# NAVIGATING NEW ZEALAND'S DIGITAL FUTURE: CODING OUR WAY TO PRIVACY IN THE AGE OF ANALYTICS

M A H O N E Y  T U R N B U L L

A dissertation submitted in partial fulfilment of the Degree of Bachelor of Laws (Honours) at the University of Otago, Dunedin

October 2014

# Acknowledgments

Nga mihi nui to my supervisor Andrew Geddis, for your pithy prompts and guidance amidst the pundit-ing, and willingness to diverge from Public Law to the data domain.

To Colin Gavaghan for your LAET stimulation and helping merge the legal and tech worlds.

Muchas gracias to my whanau, for your endless amor, perseverance, linguistic genes and growing enthusiasm for tech jargon.

谢谢你们 A standing ovation to the STD crew and the endurance of our elevation, and to Jessie, for your much appreciated nurturing.

To Derek Johnston for your mentorship and regular calls from the Chambers that challenged and refined my project.

To Internet NZ, Judge David Harvey, all the fellows at the Nethui Summit and the tech savvy experts scattered around the globe who persisted with the net (non) neutrality skype dates from the bottom of the world.

To the United Nations, for hosting me on that fateful day in the Human Rights Council in Geneva where it all began with Sir Tim et al.

And lastly to the web itself, for all your tweets, big data leaks and analytical feats that inspired, shocked, and entertained.

#bigdatabigdiss

# Navigating New Zealand's Digital Future: Coding our Way to Privacy in the Age of Analytics

MAHONEY TURNBULL

## TABLE OF CONTENTS

# PART I

## INTRODUCTION

We are now in the midst of a data revolution and New Zealand's digital future is uncertain. The data path we are steering towards is taking us into new cyber territory and is challenging fundamental concepts in privacy and data protection law. In this new digital terrain, big data represents a highly valuable reserve of personal information ripe for the picking. It is 'the new oil'[1], and the digital space that this sought-after commodity operates in is highly unregulated and open to exploitation. New Zealand's position on the extraction of this critical resource will be indicative of our commitment to enabling protected use of shared data to deliver a prosperous society. New Zealand's policy is suffering a critical regulatory disconnect, with technology fast outstripping the legislation that exists in the data protection domain. This dissertation addresses the question of how New Zealand's data stewardship should be governed, with a view to proposing how personal data management could benefit from clear national guidelines.

Part II provides context to the burgeoning industry surrounding big data and the role that it now plays in the ever-evolving digital economy. First, I consider the ecosystem in which big data lives, and the positive outcomes from strategic use and reuse of the wealth of data available. This is balanced by an examination of the more disturbing uses of data that have the potential to cause devastating data 'oil spills' and privacy scares. Following on from the contextual analysis, Part III outlines New Zealand's current legal framework, and whether our data protection architecture can truly claim 'adequate' status. This will focus on the key features of the Act that arguably place New Zealand's data protection future in good stead. In contrast, this section will also elucidate the technical inconsistencies that have emerged, and make the Act outmoded. Expanding upon the evolving genre of what constitutes personally identifiable information, this analysis will probe into the current de-identification techniques and the shift towards personally 'predictable' information; both trends that challenge the efficacy and endurance of the Privacy Act. Furthermore, it will highlight the need to progress towards more relevant legal tools, to oversee responsible data disclosure behaviour.

[1] Bruce Schneier, Chief Security Technology Officer, British Telecom "Privacy in the Age of Big Data" (speech presented to the New Zealand Privacy Forum, Wellington, May 2012) available at <https://www.youtube.com/watch?v=L_UIdkbp3xo>.

Picking up on this concern, Part IV explores the regulatory remedy that New Zealand could pursue in order to create progressive mechanisms that enable a coherent data management framework. By analysing examples of Standards Authorities and recent legislative changes, this section lays out the potential scope of the proposed Data Standards Authority, and the administrative features that would need to be addressed in forming this body. It will describe the interface with the Privacy Act, and possible response mechanisms that could be incorporated into its design.

The final part elucidates the principles that ought to govern the Data Standards Authority. It offers concrete suggestions for two overarching principles that may serve as valuable touchstones for the resulting data standards that would be contained within industry-specific codes. The initial focus will be the Privacy by Design principle, involving clarification of de-identification protocols that reflect the importance of technological systems in tackling the legal issues at stake. The second principle will address the core problem of data empowerment, and offer three ways in which consent can be enhanced, through visualised, informed and live consent. My proposal promotes a paradigm shift in privacy policies towards the idea of user-centricity, and the creation of consumer friendly privacy settings. It encourages a reshaping of the rules of engagement to secure a more responsive data ecosystem that can unlock the value of data within a more digitally relevant legislative landscape.

# PART II

## THE BIG DATA ECOSYSTEM

---

## A. THE SEED FROM WHICH DATA GREW

This part establishes the potential benefits and risks that have arisen from the big data industry. It will shed light on the nature of the data ecosystem and the value that lies in effective use of personal data sets. It also lays out the inherent risks associated with this unregulated industry, which has the power to generate privacy breaches through adverse and discriminatory profiling. Exposing the harms that flow from data misuse, this part will underline the importance of effective data regulation, for New Zealand to maximise the value from granular analysis of people, behavioural patterns, and the environment.

~

It is hard to imagine the world without the internet. A world without data and the ubiquitous connectivity that we as digital natives feel empowered to engage with. Our digital habitat is one where neither borders nor language appear as barriers to communication. [2] It is within this environment that we are witnessing the dawn of the data-driven era. A big data tsunami has risen, and is prompting a new industrial revolution driven by analytics, computation and automation. The tracking of human activities, industrial processes and research is all leading to data collection and processing of an unprecedented scale, spurring new products and services as well as business opportunities and scientific discoveries.[3]

---

[2] Ronald Deibert and Rafal Rohozinski "Beyond Denial" in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds) Access Controlled, The Shaping of Power, Rights, and Rule in Cyberspace (Cambridge, MIT Press, 2010) at 9.

[3] European Commission *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Region: Towards a Thriving Data Driven Economy* (Brussels, July 2014) available at <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6216> at 2.

: Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic forecast Update, 2012-2017 (Cisco, 2013) available at <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf>. The number of mobile connected devices has now exceeded the number of people on the planet. By 2020 an estimated 50 billion devices will be wirelessly connected.

The term, 'Big data', refers to datasets beyond the scale of a typical database, which are held and analysed using computer algorithms.[4] It is the 'non-trivial extraction of implicit, previously unknown and potentially useful information from data.[5] In essence, the concept of big data combines more data, faster computers and novel analytics which organisations, government and businesses use to extract both hidden information and surprising correlations.[6] The newly discovered information that results is not only unpredictable but also results from a fairly opaque process.[7]

As its name implies, the hallmark of big data is its quantitative greatness. In juxtaposition to the gains made from shrinking scope in the field of nanotechnology, big data gains its force from its sheer magnitude.[8] Now estimated to be in the order of zettabytes[9], the phenomenal production of data coupled with escalating storage capacity is enabling collection and sharing of information at unprecedented levels.[10] Although in the analogue age this kind of storage was costly and time-consuming, the current trend of 'datafication' and cloud-based servers is enabling rapid shifts. This change of scale has led to a change of state, and the quantitative growth is now prompting a qualitative one.[11]

---

[4] European Commission *Privacy and Competitiveness in the Age of Big Data* (Brussels, April 2014) available at <http://www.insideprivacy.com/international/european-union/the-new-edps-opinion-privacy-and-competitiveness-in-the-age-of-big-data/> at 6 : McKinsey Global Institute *Big Data: The New Frontier for Innovation, Competition and Productivity* (1 May 2011) available at <http://www.mckinsey.com/client_service/telecommunications/latest_thinking> at 2 : Wei Fan and Albert Bifet "Mining Big Data: Current Status, and Forecast to the Future" (2012) 14 ACM at 9.
This references the first time the term 'big data' appeared in a 1998 Silicon Graphics slide deck by John Mashey.

[5] Usama Fayyad and others (eds) *Advances in Knowledge Discovery and Data Mining* (MIT Press, Cambridge, 1996) at 37 as cited in Tal Zarsky "Mine your own! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion" (2003) 5 Yale J L & Tech 2 at 6, n 13.

[6] Ira Rubenstein "Big Data - The End of Privacy or a New Beginning?" (2013) 3(2) International Data Privacy Law 74 at 1
: Viktor Mayer-Schönberger and Kenneth Cukier *Big Data: A Revolution That Will Transform the Way We Live, Work and Think* (1st ed, Eamon Dolan, New York, 2013) at 7. Society will need to shed some of its obsession for causality in exchange for simple correlations.

[7] Tal Zarsky "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society" (2004) 56 (13) Me. L. Rev. at 13.

[8] At 10.

[9] A zettabyte is equivalent to one sextillion bytes, or two to the seventieth power.

[10] Julie Brill, Federal Trade Commissioner "Reclaim your name" (speech presented at NYU Sloan Lecture Series: Privacy in the World of Big Data, NYU, October 2013) available at <http://engineering.nyu.edu/sloanseries/reclaim-your-name.php>.

[11] Mayer-Schönberger and Cukier, above n 6 at 5-10. The fact that 90% of the world's data was only generated in the last two years, with this figure doubling every two years from now on, indicates the overwhelming pace at which big data is growing, as a wholly regenerative resource. If all the data today was placed on CDs and stacked up, it would stretch to the moon in more than five separate piles.

Compounding this issue is the Internet of Things (IoT).[12] This phenomenon reflects the 'machine-plus-human' hybrids that life in the digital age is making more mainstream.[13] Our lives are digitally disassembled, disaggregated and dispersed into a multitude of digital domains.[14] Within this space, we are seeing the rise of connected devices, which will push data accumulation to unparalleled levels.[15] The increasing number of people, devices, and radars that are now connected by digital networks has revolutionised the ability to generate, access and share data.[16] Mobile devices are not the only sensory gateway, as embedded technologies that are passively collecting data pervade the marketplace.[17] This trail of digital breadcrumbs, via the world of ambient intelligence, is creating an immense data ocean [18] in which the race to create new algorithms is pulling us in diverging directions.[19]

Whilst this data, hailed as the 'new oil', may be ripe for mining, it also poses considerable risks. Privacy expert Bruce Schneier has been a strong advocate of the data pollution problem reflecting our tendency to storm into a digital era whilst naively overlooking the deluge of data.[20] True to

[12] Mireille Hildebrandt "Who is Profiling Who?" in Gutwirth and others (eds) Reinventing Data Protection (Springer, Amsterdam, 2009) at 239.
[13] Lisa Gitelman (ed) Raw Data is an Oxymoron (MIT Press, Cambridge, 2013) at 10.
[14] Deibert, above n 2 at 9. In this sense, cyberspace is not such a distinct realm as it is the very environment in which we inhabit.
[15] Larry Hardesty "Algorithm recovers speech from vibrations of potato-chip bag filmed through soundproof glass" (August 4, 2014) Phys.org <http://phys.org/news/2014-08-algorithm-recovers-speech-vibrations-potato-chip.html>. The emerging possibilities in gathering data on physical assets could also generate a new level of data signals. MIT researchers are now reconstructing audio signals by analysing vibrations of objects.
[16] Jules Polonetsky and Omer Tene "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Nw J Tech & Intell Prop 11 (5) 239 at 241.
[17] Rubenstein, above at n 6 at 77. By 2020 the majority of data will be collected passively and automatically: Drew Olanoff, "Google wants to serve you ads based on the background noise on your phone calls" (21 March 2014) The Next Web <http://thenextweb.com/google/2012/03/21/google-wants-to-serve-you-ads-based-on-the-background-noise-of-your-phone-calls/>. To this end, Google has already patented targeted ads that listen to the background noise in your phone call to deliver targeted advertising.
[18] Email from Mia Garlick, Head of Policy, Facebook Australia and New Zealand to Mahoney Turnbull regarding data governance structures (8 August 2014).
[19] Fan and Bifet, above n 4 at 1.
[20] Schneier, above n 1.

Moore's law,[21] a new landscape of data accumulation has emerged[22] giving rise to the infinite 'digital tattoo'.[23]

The business model of the digital ecosystem[24] is geared towards our commodification. In this sense, the users are the "products not the customers", and are responsible for generating the value as well as the byproduct.[25] It is becoming clearer that big data poses significant challenges to the sanctity of the individual.[26] The data dependency is an inequitable one in which data assets are subject to market distortion which inhibit users from gaining true value for their data.[27] To facilitate this undemocratic process, a culture is developing in which socio-technical systems are expertly configured to obscure privacy features. The veil that can be pulled over user's eyes promotes a sense of the unknown, to the extent that individuals are now signing over their children for access to desirable online platforms.[28] The issue of consent, or lack thereof is addressed in part V.

