of ways you can get involved.

Visit our website, vote in our online poll or join a discussion:

www.nzdatafutures.org.nz

Send us your comments:

info@nzdatafutures.org.nz, or

NZ Data Futures Forum, Statistics New Zealand,

PO Box 2922, Wellington 6140

Tweet us:

[@nzdatafutures](https://twitter.com/nzdatafutures) or [#nzdff](https://twitter.com/nzdff)

Invite Forum members to speak at events or discussion groups

– contact us via our website

We will be listening to your feedback as we develop our third paper. The third paper will discuss options for the foundations that need to be put in place to enable the sort of data environment that will support collaboration and data sharing, and safely generate economic and social value for New Zealand. The third paper will be published in June.