The purchasing power of data has been hailed as a disruptive force to the current business model. The 'freemium'[29] model is a contentious element of the big data sensation, and highlights the core reliance on accessible data extraction to enable the data monetisation machine to run smoothly. Firms will not realistically provide free services free unless it enhances their data harvest through valuable sets of personal data points.[30] This industry certainly has the potential to develop anti-competitive behaviour with data brokers mediating the trade in data and overseeing the increasing

[21] Moore's law dictates how overall processing power for computing will double every two years. True to this phenomenon, there has been simultaneous reduction in storage costs and increase in data production.
[22] OECD *Thirty Years After: The OECD Privacy Guidelines* (OECD, 2011) available at <http://www.oecd.org/sti/ieconomy/49710223.pdfAddress> at 8.
[23] Juan Enriquez "How to think about digital tattoos" (podcast, December 2012) TedTalks <https://www.ted.com/talks/juan_enriquez_how_to_think_about_digital_tattoos>.
[24] Andrew McAfee "Big Data: The Management Revolution" *Harvard Business Review* (online ed, Boston, December 2012).
[25] Sive Vaidhyanathan *The Googlization of Everything (And Why We Should Worry)* (University of California Press, Berkeley, 2011) at 111. The data users not only provide the raw materials to determine and deliver relevant search ads, but are used to train its search algorithms to develop new data intensive services.
[26] Mayer-Schönberger and Cukier, above n 6 at 17.
[27] Schneier, above n 1 at 21.
[28] Tom Fox-Brewster "Londoners give up eldest children in public Wi-Fi security horror show" (29 September 2014) *The Guardian*<http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>.
[29] The 'freemium' business model is one in which the company gives away the core product for free to the majority of users and sells premium products to a smaller fraction of this user base.
[30] Viviane Reding, Vice Commissioner European Commission "Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" (speech presented to the Digital Age Innovation Conference, DLD Munich, January 2012) available at <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm>.

digital servitude.[31] The bewildering acceptance of the emptiness of 'free services' seems to indicate online platforms may well be as powerful a narcotic as the Soma was in Huxley's 'Brave New World'.[32]

It is against this backdrop of data wealth that we are witnessing a global call to embrace the digital data renaissance.[33] Industries are moving towards data-driven systems[34] with personal information now operating as the currency of the digital economy, which is growing at unprecedented levels. This is no ordinary asset, but one that can offer a steady stream of innovation and new services to those with the humility, willingness and the tools to listen. [35]

Yet in the face of this compelling movement, the New Zealand economy has shown a considerable lag in embracing the data revolution and could also be criticised for lacking sufficient R&D on data. Combined with a shortage of data experts, there is a definite lack of industrial capability when compared to countries like the United States. New Zealand should consider a similar approach to the UK, which announced the establishment of a world-class research centre for big data science in this year's budget.[36] Indeed new opportunities exist in a number of sectors where the application of these methods is still in its infancy and global dominant players have not yet emerged. New Zealand has the chance to capitalise on this gap and ensure that a robust regulatory framework is created. Treating data as a strategic asset that benefits from clear governance machinery and legal protections will ensure that the data-use ecosystem can move with the pace of this industry.

---

[31] European Commission, above n 4 at 10. Data brokers collect personal information about consumers and sell that information to other organisations using a variety of public and non-public sources including website cookies, and loyalty card programs to create profiles of individuals for marketing and other purposes : Alexandra Suich "Special Report Advertising and Technology: Getting to Know You" *The Economist* (September 13th 2014) at 5. Data broking firms may specialize in selling certain segments, such as eXelate, sells "men in trouble", whereas the IXI firm specialize in the "burdened by debt" segment.

[32] Aldous Huxley *Brave New World* (Harper Collins, New York, 2000) : Alessandro Acquisiti "Why Privacy Matters" (podcast, October 18 2013) TEDtalks <http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters>. These online 'free to download' games may expand our digital freedom, yet also carry the price of privacy invasion and exploitation.

[33] Ian Fletcher, Director Government Communications Security Bureau "Privacy and Security: Identity, society and the state in the internet age" (speech at NZ Privacy Forum Week, Wellington, 7 May 2014) at 2.

[34] Schneier, above n 1.

[35] Mayer-Schönberger and Cukier, above n 6 at 5.

[36] Department for Business Innovation and Skills "Plans for World Class Research Centre in the UK" (United Kingdom Government, 19 March 2014) available at <https://www.gov.uk/government/news/plans-for-world-class-research-centre-in-the-uk>.

## B. The 'Big' benefits of Big Data:

*"The ability to see the details of the market, of political revolutions, and be able to predict and control them is definitely a case of Promethean fire – it could be used for good or for ill, and so Big Data brings us to interesting times. We're going to end up reinventing what it means to be a human society".* [37]

Whilst a lot of criticism has been levelled at the wave of big data flooding our digital environment, there is no doubt that the "dual use"[38] of big data can be readily harnessed to serve the public good in a multitude of ways. The increasing synonymy of big data with data analysis, which is the lynchpin of modern science, considerably constrains any argument against its fundamental value.[39] It is the new 'final frontier' for scientific data research and we seem to be at the beginning of a new era in which we are unearthing novel knowledge.[40] Big data will yield important benefits, whether applied to medicines, climate, food safety or geo-spatial mapping.[41] Moreover, in the commercial sphere, global studies show that it can create 'significant value for the world economy, enhancing the productivity and competitiveness, and creating substantial economic surplus for consumers."[42] The gains to be had from big data are certainly big, and have the power to generate new, life-enhancing outcomes.

Big data offers the capacity to unleash a wave of innovation through the 'featurization' of data.[43] As big data pioneer Sandy Pentland as noted, big data has the power to bring to light information about people's behaviour.[44] The most valuable class of big data does not originate from Facebook posts or RFID's for instance, but from the behaviour-based digital footprints like location data, credit card data and quantified-self data. Importantly, this data manages to operate free from the self-editing

[37] New Zealand Data Futures Forum (NZDFF) *Full Discussion Paper* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/first-discussion-paper_0.pdf> at 10.
[38] Executive Office of the President *Podesta Report: Big Data: Seizing Opportunities, Preserving Values* (Washington, May 1 2014) available at <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf> at 56. This refers to the "dual use" of data, as the contextual use can either be beneficial or harmful.
[39] At 340.
[40] Fan and Bifet, above n 4 at 4.
[41] Paul Ohm "The Underwhelming Benefits of Big Data" (2013) 161 U PA L Rev Online 339 at 339 : Jan Eliasson, Deputy Security General "Remarks on a Data Revolution for Sustainable Development" (Speech presented to the United Nations Independent Expert Advisory Group for Big Data, 24 September 2014) available at <http://www.undatarevolution.org/2014/09/26/deputy-secretary-generals-data-revolution/>.
[42] McKinsey, above n 4 at 1-2.
[43] Tene and Polonetsky, above n 16 at 242. The 'featurization' refers to user-side applications and services based on access to personally identifiable information.
[44] NZDFF, above n 37 at 10.

that underpins personal posts, on platforms like Facebook. Extrapolating certain behaviours derived from evidence not explicitly in the data enables a powerful flow-on effect of comparable analytics. Companies are no longer confined to averages, but have in their possession data that is opening up astounding changes in the granularity[45] of individual analysis.[46]

The connecting force of big data offers "super wicked' [47] correlations between behaviours and outcomes. There are distinct advantages when compared to traditional forms of web science analysis, particularly when examining financial bubbles and recessions.[48] Recent research from Warwick and Boston Universities has produced fresh evidence of methods identifying search terms that precede stock market crashes.[49] The real value also lies in these predictive modelling techniques being applicable to other commercial factors, which could signal a new modus operandi for the financial industry.

The inherent human component of big data also enables the analysis to assume a more holistic form of knowledge discovery. For the public sector, 'smart data' can lead to stronger policymaking decisions by providing sophisticated evidentiary bases.[50] Smart data can then be used in real time to monitor the efficacy of policy decisions and allows for adjustments, which can make solutions even more effective.

Harnessing big data for development is another strategic outcome. Humanitarian-orientated 'Born Digital' projects are indicating the transformative impact of data through real-time feedback and

[45] The 'granularity' of data refers to the customized breakdown of personal data sets that offers greater insights into an individual's behavior patterns.
[46] NZDFF, above n 37 at 10.
[47] Jonathan Boston "A New Global Climate Change Treaty – Can Humanity Deliver? Our Challenge after Durban for 2015" (paper presented at University of Otago, Dunedin, 14 March 2012) at 4. "A super-wicked problem has the following characteristics: the policy is complex and controversial, with competing problem definitions; all the available solutions are problematic; delay is costly; those most responsible for the problem have the least incentive to solve it' and the central control or enforcement mechanisms are weak".
[48] NZDFF, above n 37 at 11.
[49] Alice Truoing, "How Google searches can predict the next stock market crash" (July 24 2014) Fast Tech Company <http://www.fastcompany.com/3033661/fast-feed/how-google-searches-can-predict-the-next-stock-market-crash>. By correlating the most valuable information in search engine data that have less obvious semantic connections to events, the potential exists for historic links to be gauged, and future falls anticipated.
[50] Spark "Submission to the New Zealand Data Futures Forum" (Wellington, July 2014). Spark chooses to use the term 'smart data' rather than big data. Smart data can provide deep analysis of a problem, help identify root causes to a problem and find correlations with other data. The use of this term emphasizes the latent value inherent in data sources, and also avoids the negative connotations of the harms connected to big data.

early warning capabilities.[51] Catalyst projects such as 'Global Pulse' and UN work in Asia, attest to the power of detecting emerging vulnerabilities. [52] Looking at its use in the developed world, the number of lives 'saved' by a Stanford professor pursuing data mining techniques and novel signal-detection algorithms, reinforces the significant gains in healthcare that can flow from big data.[53]

The economic benefits from geospatial data are equally optimistic. The flood of fresh sensing data, combined with 'smart grid' functionality is signalling a new era of 'sensing cities' as seen in the context of Christchurch.[54] Access to mobility data to track population trending patterns could help spur constructive outcomes in terms of Auckland's housing developments issues.[55] The working relationship between Auckland Council and citizens to enable strategic assessment of growth capacity is just the beginning of new data-driven methodologies for dynamic public engagement.

The range of data points required for these investigations is diverse, and is being facilitated by the trend towards wearable technology and mobile fitness apps. The extent to which mobility-tracking should be mined for arguably beneficial societal outcomes remains controversial. Various stakeholders are indicating interest in this trend, not all of which intend to use it for economic enrichment. In the education space, a South Island primary school has proposed an uptake on microchip 'Fitbit' [56] style bracelets to enable student behaviour tracking. [57] While this has raised cries of 'surveillance-school' systems, there is a case for these devices fitting seamlessly into our lives to subconsciously capture activity. The rise of the 'Fitbit' device shows potential for being more than a fad, whether this has an educational, wellbeing or commercial focus. [58]

---

[51] Price Waterhouse Coopers *PWC Big Data: big Benefits and imperilled Privacy* (United States, June 2014) at 5.
[52] Fan and Bifet, above n 4 at 2.
[53] Tene and Polonetsky, above n 16 at 246. This data study showed the adverse effects of a diabetic by exposing the correlation of 27,000 cardiac arrests from using the drug. This led to the drug's withdrawal from the market.
[54] Sensing Cities "Project to Create Sensing Cities Launches in Christchurch" (4 September 2014) Sensing City <http://www.sensingcity.org/stay-informed/project-to-create-%E2%80%98sensing-cities%E2%80%99-launches-in-christchurch>.
[55] Interview with Cyrus Facciano, General Manager of Qrious (Mahoney Turnbull, July 25th 2014).
[56] Fitbit "The Fitbit Story" <http://www.fitbit.com/nz/story>. The emerging trend of fitbit-style bracelets, google glasses and wearable technologies is catapulting quantified self data to a mainstreamed mode of analysis.
[57] Interview with Swannanoa Primary Principle (Guyon Espiner, Morning Report, National Radio, 31 July 2014).
[58] Fitbit, above n 56. Users are taking 43% more steps by using the Fitbit. The technology uses an accelerometer which reflects personalized statistics that generate unique welfare profiles.

Against this backdrop of 'quantified self' data, it is possible to project positive visions of personal profiling from a price point perspective.[59] Although digital discrimination and service exclusion have been cited as a strong basis for negating the usefulness of 'quantified self' data,[60] there is potential for industry to fine tune prices proportionate to lifestyle choices, reflecting the trends towards the 'segment of one.'[61] Insurance companies in the UK are already jumping on this bandwagon, offering packages that cut premiums and sponsor gym memberships to enhance the longevity of their customers.[62] This form of positive price discrimination suggests the scope for big data to help future-proof and incentivize sustainable lifestyle choices, is rapidly expanding. The potential benefits are clear, however there is a clear lack of regulation surrounding data use that needs to be addressed.

## C. The 'Big' Concerns of Big Data: The era of predictive analytics

Big data poses serious privacy concerns that could stir a regulatory backlash, stifle innovation and dampen the data economy. The risks we are seeing emerge have the potential to override the value to be gained from smart data.[63] Thus, stronger data protection and data management must be engineered. New Zealand's legal mechanisms that deal with privacy and data protection should be re-examined and refreshed to cope with the negatives of predictive analytics.

The prime cause for anxiety stems from how individuals can be profiled and targeted.[64] This poses a serious threat to data subjects being able to exercise inherent freedoms safeguarded in the New Zealand Bill of Rights, namely Freedom of Expression and Freedom of Thought, Conscience and Religion.[65] In the context of big data, this manifests in the restrictions on an individual's capacity to act with agency and consume online information without being subject to unjustifiable manipulation. The issue here is not aggregation, but rather disaggregation of personal insights that

[59] Interview with Dele Atanda, founder of the Universal Declaration of Digital Rights and Digiterra (Mahoney Turnbull, 30 July 2014).
[60] See below Part 1, section C.
[61] United Kingdom Office of the Information Commissioner *Big Data and Data Protection* (London, July 2014) <http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf> at 11. This expands upon the 'segment of one' approach, where product and services offerings are fine-tuned according to the individual.
[62] Pruhealth "Vitality Health Programmes" <http://www.pruhealth.co.uk/>.
[63] Eliasson, above n 41.
[64] Rubenstein, above n 6 at 24 : Ryan Calo "Digital Market Manipulation" Geo Wash L Rev (2014) (forthcoming).
[65] New Zealand Bill of Rights Act 1990, s 13, s 14.

can be brokered and used against the individual.[66] There is no shortage of evidence for the ability of analysts to proactively anticipate, persuade and manipulate individuals and markets.[67] The criticisms directed at companies who "vampirically feed of our identities" should not be taken lightly, and highlights the looming 'dataveillance' that is casting big data in a darker light.[68] The most recent White House Report has reinforced this sentiment and called for expanded technical expertise to halt the discrimination leading big data down a digitally manipulative track.[69]

The danger of predictive profiling is a persuasive factor in the appeal for a stronger data protection regime. The 'pregnancy score' formulated by Target provides one pertinent example of how the big data industry is encroaching on the personal realm and resulting in discriminatory profiling and constraining fundamental freedoms.[70] Corporates are becoming increasingly adept at executing profiling with alarming specificity and foresight. Target's capacity to employ time-tracking analytics on the types of purchases made by customers, enabled a timeline that predicted precise stages of their customers' pregnancy cycles.[71] It was against this backdrop that the 'creepiness' Panopticon-like threshold set in[72], and customers began to question the extent of Target's consumer tracking systems.[73] This predictive analysis is disturbing when sensitive categories protected by New Zealand's rights-based legislative instruments, such as health, race and sexuality, are compromised.[74] It is one thing for a customer to be recommended books they may be interested in to enable more 'efficient' consumption patterns, but it is quite another to surreptitiously track when a customer is

[66] Fletcher, above n 33.
[67] World Economic Forum *Rethinking Personal Data* (Geneva, May 2014) available at <http://reports.weforum.org/rethinking-personal-data/> at 24.
[68] Gitelman, above n 13 at 10 : David Lyon *The Surveillance Society* (Open University Press, Philadelphia, 2001) at 3. "Surveillance in the context of big data is an expansive term, and not just limited to espionage or video monitoring, but "any collection and processing of personal data, whether identified or not, for the purposes of influencing and monitoring those whose data has been garnered."
[69] Executive Office of the President, above n 38 at 30. The Report highlights the capacity to segment data subjects, and stratify customer experiences so seamlessly as to be almost undetectable.
[70] Charles Duhigg "How Companies Learn Your Secrets" *New York Times Magazine* (online edition, New York, 16 February 2012). This revealed the situation here the girls father only discovered his teenage daughter was pregnant after Target had pre-determined this via her buyer behavior and sent various pregnancy related promotional material to the home address.
[71] Tene and Polonetsky, above n 16 at 253.
[72] Jeremy Bentham *Panopticon; Or, The Inspection-House: Containing The Idea of a New Principle of Construction applicable to any Sort of Establishment, in which Persons of any Description are to be kept under Inspection: And in Particular To Penitentiary-Houses, Prisons, Houses of Industry, Workhouses, Poor Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals, And Schools: With a Plan Of Management adapted to the principle: in a series of letters, written in the year 1787, from Crecheff in White Russia* (T Payne, London, 1791).
[73] Quentin Hardy "Rethinking privacy in an Era of Big Data" *The New York Times* (4 June 2012) <http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?_php=true&_type=blogs&_r=0>.
[74] New Zealand Human Rights Act 1993, s 21.

pregnant before her closest family even know. Alarmingly, the accumulation of knowledge organizations hold about users entitles them to infer desires before individuals even form them, and to buy products on their behalf before they even know they need them.[75]

Therefore, the gender-based discrimination that flows from predictive profiling reinforces the need for a data protection ecosystem that better defends against threats to an individual's privacy.[76] The current ecosystem generates a user experience in which the individual is presented with gender-biased digital experiences according to societal assumptions. The dangerous development of Facebook's 'Promoted Posts'[77] adds another layer to the predictive profiling problem through the customized filtering of 'irrelevant' content. The way that profiling can cut across Human Rights protections should raise alarm bells. The effects of skilful targeting ought to propel the establishment of a legal framework that guards against the discrimination caused by powerful analytics.

Another core concern related to discriminatory profiling is its capacity to be ethnicity-based.[78] In the New Zealand sphere, caution is being urged in regards to genetic indigenous material being used for discriminatory purposes. Biometric profiling, and the use of ethnicity as a digital flag, could have stark ramifications, particularly in light of well-documented criminal justice biases in regards to Maori and Pacifika.[79] This could spark an unhealthy drift towards marginalisation from services based on analytics, which may not necessarily have accurate correlative strength.

Another facet of the profiling dilemma is the danger of employer profiling.[80] Checks on prospective candidates are frequently being executed without their knowledge.[81] Recent New Zealand studies[82] indicate the extent to which data-driven categorical recruitment determinations restrict an individual's ability to know and be considered for job opportunities without prejudice, which the

[75] Acquisiti, above n 32.
[76] New Zealand Human Rights Act 1993, s 21 (1)(a).
[77] Facebook <http://www.facebook.com/help/promotee> : Richard Metzger "Facebook: I want my friends back" Dangerous Minds (24 October 2012) <www.dangerousminds.net>.
[78] Omer Tene "Privacy: For the Rich or for the Poor?" (26 July, 2012) Concurring Opinions <http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html>.
[79] Committee on the Elimination of Racial Discrimination *CERD Report on New Zealand* CERD/C/NZL/CO/17 (2007) : New Zealand Human Rights Act 1993 s 21 (1) (g).
[80] Eric Markowitz "Meet a Startup with a Big Data Approach to Hiring" (September, 2013) INC <www.inc.com/eric-markowitz>.
[81] Andrew Couts "Senator Promises Bill to Block Invasive Employer Facebook Checks" Digital Trends (23 March 2012) <http://www.digitaltrends.com/social-media/senator-promises-bill-to-block-invasive-employer-facebook-checks/>.
[82] Dr Kathleen Kuehn "Media Technologies and Surveillance" (Victoria University of Wellington, 2014) available at <http://www.victoria.ac.nz/seftms/about/news#a248532>.

Human Rights Act sets out to guard against.[83] The added pressure to be 'on the grid' and engage in platforms such as Linkedin in order to mitigate accusations of technical illiteracy, also highlights the powerful reach of employer bias. The threat to New Zealanders' rights to freedom from discrimination again calls for careful consideration of how data ought to be managed by companies, who have the potential to misuse the analytics at their fingertips.[84]

The profiling problem and its threat to freedom from discrimination can also be seen in the automated decision-making assumptions.[85] This situation seems to have the hallmarks of Chomsky's 'manufactured consent',[86] where data controllers have enormous discretion in determining what the user 'wants' to see. The trend towards 'dynamic pricing' is shifting focus onto browser history and postcodes as the key pricing mechanisms in online shopping experiences.[87] Invisible decisions made on the basis of data-driven assumptions also run the risk that users, faced with increasing privacy intrusions, will decide to forgo online-enabled services. Not only does this deepen the digital divide,[88] and exacerbate issues around s14 of the Bill of Rights Act, but also spurs negative impacts on innovation and engagement in the digital economy.[89]

The impacts of profiling are wide-ranging and reinforce the power imbalance at the heart of data analytics. Sir Tim Berners-Lee is one outspoken advocate for addressing such disparity. Whilst he recognizes that exploiting data, such as "how many stairs I've been walking up" can provide useful individual services, this is premised on appropriate levels of users information symmetry.[90] A core concern is that online platforms realistically engage in data siloing, which reinvigorates the angst of

[83] New Zealand Human Rights Act 1993, s 21.
[84] : New Zealand Bill of Rights Act 1990, s 19 : New Zealand Human Rights Act 1993, s21.
[85]New Zealand Bill of Rights Act 1990, s 14.
[86] Noam Chomsky *Manufacturing Consent: The Political Economy of the Mass Media* (Pantheon, New York, 1988).
[87] Thorin Klosowski "How Websites Vary prices Based on your Information (and what you can do about it)" LifeHacker (July 2013) <http://lifehacker.com/5973689/how-web-sites-vary-prices-based-on-your-information-and-what-you-can-do-about-it>. Dynamic Pricing encompasses the trend of price variability based on location data.
[88] Statistics New Zealand "The Digital Divide" (Wellington, 2013) available at <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/digital-divide/introduction.aspx> : Joy Liddicoat *Association for Progressive Communications New Zealand Digital Freedoms Report* (Wellington, 2014) available at <https://www.apc.org/en/irhr/i-freedom-nz/about>.
[89] Barbara Daskala and Ionnis Maghiros *Digital Territories: Towards the Protection of public and private space in a digital and Ambient Intelligence environment* (Institute for Prospective Technological Studies, Seville, 2007) at 11.
[90] Ian Katz "Tim Berners-Lee: demand your data from Google and Facebook" *The Guardian* (online ed, London, 18 April 2012) <http://www.theguardian.com/technology/2012/apr/18/tim-berners-lee-google-facebook>.

'secret big data', prompting Kafkaesque visions of inhumane bureaucracies.[91] As Berners-Lee warns, it does not take much for the pendulum to swing too far in the data-obscurity direction. Thus, identifying and anticipating the harms is crucial in addressing the precarious relationship between data users and industry, and formulating stronger safeguards to manage the risks of profiling.

Another destructive attribute of the big data industry is the phenomenon of 'big data washing' and the breach of an individual's wall of trust. There is a concerning trend for "big data cheerleaders" to talk of the benefits, whilst blurring the significant with the trivial.[92] Google Flu Trends[93] casts light on the questionable results from analysing mobility-based data for healthcare purposes. In this instance, it is important to note that Google was breaching the user's in several ways. Firstly, they were accessing private data searches beyond the normal search query data. Secondly there was known to be limited value in the granularity of their heat mapping output. As the maps were not able to examine data at a postcode level, Google's failure to share this with the Centre for Disease Control reflects the limited value of the map's predictive strength.[94] Another breach of trust was evidenced by the privacy debate being held firmly within the walls of Google, preventing any consultation or user acquiescence, which in the New Zealand context would restrict the fulfilment of s14 NZBORA. In light of these privacy and rights-based concerns, instantly approving initiatives like Google Flu Trends may be unwise.[95] This begs the question whether corporates, under the pretence of societal good, should be limited in operationalizing these big data projects.

On a technological level, there is also the danger in the blind faith in algorithms, and their potential to backfire. Algorithmic-based decisions through automated processes are naturally susceptible to imperfect aggregations, and require increasing trust in their completeness.[96] Although data analysis is an interpretive process which is prone to error, there is a point at which this becomes more than an acceptable mishap.[97] Claims regarding the impressive accuracy of big data can mislead.[98] In fact,

---

[91] Daniel Solove *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, New York, 2006) at 27.
[92] Ohm, above n 41 at 340 : UK Information Commissioner's Office, above n 61 at 4. Many businesses are skeptical of the 'hype' surrounding big data. This may be because they do not consider that what they are doing creates any new issues for them, in terms of data protection or data analytics.
[93] Mayer-Schönberger and Cukier, above n 6 at 179. Google's algorithm was the result of testing 450 million mathematical models. The algorithm was able to detect flu outbreaks up to two weeks faster than physicians at the Centre for Disease Control.
[94] Ohm, above n 41 at 341.
[95] At 344.
[96] Bendert Zevenbergen *Ethical Privacy Guidelines for Mobile Connectivity Measurements* (Oxford Internet Institute, 2013) at 19.
[97] Tene and Polonetsky, above n 16 at 272.

the example of false correlations between the S&P 500 stock index and butter production in Bangladesh, highlight the fallible nature of analytics.[99] There is a sense that false confidence in the 'big data saviour' could spur negative outcomes if taken to the extreme.

*"Big data is coming, like it or not. We have an opportunity to shape it, to ensure it operates for us, not on us. The coming debate whether and how we might do this promises to be a vigorous one."* [100]

[98] Nassim Taleb *Antifragile: Things that Gain from Disorder* (Penguin Books, New York, 2012) at 127. As Taleb explains, when data is sterile, it can become meaningless. See chapter 24 of Taleb's work on Big Data and the Researcher's Opinion.
[99] Fan and Bifet, above n 4 at 3. Aside from the butter correlation, many other strange correlations were found to occur.
[100] Ohm, above n 41 at 346.

# PART III

## NEW ZEALAND'S DATA PROTECTION ARCHITECTURE

*"Code changes quickly, user adoption more slowly, legal contracting and judicial adaptation to new technologies slower yet, and regulation through legislation slowest of all. This is not to criticize regulation but to point out that law reform typically follows technological change at a measured rate.* [101]

This chapter outlines New Zealand's legal position on data protection that enables protection of personal information. It discusses the structure of our privacy architecture and the international influences at play. It then explains the technical inconsistencies concerning how the Privacy Act recognises personal information focusing on the legal loophole created by the outmoded rationale that de-identification techniques *can* ensure non-identifiability. This section will also expose the new category of personally *predictable* information, which poses a nuanced threat to the data protection regime. Thirdly it will explore the issues regarding Principle 3, and its clash with the future repurposing of data. The chapter begins to consider how New Zealand would be better placed to respond to this issue and which legal tools may be required to tackle the divide between technological advancements and privacy safeguards.

### A. The Privacy Act: An 'adequate' instrument?

The New Zealand position on data protection has its origins in the Universal Declaration of Human Rights 1948 and the International Covenant on Civil and Political Rights 1966, which both acknowledge the right to privacy as a fundamental human right.[102] New Zealand's current data protection law has been strongly influenced by the 1980 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, which sets out eight core principles to protect data.[103] These principles are reflected in the New Zealand's Privacy Act 1993.[104] Additional data

[101] Ian Brown *Regulating Code* (MIT Press, Cambridge, 2013) at xv.
[102] Interview with John Steadman, Legal counsel at Spark (Mahoney Turnbull, 8 July 2014).
[103] OECD *OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data* (Geneva, 1980) available at <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

protection rights are contained in the NZ Bill of Rights Act, which affirms rights against unreasonable search and seizure and liberty of the person.[105]

The influence of the OECD Principles and New Zealand's commitment to them is evidenced in the 2010 amendment of the Privacy Act.[106] These Guidelines, rooted in strong rights based ideal, reflect New Zealand's commitment to advancing human rights and the free flow of information and ideas.[107] The Privacy Act avoids taking a proscriptive approach and instead lays out 12 principles that apply to both the public and private sectors when they hold "personal information" about a natural person.[108] A positive feature of the Act is the latitude in application of the principles to suit the circumstances of a wide variety of different agencies.[109] The wider spectrum includes both persons and companies, yet excludes various branches of the executive (such as Ministers) and the news media.[110] This flexible approach also helps with adaptation to new technologies and shifts in privacy expectations. It was for this reason that the Law Commission in 2011 did not want to overturn the fundamental approach of the Act, believing the principles should remain largely intact, albeit with some amendments.[111]

In contrast to the debates concerning the inadequacy of data protection legislation in countries like the United States, New Zealand's Act has been hailed an 'elegant transition from the analogue to the digital world".[112] From the Privacy Commission's perspective, the Act sits as a leading "jurisdictional benchmark" in its ability to manage the different values and interests in a data driven future.[113] Thus, it offers a competitive advantage and an excellent platform from which to strengthen and modernise in the age of analytics.

---

[104] New Zealand Privacy Act 1993.
[105] *R v Jefferies* [1994] 1 NZLR 290 (CA).
[106] New Zealand Privacy Act 1993, Annex 5 A : Michael Kirby "Legal Aspects of Transborder Data Flows" (1991) 11(3) Computer L J 233 at 234.
[107] Lee Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) at 113.
[108] Steadman, above n 102.
[109] New Zealand Law commission Questions and Answers to the Law Commission Review 2011 (Wellington, August 2011) at 1.
[110] At 4.
[111] At 2.
[112] Interview with Vikram Kumar, Chief Executive New Zealand Internet Party (Mahoney Turnbull, 25 April, 2014).
[113] John Edwards "New Zealand's Data Future: A View from the Privacy Commissioner" (Wellington, 4 July) at 1. See Bruce Arnold's analysis in Bruce Baer Arnold "Ending the OIAC and new frameworks for privacy law" (2014) 11(5) Privacy Law Bulletin 66 at 66.

Such international repute prompted the European Union to recognise New Zealand's Act as offering an 'adequate' standard of data protection for the purposes of European Law. This recognition reflects Europe and New Zealand's common commitment to upholding human rights and is a claim only a handful of other countries can assert.[114] The ability for European businesses to transfer data to New Zealand without requiring special contractual provisions is an important commercial consideration for New Zealand companies wanting to offer data processing services on a global scale.[115] It is important to note that although there are no specific provisions protecting data transferred to third countries, s 10 provides for situations when data is collected from New Zealand, and a New Zealand agency transfers information offshore.[116] In this instance, the New Zealand-based disclosing agency will remain liable for any subsequent breaches. The EU Working Party's report alerted the Privacy Commissioner (PC) to the need to maintain oversight of transfers to countries who do not have 'adequacy' status.[117] It is in the interests of New Zealand companies and policymakers to minimise risks of harm or loss by establishing strong data management frameworks. The value of New Zealand's alignment with OECD guidelines reinforces the need for both New Zealand and the EU to be acutely aware of advances in big data, to ensure the technical realities translate into privacy protection.[118]

[114] European Commission Directorate of General Justice Opinion 11/2011 on the level of protection of personal data in New Zealand (Brussels, 2011) available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf#h2-13> at 5 : New Zealand Office of the Privacy Commissioner "NZ Data Protection gets tick from EU Committee" (13 April 2011) <http://privacy.org.nz/news-and-publications/statements-media-releases/nz-data-protection-law-gets-tick-from-eu-committee/>.

[115] EU Data Protection Law "EU Data Protection Regulation Timeline" (13 May 2014) <www.eudataprotectionlaw.com>. The need for New Zealand and EU alignment highlights the need to take note of upcoming changes to the EU's Data Protection Directive, which will reach final agreement in 2015. The next phase will be the Council of Ministers meeting to revise the text in October 2014. It will again be analysed at Forum Europe's 5th Annual Data Protection Conference on 9 December 2014 : Hunton Williams "Privacy Law Update" (podcast, 16 September 2014) <www.hunton.com/media/20140916_privacy/20140916_privacyupdate2_Mono2.mp3>.

[116] New Zealand Privacy Act 1993, s 10, s 3 (4).

[117] Cabinet Social Policy Committee "Government Response to Law Commission Report: Review of the Privacy Act" (12 March 2012) SOC Min (12) 3/1 at 2. The issue of international interactions also prompted the Law Commission to recommend a new obligation to ensure overseas recipients are able and willing to observe acceptable privacy standards.

[118] The need for New Zealand to stay in line with the EU Data Protection Directive will help ensure a new approach does not trading opportunities for "New Zealand Inc" are not jeopardized. An entirely new approach for New Zealand's Privacy Act would only create medium to long-term uncertainty.

## B. Two 'key features of the Act' from the Commissioner's standpoint

In the recent submission to the NZDFF, the PC asserted two key features of New Zealand's privacy law that render it an effective model to address some of the big data challenges.[119]

**1.** The first is the breadth of the definition of 'personal information', which allows the Act to encompass de-identified and pseudonymous information.[120]

The most recent Law Commission Report explained that the definition of personal information only requires that the individual be 'identifiable', as opposed to 'identified'.[121] It must be clarified whether this encompasses instances where, when combined with other information, identification is possible.[122] For this reason, a test akin to the United Kingdom's 'reasonableness' criteria for identifiability was proposed, whereby identification must be "reasonably practicable" and not simply theoretically possible.[123] To adequately tackle this issue, the Commission considered it most fitting for the PC to release guidance material, since an additional clause would "significantly lengthen and complicate the current definition."[124]

**2.** The second aspect entails the broad exceptions to principles on collection, use and disclosure, where information will be used in a form in which individuals will not be identified.[125] This means 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 identifiable, then they are free to do so without having to obtain consents that apply to all future uses.[126] There is still an integral feature of trust in this bargain, as agencies have responsibilities to collect data only if they have a use for it, can store it securely, and must delete it when they no longer have a use for it.[127]

---

[119] Cabinet Social Policy Committee, above n 117 at 4.
[120] John Edwards, above n 113 at 3.
[121] New Zealand Law Commission Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (Issues Paper, 2010) at 3.20.
[122] At 3.20.
[123] At 2.53. Other jurisdictions such as the UK have required the Information Commissioner to release guidance elaborating on the EU Data Protection Directive that it must be more than a "hypothetical possibility" of identifiability.
[124] Law Commission, above n 121 at 3.20. Cabinet Social Policy Committee, above n 117 at Attachment 1.
[125] Edwards, above n 113 at 3.
[126] New Zealand Privacy Act 1993, s 6, Principle 3.
[127] At s 6, Principles 3,4,5,9.

The PCs confidence in the available exceptions[128] to cater for beneficial re-use of data echoes the Law Commission's conclusion. However the Commission failed to acknowledge the re-use issues related to aggregated data sets stemming from groups as opposed to single individuals.[129] The consensus was that if the uses of aggregated information as described by Gunasekara were a problem, they could be dealt with in other ways, such as through consumer legislation.[130]

The use that Gunasekara was referring to, in which the aggregated data could still be used for effective group classification, relates to the predictive profiling that may have discriminatory or otherwise adverse effects on individuals. This foresight was a valuable addition to the review, yet was largely sidelined for fear of casting the net too wide. While the issue of widespread aggregation may not have been so acute in 2011, the concern is much more real now. The technological advances since Gunasekara's comments now pose greater privacy risks and should be at the forefront of strategic planning for data regulation.

Not only does the Act afford the Use and Disclosure exceptions, but coupled with the technological capacity of re-identification, there cannot be a "reasonable belief" that the information will be used in a form in which "the individual concerned is not identified".[131] By failing to respond to information being identifiable, as opposed to conclusively identified, the agency can simply believe on 'reasonable grounds' that sharing would be a justified exercise of the exception.[132] In light of such latitude to claim "reasonable" exceptions, it is understandable why disparaging comments have been directed at the statute. The ability for organisations to "drive a truck though the Act" suggests the law may be heading for a blunt head-on collision with big data.[133]

Even if the Act was to acknowledge that identifiable data should be recognised in the provisions regarding disclosure limits, another issue remains. This is due to a new subset of personal

[128] At s 6, Principles 10 (f) (i)(ii), 11 allows an agency to use the information as it wants, provided it is used in a form in which the individual concerned is not identified, or is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.
[129] Law Commission Report, above n 121 at 2.50.
[130] At 2.50. Auckland University academic Gehan Gunasekara's submission was expressly mentioned. His point was that the de-identification techniques, which are prompting information to be aggregated so that it no longer relates to identifiable individuals, still enable classification into groups.
[131] New Zealand Privacy Act, s 6, Principle 10 (f)(i) and 11 (h)(i).
[132] At s 6, Principle 10, 11. In this instance, the phrase "on reasonable grounds" does not entail any objective standard but rather enables the agency to determine according to their interests, whether it is a "reasonable" use that can legitimise disclosing the personal information.
[133] Interview with Paul Roth, University of Otago Law Professor (Mahoney Turnbull, 7 August, 2014).

information which has emerged, which threatens to upset the already precarious balance between data sharing and privacy protections. Its emergence reinforces the Microsoft Privacy Summit's conclusion that "to limit personal data to what is recognized as 'personal' is too narrow".[134] The result is a class of 'personally predictable information', that does not even hinge on being personally identifiable let along identified.[135] Recognising the inherent tensions in this nuanced category of personal information is critical in appreciating how big data can circumvent current notions of privacy law.

The Law Commission did pinpoint identifiability as a challenge, noting it would "become more acute over time". Yet the decision not to engage proactively in reframing the nature of identifiable material indicates a lack of foresight regarding the relevance of this class of data.[136] Accordingly, companies enjoy unbridled ability to leverage the exception, and justify the disclosure of effectively personal information. This implies that New Zealand's adequacy status is dubious in the context of big data. In assessing its suitability, let us now turn to explore some of the technical inconsistencies.

### i. The de-identification myth

Notwithstanding the lack of guidance on the process of anonymisation,[137] the technical inconsistencies that form potent threats to privacy hinge on two factors:

1. The concept of de-identification has become increasingly outdated.[138] Not only is de-identification now recognised as an illusory guard against privacy breaches, it is also subject to a re-identification arms race.[139]

---

[134] Fred Cate and Viktor Mayer-Schönberger *Notice and Consent in a World of Big Data: Global Privacy Summit Report and Outcomes* (Washington, 2012) at 10: Bernard Stiegler "Die Aufklärung in the Age of Philosophical Engineering" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) Digital Enlightenment Yearbook (IOS Press, Amsterdam, 2013) at 31.

[135] Andy Green "Personally Identifiable Information Hides in Dark Data (13 April 2013) Varonis <http://blog.varonis.com/personally-identifiable-information-hides-in-dark-data/>.

[136] NZ Law Commission, above n 109 at 54.

[137] New Zealand has refrained from incorporating into the Act any specific indications on de-identification protocols or how the de-linking of personal identifiers is meant to occur. The Australian Privacy Act with its recent changes to this sphere, now references the technique of de-identification, which is bolstered by numerous anonymisation guidelines and resources released by the National Statistical Service.

[138] Ann Cavoukian and El Emam *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (Ontario, June 2014) available at <http://www2.itif.org/2014-big-data-deidentification.pdf> at 3. This report defines de-identification as the process of removing or modifying of both direct identifiers and indirect or quasi-identifiers, unlike 'masking' which only involves the removal or modification of direct identifiers:

2. We now have a new genre of 'personally identifiable information' which routes around the element of identifiability.[140]

De-identification and its opposing force, re-identification, are disrupting the privacy landscape.[141] It is now well accepted that de-identified data sets can still be attributed to specific individuals, which casts doubt on the fundamental distinction between personal and non-personal data.[142] At the same time, re-identification has heightened the harms associated with invasive aggregation methodologies by allowing data controllers to link more information to an individual's profile.[143] Like an unbalanced chakra, the 'yang' of re-identification appears to be overpowering the 'yin' of de-identified material. Thus the body of data is out of balance, and upsetting our cyber law system.

The developments in de-identification and re-identification can be seen by the out-dated guidance from the UK Information Commissioner included in the Law Commission's report.[144] The view that "a slight hypothetical possibility that someone might be able to reconstruct the data in a way that the data subject is identified, is not sufficient to make the individual identifiable for the purposes of the Directive," reflect the rapid changes that have occurred.[145] The reference to data reconstruction being 'hypothetical' is interesting, and could now be perceived as naïve. At the time of its publication however, nimble methodologies were only nascent. Indeed, the work of privacy expert

---

See also Spark's submission to NZDFF ("data which has been treated to decrease the ability to be linked back to identify individuals").

[139] Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1752 : Paul Schwartz and Daniel Solove "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) NYU L Q Rev 1814 at 1879-1883. This race is gaining traction with computational innovation which exposes individuals to "the database of ruin" : The crossing of identify boundaries is not a new phenomenon but the ability to easily do so in the digital era is a significant innovation and represents a normative shift in social expectations of privacy.

[140] Green, above n 135.

[141] Ohm, above n 139 at 1704.

[142] The Sweeney Test, highlighted by Ohm, refers to the research pioneered by Latanya Sweeney and made accessible by Ohm. The results of the test marked a turning point in debunking de-identification as she was able to show that in 2000, 87 percent of all Americans could be uniquely identified using only three bits of information: post code, birthdate and sex.

[143] Daniel Solove "A Taxonomy of Privacy" (2006) 154 Penn. St L Rev 477 at 511. Big data makes aggregation of datasets more granular, more revealing and more invasive.

[144] New Zealand Law Commission Report, above n 121.

[145] United Kingdom Information Commissioner's Office *Data Protection Technical Guidance Determining What is Personal Data* (2007) <http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx> at 7.

Alessandro Acquisiti is proving how creative algorithmists can be in finding "new and exotic ways to link information to individuals".[146]

Whilst pro-market thinktanks may be producing evidence to prove that the risks of re-identification are grossly exaggerated,[147] the vast majority of computer scientists are consistently rebutting this claim.[148] Fresh evidence from Princeton scientists shows that attempts to quantify the efficacy of de-identification are unscientific and promote a false sense of security by assuming "artificially constrained models of what an adversary might do".[149]

It appears that de-identification, traditionally viewed as a silver bullet, has been debunked.[150] De-identified material is not a stable category, but rather a transition point to ultimate re-identification, a point which is becoming easier to reach.[151] This cuts to the core of the increasingly malleable nature of personal information.[152] Importantly, it relates to the second technical inconsistency that is threatening the data dynamic: the personally predictable nature of data.

### i. Personally predictable genre

The Commission's 2011 Report recognised that an absolute ability to be 'identified' was no longer a reasonable standard to aspire to; the emphasis should be on being identifiable. This insight was supported by the PC recognising that over time, more information would start falling within the definition of personally identifiable information.[153]

---

[146] Acquisiti, above n 32. Using facial recognition software, Acquisiti was able to derive social security numbers and intimate details about the individuals involved in the study.

[147] Ann Cavoukian and Daniel Castro *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (Information and Privacy Commissioner, Ontario, 2014) <www.itif.org/2014-big-data-deidentifaction.pdff> at 2.

[148] Arvind Narayanan and Edward Felten "No silver bullet: De-Identification Still Doesn't Work" (unpublished manuscript, Princeton University, 2014) at 1. Relying on Protocols like anonymisation, pseudonymisation, encryption, key-sharing, data-sharing and noise addition, are insufficient.

[149] At 5. The 'penetrate-and-patch' method that has been recommended, in which systems are fielded with live data, broken through challenges and then revised, has been largely ineffective in both traditional information security development and in de-identification efforts.

[150] Ira Rubenstein, Ronald Lee and Paul Schwartz "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) U Chicago L Rev 261 at 268-29.

[151] Colin Bennett and Christopher Parsons "Privacy and Surveillance" in William Dutton *The Oxford Handbook of Internet Studies* (Oxford University Press, Oxford, 2013) at 499. The ability to re-identify demonstrates the dangers of releasing granular information about search terms.

[152] Solove, above n 143 at 1814.

[153] New Zealand Law Commission Report, above n 121 at 2.48. Reference was also made to the International Institute of Communications' Report on Personal Data Management, which concluded a simplistic, binary

Google and other similar companies made submissions opposing an expansive interpretation of personal information to the extent of identifiability. They clarified an unduly wide definition would subject service providers to "potentially unnecessary regulation regarding collection, notification and use of disaggregated and uncombined pieces of information". These 'pieces of information' serve as essential data points that determine the ability of companies like Google to provide 'freemium'[154] services. They would not, Google argued, necessarily be "intended to identify a particular individual".[155] While reflecting the commercial realties of the data industry's business model, this resistance indicates a more nuanced understanding of re-identification forecasts. The Commission should have been more cognisant of this. Online service providers like Google foresaw the growing trend of inventive algorithms and the strategic significance of being able to engage in the 'necessary' relinking of "uncombined" data sets in ways that would not specifically subject them to privacy legal frameworks.

The ease with which 'recalibration' occurs has shifted. The reality is that personally identifiable information is in a state of flux.[156] By using the terminology of 'not personally identifiable', the Act makes no distinction between data entered into standardised fields and information entered as free text.[157] The development of the 'semantic web'[158] reflects the increasing flexibility with which data sets are interpreted to derive granular strains of value. The demonstrates that technologists are increasingly adept at interpreting free unstructured text and linking it back to a person.

The issue is that in the digital domain of 'dark data', invention of algorithms will not stop anytime soon. If Acquisiti's work concerning augmented reality and facial recognition is anything to go by, we are still in for some major upheavals. This trend is likely to see us progressing towards increasing

---

and static data- management policy that dictates a priori whether data is considered personal, is insufficiently flexible for the rapidly evolving digital world.

[154] Freemium, above n 29.

[155] New Zealand Law Commission Report, above n 121 at 2.48.

[156] Ohm, above n 139 at 1704. Ohm has been bold enough to disregard the concept of 'personally identifiable information' completely. He advocates instead for embracing the ever-expanding category, and focus on the risks of harm in specific contexts, weighed against the benefits of free flow of information in those contexts.

[157] Green, above n 135 : UK Anonymisation Network <www.ukanon.net>. The term 'identifiers' is often misunderstood to simply mean 'formal identifiers' such as the data subjects name, address etc. But identifiers could in principle include any piece of information, or combination of information, that makes an individual unique in a dataset and as such vulnerable to re-identification.

[158] Green, above n 135. The 'semantic web' focuses on looking to the meaning of the data as a whole, rather than particular letters or numbers.

fusion of offline and online.[159] On this basis, there can be no faith in the current definition of 'personal information' being able to cater for what is actually occurring in the big data domain.

### C. Repurposing in the dark: Principle 3 and unknown purposes

The question whether big data increases or changes the risk to privacy, is a critical one. Judging from the current landscape, it is clear the law would not be experiencing such tension with technical realities, if it were only a case of the risk being increased. We know that the problem has been transformed and the value of information no longer resides solely with its primary purpose, but in its secondary purpose.[160]

The fact that companies do not know in advance what they may discover, creates a tension in applying the Act to current big data patterns.[161] As the OECD have recognised in recent reports, personal data is increasingly used in ways unanticipated at the time of collection.[162] The legitimacy of collecting data for its own sake, as opposed to a specific future purpose, is a grey area in the current framework. By its very nature, big data entails collecting personal information with a blank purpose. This fundamentally cuts against the Act's first privacy principle which places importance on the purpose connected to the core function of the company.[163] Furthermore, the inherent 'unknowns' of big data render it difficult for companies to genuinely comply with the requirement of Principle 3, and inform the individual concerned of the purpose for which it is being collected.[164] Since the majority of innovative secondary uses have not been imagined when the data is first collected, the question arises as to how individuals can give consent to an unknown scenario.[165]

---

[159] Acquisiti, above n 32.
[160] Mayer-Schönberger and Cukier, above n 6 at 153.
[161] Carolyn Nguyen "A User-Centered Approach to the Data Dilemma" in Hildebrandt, above n 134 at 233 : New Zealand Privacy Act 1993 s 6, Principle 1.
[162] OECD, above n 103 : Cate and Mayer-Schönberger, above 134 at 3. Much of the value of personal information is not apparent at the time of collection.
[163] Paul Roth and John Edwards "Structure and Overview of the Privacy Act" in Privacy Law: Where are we now?" (New Zealand Law Society, May 2013) at 3. NZPA Principle 1(a) requires that information must be collected for a purpose connection with a function or activity of an agency. This prima facie excludes an unrelated linking of that data to a novel purpose which may still have beneficial outcomes.
[164] New Zealand Privacy Act 1993 s 6, Principle 3.
[165] This issue will be expanded upon in the following Part IV (ii)(a) analysis.

Principle 3, which requires the agency to make known to the individual the future purpose of their data collection[166] is no longer fit for purpose. This undermines the central role assigned to the data subjects under the current privacy framework. It also threatens the spirit of informational self-determination, which the German Federal Constitutional Court recognised can be crucial to the growth of society as a whole.[167] According to the Act's principles, of purpose,[168] collection[169], and reuse,[170] individuals have an opportunity to agree to lawful data collection. It is this unease over user acquiescence to unknown future use and potential data exploitation that prompts closer analysis of the interface which should govern data-sharing initiatives. This pressing issue, which cuts across fundamental contractual, privacy and informational self-determination rights, will be further explored in Part V.

## D. Towards more progressive legal tools

Having preceded the advent of personally predictable information, the Privacy Act is now showing its age.[171] Whilst we know the benefits of data-sharing are undoubtedly significant, the legal loopholes enabling companies to capitalise on the expansive nature of the exceptions, seems unjustified. Instead of playing catch-up to emerging technological capabilities, New Zealand's toolkit ought to demonstrate a more progressive approach, and lead the charge in coherent data governance.

Whilst it is important to examine the changing scope of information viewed as personally identifiable, and the repurposing inconsistency from a technical standpoint, this can mask a fundamentally normative question: whether the data should, and how the data ought to be used. In designing this toolkit and guiding principles, it will be necessary to consider which activities are socially acceptable. This process must weigh the value of data uses against potential privacy risks,

[166] New Zealand Privacy Act 1993, Principle 3(1)(a),(b). Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of the fact the information is being collected and the purpose for which the information is being collected.
[167] Mayer-Schönberger and Cukier, above n 6 at 154 : Paul de Hert "Identity Management of e-ID, privacy and security in Europe. A Human Rights view" (2008) 13(2) Informational Security Technical Report 71 at 72.
[168] New Zealand Privacy Act 1993 s 6, Principle 1.
[169] New Zealand Privacy Act 1993 s 6, Principle 3.
[170] New Zealand Privacy Act 1993 s 6, Principle 11.
[171] Christopher Kuner "The Challenge of 'Big Data' for Data Protection" (2012) 2 International Data Privacy Law 47 at 47-48.

the practicality of obtaining informed and dynamic consent, whilst keeping in mind the consequences of repurposing.[172]

It is therefore encouraging to see this issue coming to the forefront of the legislature's attention. Since the Law Commission Report's release in 2011, statements from the Minister of Justice have signalled the "need to develop new ways to achieve trust and privacy".[173] Emphasis has been placed on upcoming reforms, ensuring that the law better reflects the digital age, whilst bringing New Zealand into alignment with its major trading partners.[174] The expectation is these proposals will put stronger incentives in place to ensure the private sector takes data protection seriously.

Yet with no timeline in place for introducing amendments, little is known what form such proposals will actually take and how many recommendations will be enacted. With rounds of technical discussion prior to the amendment still forthcoming, it is critical that a retooling of privacy measures is carefully thought through. Effective legislative and regulatory action could place New Zealand at the forefront of big data stewardship and signal the country's capacity to drive data-led innovation in a principled, privacy-enhancing way. The following chapters will further develop this issue, and suggest measures New Zealand could take in this direction.

[172] Omer Tene "Symposium Issue: Privacy in the Age of Big Data: A Time for Big Decisions" (2012) 64 Stan L Rev 63 at 66.
[173] New Zealand Parliament "Judith Collins Press Statement Privacy Act Changes " (Wellington, 28 May 2014) available at <http://www.beehive.govt.nz/release/privacy-law-changes-strengthen-protection>: Cabinet for Social and Policy Committee, above n 117 at 30.3. Taking an entirely new approach would take New Zealand out of line with major trading partners in the OECD.
[174] At 10. The Privacy Commissioner made the comment that the Act must remain internationally acceptable and continue to support innovation and responsible modern business.

# PART IV

## THE REGULATORY REMEDY : A DATA STANDARDS AUTHORITY

This chapter clarifies the justification for a new body to regulate the wider uses of data and the standards that ought to govern data management. It will offer an example of an existing Standards Authority and relevant elements that the Data Standards Authority (DSA) could draw upon.[175] It describes the anticipated interface with the Privacy Act, and how an Amendment to the Act could enable this body to come to fruition. It then looks at the structure of the DSA and the possible membership, whilst also exploring the advisory role, in particular the oversight of industry-specific codes of practice. The chapter then looks at possible response mechanisms the DSA could exercise, ranging from infringement notices to pecuniary penalties. It touches on the possibility of overlaying these measures with publicity, and the prospect of compensatory and exemplary damages.

### A. The call for a new standards body

*"The time may have come to set up an independent body specifically focused on maximizing the benefits to New Zealand from data".* [176]

We should not take the PC's call for the establishment of a new body lightly. It is a powerful signal that the privacy scene has shifted, and the legislative instrument to tackle these changes needs a rethink. The Commissioner's recognition that his mandate fails to encompass 'wider uses of data' is a pertinent reminder of the danger in neglecting to account for the extending reach of personally identifiable material. Any policy response to this omission must acknowledge that the internet is a domain enmeshed in emerging forms of governance, which are still amorphous. What is needed to help cure the disjunction between the rapidly expanding data network and the laws that govern it, is immediate clarification on personal data benchmarks. There is little doubt that the digital ecosystem could benefit from a clarified framework of standards to help guide New Zealand data holders and users towards greater data responsiveness.

[175] In contrast to the NZDFF's proposal of a Data Council, this dissertation will use the terminology of a Standards Authority, to emphasize the standard-based regulatory powers which this body would possess.
[176] John Edwards, above n 113 at 3: John Edwards "Privacy and Big Data" (speech presented to Ministry of Social Development, Wellington, 2 September 2014).

The challenge is to formulate regulations that focus on responsible data stewardship. This requires devising the mechanisms that data processors can use to ensure compliance and protect individuals without having to destroy the socio-economic potential of data.[177] The regulatory solution will need to possess the capacity to breed a sound data ecology that reflects the pulse of New Zealand digital society. Within this new data environment, ethical and safety requirements will play a key role in helping form a "New Deal on Data".[178] Practical approaches will be vital in maximizing the utility of data whilst minimizing privacy risk. The flexibility of standards to guard against privacy risks whilst focusing on ethical considerations must be convincing.[179] The true test of the framework will be its sustainability in the changeable dynamic of data.

The best approach is to provide a transition point towards an international charter for Data Protection and Privacy standards.[180] This would take the form of a New Zealand-centric data standards framework, which would ensure that individuals remain protected, data processors embrace their responsibilities, and innovation is not artificially constrained.[181] Leveraging New Zealand's existing architecture and building a framework around this in an efficient regulatory manner, would be the most sustainable way to future-proof against big data challenges.[182] Although there is a case for delaying major proposed changes to the Privacy Act until the upcoming amendments of the EU Data Protection regime are made official,[183] this factor would not have to

[177] Nguyen, above n 161 at 230. The question of monetization prompts the question of whether we can develop a personal data ecosystem that allows for the trading of personal data in a way that is fair and comprehensible for individuals.
[178] Julia Lane and others (eds) Big Data, Privacy and the Public Good (Cambridge University Press, Cambridge, 2014) at ix.
[179] Carol Rose "Crystals and Mud in Property Law" (1988) 40 Stan L Rev 577 at 592-93 : Zevenbergen, above n 96 at 11.
[180] International Conference of Privacy Commissioners *Madrid Resolution: Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* (Madrid, November 2009) at 29. New Zealand was one of ten countries who proposed the Resolution for International Standards.
[181] Cate and Mayer-Schönberger, above n 134 at 15.
[182] In the same way that the Privacy Commissioner can create subordinate legislation, or Disallowable Instruments that are not legislative instruments (DINLI) through the code creation powers in Part 6 of the New Zealand Privacy Act, this body would have similar powers to create DINLI that pertain to the data standards.
[183] Assuming New Zealand wants the best chance at maintaining its 'adequacy' status and certainty with what European Standards, New Zealand commentary has been indicating major changes to the Privacy Act should wait until the EU amendments are implemented.

impact on regulatory measures that are classified as Disallowable Instruments Not Regulatory Instruments (DINRI).[184]

A heavy regulatory approach, with prescriptive provisions enshrined in legislation, would rapidly become out of date, at best becoming irrelevant, and at worst stultifying innovation and strangling development.[185] Light, technology-neutral regulation should be embraced for encouraging an environment where agility can be guided by assured benchmarks and data practices.[186] Avoiding rigidity will enable progressive responses to this area of data law that lack an "epistemological maturity".[187]According to some privacy scholars, the right architecture may be contingent on a regulatory system that is "akin to the ones we have in place regulating our food, environment and financial institutions".[188] This demands cognisance of the 'innovation and sustainability objectives', which require the regulatory solution to encompass enough neutrality to enable innovation and changes in the social and technical landscape.[189]

The European Commission's recent announcement of 'Horizon 2020' and its focus on developing common standards to facilitate the data-driven economy, indicates the increasing lean towards this regulatory strategy.[190] The European Commissioner's plan to identify sufficiently homogenous sectors, suggests New Zealand should take a similar route in creating a body to provide customised data protection. This would foster a stronger security culture, and help detect and respond to data mismanagement across sectors.[191]

The establishment of the New Zealand Data Futures Forum (NZDFF) earlier this year, demonstrates exactly the sort of thoughtful discussion of data stewardship that is necessary. Moreover, it highlights the call from the business community for more certainty to enable data experimentation

[184] Regulations Review Committee "Inquiry into the oversight of disallowable instruments that are not legislative instruments" (July 2014) I.16H <http://www.parliament.nz/resource/en-nz/50DBSCH_SCR56729_1/2dd6b5922847c918b02457adfb7e83f055a20f35> at 6. Unlike legislative instruments, these instruments as defined by s38(1)(b) of the Legislation Act 2012 provide greater scope for change and industry-specific tailoring.
[185] Isaac Ehrlich & Richard Posner "An Economic Analysis of Legal Rulemaking" (1974) 3 J Leg Stud 257 at 268 : Lyon, above n 68 at 173.
[186] Neil Gunningham "Environmental Management Systems and Community participation: Rethinking Chemical Industry Regulation" (1998) 16 UCLA J Envtl L. and Pol'y 319 at 327.
[187] Solove, above n 136 at 1872.
[188] Daniel Solove *Understanding Privacy* (Cambridge University Press, Cambridge MA, 2008) at 117.
[189] Mireille Hildebrandt "The Value of Personal Data" in Hildebrandt, above n 134 at 509 : Brill, above n 10.
[190] European Commission, above n 4 at 9.
[191] At 11.

within well-understood and navigable boundaries.[192] Innovation ironically requires certainty.[193] It is clear that the requisite innovation has already begun. We now need to regulate the exchanges of data in a meaningful way and it seems best to begin this process with standard-based architecture.

## B. Model Examples

The essence of regulation is based on controlling human behaviour by rules or restrictions to achieve certain effects in society.[194] Implementing effective data regulation therefore requires an understanding of the motives underpinning the data industry. Considering Parliament's current nod towards conferring greater powers on regulators, the call for a Data Standards Authority to take a stand within this pro-regulatory environment is a strong one.

Since regulation revolves around achieving certain societal effects, it is useful to look at the Broadcasting Standards Authority (BSA). As an Independent Crown Entity set up under the Broadcasting Act 1989 to oversee the broadcasting standards regime in New Zealand, it offers a relevant template for the DSA.[195] The independent nature of the BSA correlates with the independence of the Office of the PC that the DSA would be linked to. The DSA could be associated with the Ministry of Communications and Information Technology, reflecting the BSA being under the umbrella of the Ministry of Culture and Heritage. The alternative would be to make the body free from ministerial or governmental control, in line with the current status of the Commission.[196]

Relevant features of the BSA that could be drawn into the DSA include the provision of industry-specific codes containing standards.[197] On this basis, codes could be developed alongside industry bodies, with the opportunity for the public to provide meaningful input.[198] The target would be to

[192] New Zealand Data Futures Forum (NZDFF) *Second Discussion Paper* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/first-discussion-paper_0.pdf> at 15.
[193] At 15.
[194] Bert-Jaap Koops "Should ICT Regulation be Technology-Neutral" in Bert-Jaap Koops and others *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague: TMC Asser, 2006) at 2.
[195] New Zealand Broadcasting Act 1989.
[196] This could parallel the Privacy Commission, which is completely independent and free of government or Ministerial control.
[197] New Zealand Broadcasting Act 1989, s 22.
[198] See the reference to public comment in s 22. Considering the societal impact of big data, public engagement would be encouraged at all levels of the code formulation process.

tailor the standards to respective industries, whilst remaining true to the core data stewardship principles contained in the amending section to the Privacy Act.[199]

The most suitable enabling Act for establishing the DSA would be the Privacy Act.[200] This would entail inserting an amendment into the Act, in accordance with the Crown Entities Act, echoing the amendment to the Broadcasting Act that established the BSA in 2005.[201] It would be appropriate for this amending provision to outline the key principles of data stewardship, upon which the standards contained in the codes would be based. It would not present a radical departure from the current system but rather a reboot of the Information Privacy Principles in alignment with data protection developments that require more nuanced principles. This interface with the Privacy Act would enable the confluence of personal data issues with the structure of an established system designed to endure changes in our digital landscape.

## C. Structure of the DSA

### i. The Data Council

In line with the NZDFF's proposal of an independent data council to serve as 'guardians' of the data ecosystem, the DSA could encompass this form of strategic leadership from a mix of stakeholders. [202]

In terms of composition, the council could take its cue from recent developments in the domestic policy sphere. The inclusion of a 'Chief Technology Officer'[203] (CTO) would be a valuable addition as

[199] Privacy Commission Privacy Commission Guidance Note on Code Creation (New Zealand, June 2008) available at <http://www.privacy.org.nz/news-and-publications/guidance-notes/guidance-note-on-codes-of-practice-under-part-vi-of-the-privacy-act/ >. The purpose of the codes of practice is to increase relevance, certainty, precision and clarity.

[200] New Zealand Privacy Act 1993: Interview with John Edwards, Privacy Commissioner (Mahoney Turnbull, July 2014).

[201] New Zealand Broadcasting Act 1989, s 20 : New Zealand Crown Entities Act 2004, s 7, s 200.

[202] New Zealand Data Futures Forum (NZDFF) *Third Discussion Paper: Harnessing the economic and social power of data* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/NZDFF_harness-the-power.pdf> at 16.

[203] This concept was first incorporated in the Green Party's proposed Internet Rights and Freedoms Bill to supplement the role of the Privacy Commissioner and advise Parliament and Cabinet on the challenges and risks for New Zealand's digital ecosystem.

a neutral data arbiter.[204] The endorsement of a CTO in the NZDFF's discussion paper, bolstered by support from academics[205] and industry leaders, reinforces the value in creating this position to help identify and tackle emerging issues whilst encouraging a secure data environment.[206] In contrast to the traditional framework that tends to engender businesses working reactively on legislative action, this would enable a proactive engagement model to grow between the public and private sectors.

To supplement the role of the CTO, there is also a need for key stakeholders who already have responsibility for issues concerning data and emerging technologies, to be actively involved. The PC, Government Chief Information Officer and Chief Government Statistician, represent relevant participants in the data governance frame.[207] Membership could include a mix of industry, academic and the research communities, as well as international representatives.[208] Representation from Māori interests would be an important factor to ensure compliance with Treaty of Waitangi principles.[209] Regarding the directorship of the body, it may be most appropriate for the Chair of the DSA Council to be a respected independent individual, drawn from outside government.[210]

This Council could advise and adjudicate on interpretation of the Codes and possible improvements to them in a similar way to how the Complaints Board on the Advertising Standards Authority functions. Moreover, they could be charged with tabling an annual report to Parliament, which would flag important data trending patterns relevant to New Zealand. An example of this may be investigating the viability of 'Data Embassies' to leverage New Zealand's trusted data protection position in the international environment.[211] Providing a Trust Star quality certification system is another possible responsibility the DSA could assume.[212] This could copy the quality assurance model of the Registered Master Builders Federation to prompt companies to continue striving for, and maintaining the standards contained in the DSA codes.

---

[204] Internet Rights and Freedoms Bill available at <https://home.greens.org.nz/misc-documents/internet-rights-and-freedoms-bill>. This role has been likened to the Chief Science Advisor who is responsible for advising the

[205] Interview with Hon Michael Kirby (Mahoney Turnbull, August 5th 2014).

[206] NZDFF, above n 202 at 48.

[207] At 25.

[208] Facciano, above n 55.

[209] Legislation Advisory Committee "LAC Guidelines: Principles of the Treaty of Waitangi" <http://www.lac.org.nz/guidelines/lac-guidelines/chapter-5/>.

[210] NZDFF, above n 202 at 27.

[211] At 58. These 'Embassies', whilst legally under New Zealand territory, would be able to leverage New Zealand's trusted reputation as a data broker, and provide world-class transparency and robustness.

[212] Dutton, above n 151 at 500.

### ii. Code creation

Building upon the core principles outlined in the amending provision of the Privacy Act, the purpose of industry-specific codes would be defining best practice around data management. This would build upon the protocol already established in the Privacy Act for relevant industries to issue codes themselves.[213] Just as the Privacy Act already allows codes to be less or more stringent than the Information Privacy Principles,[214] the DSA codes could provide standards that are tailored to the particular requirements of different sectors operating in the economic and social fabric of New Zealand. Case studies of industry-led co-regulatory pursuits have consistently proven that the collaborative approach can be administratively efficient.[215] Combined with the lean towards expanded regulatory mechanisms for resolving market and enterprise related issues, New Zealand is well placed to draw upon these experiences and pursue a code-driven framework.[216]

The power of a code in "bringing out all the bits and pieces relevant for [an] industry"[217] highlights its potential to fuse together relevant law, albeit not as a formal legislative instrument.[218] Instead of imposing rules from the outside, bringing regulated parties into the code-drafting process could enhance the sense of ownership and generate less industry resistance.[219] This would result in greater industry self-policing and mutual accountability, with the added incentive of bringing potential free-riders up to the required data standards.[220] This method has been seen to fuel workable solutions that reflect a collaborative governance attitude. The inclusion of a regular review period, as demonstrated in the Broadcasting Act,[221] would also foster relevant policy and strengthen New Zealand's ability to be a global standard setting nation.[222]

In pursuing this consensus-based regulatory method, caution is needed to avoid soft data-sharing rules due to vested input from self-interested industry input.[223] The DSA would need to be aware of

[213] New Zealand Privacy Act, s 47(3).
[214] New Zealand Privacy Act, s 46(2)(a)(i).
[215] Dennis Hirsch Dutch Treat? Collaborative Dutch Privacy Regulation and Lessons it holds for US Privacy Law (Future of Privacy Forum, July 2012) at 44, 45.
[216] At 44.
[217] At 45.
[218] New Zealand Privacy Act, s 50.
[219] Hirsch, above n 215 at 81.
[220] At 24.
[221] New Zealand Broadcasting Act 1989, s 22.
[222] Hirsch, above n 212 at 92.
[223] At 81.

dubious regulatory commercial commitments that show more "public relations" impetus, than genuine precaution. To ward against this outcome, inclusion of privacy and consumer advocacy groups could be an essential component of the code-creation process. Against this threat however, a "game-changing" opportunity[224] exists for New Zealand to use 'co-regulatory' muscle in creating the new regulatory system.[225]

## D. Response Mechanism

### iii. Infringement notice regime and publicity

Taking into account the views of the PC, a more formal enforcement role would be antithetical to the tenor of the empowering Act for the DSA.[226] Considering the Commissioner's main focus is promoting and protecting individual privacy, using tools including education, [227] public statements,[228] monitoring legislation[229] and reporting to appropriate authorities,[230] it would seem apt for the DSA to also lean towards compliance through "lateral solutions".[231]

Without the ability to guarantee legal compliance, these regulatory measures will not attract sufficient industry involvement, nor address the necessary privacy standards.[232] For the codes to be persuasive, breaches should be subject to the same procedure under the current Privacy Act regime. Failure to comply with the code, even if not otherwise a breach of a data standard, would still be deemed a breach.[233] Likewise, any action concerning data management that would otherwise be a breach of a data standard, would not be deemed a breach if done so in compliance with the code.[234]

---

[224] NZDFF, above n 202 at 48.
[225] The White House *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, February 2012) at 32.
[226] Katrine Evans, Deputy Privacy Commissioner, "The Case for Exemplary Damages, Show me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475 at 476.
[227] New Zealand Privacy Act, s 13 (1) (a) and (g).
[228] At s 13 (1) (h).
[229] At s 13 (1) (f) and (o).
[230] At s 13 (1) (e) (f)(l).
[231] Evans, above n 222 at 487.
[232] Dennis Hirsch, "Achieving Global Privacy Standards through sector based codes of conduct" (2011) Ohio St L J 24 at 25.
[233] New Zealand Privacy Act 1993, s 53 (b).
[234] At s 53 (b).

For less serious breaches of the code, an appropriate mechanism would be an Infringement Notice regime. Since a legislative authority must enable such a scheme, this would be part of the amending section to the Privacy Act in accordance with the requirement for consultation with the Ministry of Justice.[235]

The recently implemented Financial Markets Conduct Act can provide useful guidance to determine the appropriate penalty for a breach.[236] The new regulatory 'toolbox' of the Financial Markets Authority offers this Infringement Notice remedy for minor compliance-type contraventions. This administratively efficient system could develop a proportionality test as more cases come to light, enabling the body to test out the nature of this penalty tool. Arbitrary statutory minimums or nominal penalties without a solid foundation would need to be avoided.[237] It would also be appropriate to have the option to challenge the order in the District Court.[238] If the infringements were particularly egregious, penalties could be justifiably in excess of $1000. This may be necessary to deter serious data management breaches where significant economic benefit results for the company engaging in such practices.[239]

Infringement notices would be able to be overlaid with publicity. This would be necessary in instances of high public interest or serious injury[240] whereby exposure of the data handler at fault is desirable. Lawrence explains that the power of mores, one of his four forces of internet architecture[241], provides a strong self-regulatory constraint for companies in their data circulation behaviour.[242] However this alone is not enough. To rely completely on reputational damage would fail to future-proof against the reality of data sharing. Accordingly, to help encourage accountability,

[235] Ministry of Justice Infringement Notice Guidelines, s 23. This scheme would need to be formulated in accordance with the Summary Proceedings Act 1957 and the Summary Regulations 1958, which provide a common framework when the District Court is requested to review or enforce an infringement offence notice.
[236] New Zealand Financial Markets Conduct Act 2013 Part 8, Subpart 5, s 513.
[237] New Zealand Commerce Act 1986, s 80 (2). In this provision the court must impose a penalty on an individual in certain circumstances.
[238] Ministry of Justice Infringement Notice Guidelines.
[239] Ministry of Justice Infringement Notice Guidelines. Consideration would need to be given to the level of harm involved in the offending, the affordability and appropriateness of the penalty for the target group, and the proportionality of the proposed fee with the infringement fees for other comparable infringement offences. The payment of an infringement fee would not be a personal admission of guilty and no criminal record established.
[240] New Zealand Broadcasting Act 1989, s 13 (1).
[241] Lawrence Lessig *Code 2.0* (Basic Books, New York, 2006) at 123. The Four Forces include law, norms, architecture and the market.
[242] John Edwards, "Exploring Privacy over the next 25 years: The Right to be Forgotten" (speech presented to Nethui Summit, Auckland, July 2014).

a 'whistleblower' regime within the DSA to reward reporting of data wrongdoing, would also be appropriate.[243] As the recent Privacy Policy Salon in Washington affirmed, there is a clear need for more nuanced sanctioning and auditing, to take data protection regulation to a new level.[244] The proposed DSA would achieve that.

### iv. (Civil) Pecuniary Penalties

For more serious breaches, the DSA would pursue civil pecuniary penalty orders. Designed to protect the public as a whole but lacking the stigma of a true criminal offence, the quasi-criminal nature of these sanctions could effectively deter poor data management. As raised in submissions to the '2013 Law Commission on Civil Pecuniary Penalties', the 'civil' label tends to disguise the criminal nature of their punishment function.[245] In determining the appropriate sum, there may be a danger in assuming corporates can afford the financial and reputational damage.[246] In a small economy like New Zealand, this would prove prejudicial. On balance however, it seems that pecuniary penalties would be a feasible measure, provided they are enacted with appropriate tact for the nature of the data breach.

[243] Bell Gully, Submission to Law Commission – Issues Paper on Civil Pecuniary Penalties (February 2013) at 5.
[244] Woodrow Hartzog and Daniel Solove "The Scope and Potential of FTC Data Protection" (2015) 83 Geo. Wash. L Rev. (forthcoming).
[245] Bell Gully, above n 243 at 6.
[246] Bell Gully, above n 243 at 7. In the case of imposing up to '10 per cent of turnover' per the Commerce Act 1986, it was noted in *Commerce Commission v Telecom* (2011) 13 TCLR 270 at [47] that the potential imposition of $279.2 million in the case of Telecom, could rightfully be rendered 'quasi-criminal' and was a substantial financial burden for a company to bear.

## E. Interface with Damages

The civil pecuniary penalty scheme would coexist with compensatory damages. The Privacy Act currently allows for the capacity to award compensatory damages against the defendant for interferences with privacy in respect of pecuniary losses, or humiliation and loss of dignity.[247]

The more contentious issue would be the interaction with possible exemplary damages. Considering the Tribunal currently lacks the jurisdiction to award exemplary damages under the Privacy Act, enabling the DSA to make such an award may be equally inappropriate, meaning there would be no immediate issue of a double jeopardy clash in compensatory outcomes.[248] However if the imminent Privacy Act changes were to incorporate this power to award exemplary damages[249] and recognise "contumelious disregard"[250] for data rights, the DSA could potentially also have this power too.[251] Although such a provision may have been inappropriate when the Privacy Act was first introduced, it is arguable that we need more proactive ways to punish data breaches.[252] Until official confirmation as to the extent to which Privacy Act reform will impact the nature of damages, the discussion on the junction of new data standards and remedies must continue.

## F. Conclusion

The case for a Data Standards Authority, located within the sphere of the Privacy Act to address current data protection issues, appears to be a strong one. The national conversation has started and New Zealand's legal landscape is ripe for regulatory action. This can be accomplished by tying it into existing systems and drawing upon templates that legitimize and give force to the concept. The structural benefits of the DSA and its industry-specific codes would be a welcome change to the current gap in clear standards on data stewardship. Provided the functioning of the DSA is founded

[247] New Zealand Privacy Act, s 82,s 83 s 88 govern the Tribunal's ability to award damages.
[248] New Zealand Privacy Act, s 88. This section makes no mention of exemplary damages, and only permits awards of liquidated damages, loss of benefit, or compensation for humiliation or injury to feelings.
[249] Bell Gully, above n 243 at 21. This concern arose as both mechanisms, Civil Pecuniary Penalties and exemplary damages, are intended to punish rather than compensate which violates the rule against double jeopardy. There are some exceptional cases which allow the court to impose both pecuniary penalties and exemplary damages in private proceedings in respect of the same conduct, such as s 82A of the Commerce Act.
[250] *Taylor v Beere* [1982] 1 NZLR 81: Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed. Brookers, Wellington, 2005) 1190.
[251] William Heath "Mydex, and restoring control over Personal Data to the Individual" in Hildebrandt, above n 141 at 255.
[252] Judith Collins, above n 173.

on valid principles that will guide data use towards beneficial outcomes, the development of New Zealand's digital landscape has potential to track a positive trajectory. Part 4 will explore these possible principles and assess the values that have most cogency in guiding the DSA.

# PART V

# PRINCIPLES TO GUIDE THE DATA STANDARDS AUTHORITY

This chapter outlines the guiding principles that would enable best data practice to develop. The principles would be reflected in the relevant industry codes, and incorporated into the amending provision of the Privacy Act. This chapter will propose two central principles that are fundamental to effective data stewardship. After highlighting the tension in strategic maximisation of data, it will assess the principle of prioritising Privacy by Design (PbyD),[253] with a focus on a de-identification protocol, as well as consumer friendly privacy settings. This will address concerns of data empowerment, and the underlying problems surrounding consent in the realm of big data. Whilst recognizing the potential emptiness of the notice and consent construct, it will explore ways that could help formulate more effective rules of engagement.

## A. The overarching aim of strategic maximisation of data

Simply stated, data minimization is at odds with the essence of big data.[254] An inherent conflict exists in the non-retention impulse mandated by the Privacy Act,[255] and the maximisation of data that the big data business model demands. Whilst this chapter cannot delve further into the complexities and possible solutions for reconciling the minimisation versus maximisation struggle, it is important to recognise the tension. Knowing this pressure exists, the question is how to strategically refine and repurpose data in the most strategic way. [256]

[253] 'PbD' refers to Privacy by Design. See Ann Cavoukian "Personal Data Ecosystem: A Privacy by Design Approach to an Individual's Pursuit of Radical Control" in Hildebrandt, above n 134 at 96. The objectives of Ontario Privacy Commissioner Ann Cavoukian's Privacy by Design method, which she developed in the '90's to address privacy needs, are to ensure privacy and personal control whilst allowing organizations to gain a competitive advantage following the seven foundational principles. 'Radical control' refers to individuals having the tools to predict the outcomes of their actions when interacting with organisations.
[254] Rubenstein, above n 6 at 5. : Tene and Polonetsky, above n 16 at 260.
[255] New Zealand Privacy Act 1993, s 6 Principle 9.
[256] Edgar Whitley "Towards Effective, consent-based Control of personal data" in Hildebrandt and others, above n 134 at 169.

In a big data world, the principle of data minimisation needs to be interpreted differently.[257] Flexible regulation is required to enable effective data reuse.[258] Scholars have proposed risk matrices that weigh the value of data against potential privacy risks.[259] Given the potential 'pollution' of stale data, there is a need for structural incentives to streamline data sets. On this basis, stimulating the market for privacy enhancing services that prompt greater engagement in judicious data maximisation should be a core focus in the regulatory solution.

## B. Principle 1: Prioritising Privacy by Design (PbyD) and a De-identification Protocol

### i. Nimble analytics and the role of the algorithmist

The "architectures of vulnerability"[260] around big data are prompting regulatory swings in the PbyD direction. By focusing the first principle on PbyD and embedding privacy in the design specifications of the data lifecycle, weaknesses can be corrected and organisations motivated to show sound data stewardship.[261]

Despite the contested futility in de-identification[262], the 'call to keyboards' is still being heard on the international stage.[263] The algorithmist's ability to create scalable 'Privacy Enhancing Technology' is crucial in formulating effective data standards.[264] This does not mean an abdication by policymakers, or DSA authority, but a recognition that algorithmists have the potential to make or break data protection protocol. In this way, PbyD moves beyond normative spheres of law and best practice, directly into emerging technology and the marketplace.

---

[257] Tene and Polonetsky, above n 16 at 260.
[258] European Commission, above n 4 at 6.
[259] Tene and Polonetsky, above n 16 at 260.
[260] Dutton, above n 151 at 19.
[261] NZDFF, above n 202 at 61.
[262] Lars Backstron "Wherefore art thou r3579x? Anonymised social networks hidden patterns, and structural steganography" (paper presented at the 16th International Conference on the World Wide Web, Canada, 2007) at 181-190.
[263] Edith Ramirez, Chair of the US Federal Trade Commission "Data Brokers: A Call for Transparency and Accountability: Opening Remarks" (speech presented to Federal Trade Commission, May 2014) :
[264] Simone Fischer-Hübner "Online Privacy - Towards Informational Self Determination on the Internet" in Hildebrandt, above n 134 at 137: European Commission, above n 4 at 7. Privacy-enhancing technologies has been defined as a "coherent system of information and communication technology measures that protect privacy without losing the functionality of the information system": Brill, above n 10. The 'algorithmist' is the individual in the company who will understand the use of algorithms and their legal and ethical implications.

'Informational self-determination' is important in preserving an individual's ability to control their personal information through 'radical control'.[265] The challenge lies in establishing protocols that are dependent on the actual and potential privacy risks, as opposed to post data breach responses.[266] By embedding such measures into the data management architecture, privacy will be the default setting.[267]

From a market-driven perspective, PbyD will grow a "vibrant marketplace for privacy-enhancing services" and further economic development.[268] Indeed, the World Economic Forum (WEF) attributes PbyD to unlocking the value of data.[269] New Zealand policymakers should demonstrate their support of the WEF's agenda and incentivise organisations to make privacy a key commercial priority.[270]

### ii. The DSA's clarification on de-identification

To the extent that careful de-identification can offer a partial solution to privacy concerns, it is critical one of the principles to focusses on transparent protocols around this process. As recognized by the NZDFF and the various submissions to their study, a gap currently exists in specifying de-identification techniques expected from organisations. Looking at the UK and Australia, it is evident that New Zealand is lagging behind in establishing clear standards for this technological process.

---

[265] Paul Schwartz "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination" (1989) 37(4) Am J Comp L 674 at 690 : David Currie, Chairman of UK Competition and Markets Authority "Big Data and UK Competition" (Speech presented in Beesley Lecture Series, 7th November 2013) available at <https://www.gov.uk/government/speeches/the-new-competition-and-markets-authority-how-will-it-promote-competition> : Ann Cavoukian "Personal Data Ecosystem (PDE) - A Privacy by Design Approach to an Individual's pursuit of Radical Control" in and others Hildebrandt and others, above n 134 at 89. Radical Control is the extent to which individuals can exercise their informational self-determination and excludes the possibility of an individual infringing another's control over their own personal information.

[266] Fischer-Hübner, above n 264 at 130.

[267] Cavoukian, above n 265 at 100.

[268] European Commission, above n 4 at 33.

[269] World Economic Forum *Unlocking the value of Personal Data: From Collection to Usage* (Geneva, 2013) available at <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf > at 4.

[270] Claudia Diaz, Omer Tene and Seda Gurses "Hero or Villian - the Data Controller in Privacy Enhancing Technologies" (2013) 74 Ohio St L J at 959 : Fischer-Hübner, above n 264 at 9.

New Zealand lacks an equivalent to the UK Information Commission Office's (ICO) disclosure considerations test, which aligns with the UK Anonymisation Network's resource for best practices in anonymisation of data sets.[271] The ICO justifies their effective de-identification protocol on the basis that a complacent approach, alongside an insufficiently rigorous risk analysis, causes inappropriate data disclosures.[272] By outlining best practice through the Anonymisation Code of Practice,[273] companies are able to strive for responsible information sharing, whilst ensuring that overprotection does not prevent the data offering real value. Providing guidance for running re-identification penetration tests also helps ensure that risks are weakened. Australia also offers its data holders a range of widely available resources to make de-identification a more meaningful process. These include their Privacy Business Resource and National Statistics Services, which offer comprehensive guidance on confidentialisation.[274]

On the contrary, New Zealand lacks a published anonymisation protocol. Statistics New Zealand currently does not offer companies seeking to follow its structure, a useable framework.[275] Accordingly, companies such as Telecom[276] have called for publicising this methodology so it can be reviewed and used by the industry. Not only would this enhance awareness of the desirable standard, it would also enable data holders to plan for dealing with re-identification. The DSA framework would benefit from taking the UK and Australian examples into account in order to de-mystify the de-identification process.

---

[271] Zevenbergen, above n 96 at 10 : European Commission *Article 29 Data Protection 05/2014 on Anonymisation Techniques* (Brussels, April 2014) at 25. The Article 29 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[272] UK ICO, above n 61. Techniques include data degrading, fading, reducing the frequency of publication, heat maps and removing the final 'octet' on IP addresses to degrade the location.

[273] UK ICO, above n 61. This outlines the Managing Data Protection Risk Code of Practice 2012 : Australia National Statistical Service "Confidentiality Information Series" <http://www.nss.gov.au/nss/home.nsf/pages/Confidentiality+-+the+obligation+to+protect+identity+and+privacy>.

[274] Office of the Australian Information Commissioner <www.oiac.gov.au>. 'Confidentialisation' refers to the process of making the data sets confidential.

[275] Statistics New Zealand <www.stats.govt.nz>. Reference is given to collapsing, aggregating, modifying values and suppressing data cells.

[276] Spark, above n 50. At the time of receiving the document from Telecom's legal team, the company had not yet changed the name to Spark.

A thorough de-identification protocol could also incorporate reference to developing techniques that work alongside de-identification such as 'differential privacy'.[277] This privacy-protecting practice would allow for utilisation of data to be salvaged which would otherwise have been suppressed under de-identification.[278] This reinforces the need for a national de-identification protocol which could progressively respond to changing methodologies and help translate the technically challenging techniques into more intuitive concepts[279] As the PC has continued to emphasise,[280] user confidence in the use of de-identified data is to a large extent determined by their belief in effective de-identification. A clarified de-identification protocol would help foster this element of trust and control and remedy the lack of current guidance.

## C. Core Problems of Data Empowerment: Rules of Engagement

### i. Issue of consent: an empty construct?

In order to propose suitable measures to foster stronger privacy standards, it is necessary to consider the issues with the current informed consent model.

In a world of big data, the reality of collection is that we have shifted to a landscape of passive generation and collection. Although the term 'authorisation' is used in the Privacy Act as opposed to 'informed consent', the PC and Tribunal have both interpreted authorisation to mean a "positive and deliberate" form signifying consent, whereby failure to object does not count as authorisation.[281] Although the need for consent is clear, it is impractical, if not impossible for users to give express

[277] Omer Tene *The Future of Privacy Forum White Paper: The Definition of Personal Data: Seeing the Complete Spectrum* (United States, 30 January 2013) at 7: UK Anonymisation Network <www.ukanon.net> : Jacques Bus and Carolyn Nguyen "Personal Data Management - A Structured Discussion" in Hildebrandt and others, above n 134 at 275.
[278] Zevenbergen, above n 96 at 201 : Ann Cavoukian *Privacy by Design: The 7 Foundational Principles* (Ontario, 2011) Privacy By Design <www.privacybydesign.ca> : Tene, above n 277 at 6. Differential privacy refers to techniques that enable extraction of useful insights about the population as a whole from a database containing personal information, while at the same time protecting the individuals from being identified in the sample.
[279] Zevenbergen, above n 96 at 38. This emphasizes the inherent limitations in the addition of noise to the data, which leaks information where positive correlations exist.
[280] Edwards, above n 176 at 4.
[281] European Commission, above n 114 at 6.

consent with respect to all collected data.[282] Big data thrives on surprising correlations that call into question laws that rely on traditional ideas of notice and consent.[283]

The current framework for information on data sharing practices available for companies is unrealistic and murky. The backdrop for this arrangement is increasingly complex, as data flows are channelled through dense networks of platforms and applications. Back-handling or 'downstream' agreements[284] obscure this environment, which is aggravated by the opacity of decisional criteria. The first hurdle is the expectation that organisations can effectively explain their data processing activities on progressively smaller screens via increasingly smarter devices. The next hurdle is obtaining permission from often-uninterested individuals, whereby they are expected to understand complicated privacy disclosures and somehow express 'informed' consent.[285]

The current model of stating purposes and obtaining data processing consent at the outset, highlights an important fault line between law and technology, and the redundancy of the traditional paradigm.[286] Indeed, the unknown factors in data repurposing require a workable framework to help alleviate the artificial nature of the consent model.

### ii. Information asymmetries + poor understanding = lack of engagement

The emptiness of the construct not only fails to create an ineffective contractual relationship between the parties, but also establishes an unacceptable power imbalance. Whilst the data holder is given a relatively free hand to smuggle in subversive terms, the data subject is offered a haze of complicated policy statements.[287] This form of 'engineered' consent, where an illusion of free choice

[282] See chapter 2 C, 'Repurposing in the Dark: Principle 3 and unknown purposes'.
[283] Paul Ohm "General Principles for Data Use and Analysis" in Lane and others (eds) *Privacy Big Data and the Public Good* (Cambridge University Press, Cambridge, 2014) at 100.
[284] Tene, above n 16 at 261.
[285] Aleecia McDonald and Lorrie Cranor "The Cost of Reading Privacy Policies" (2008) 17(1) J L & Policy for Info Society 540 at 3. This study found that to read every privacy policy encountered, an average individual would need to spend approximately 30 working days per year.
[286] Tene, above n 16 at 271: Cate and Mayer-Schönberger, above n 134 at 14 : Helen Nissenbaum and Solon Barocas "Big Data's End Run around Anonymity and Consent in Julia Lane and others, above n 283 at 60.
[287] Mindy Chen-Wishart "Contract Law and Uncertain Terms" (Staff Seminar given to University of Otago Law Faculty, 25 July 2014).

is proffered, plays to the hands of cognitive biases, which produce suboptimal results.[288] Behavioural studies have demonstrated the skewed nature of subjective utility, upon which the data subjects' decisions are based.[289] This is cogently illustrated by a recent performance art experiment where individuals gave away highly granular personal data in return for a facebook biscuit.[290] The immediate experiential gains from 'free services' in contrast to the temporal distance of privacy losses, casts a shadow on the authenticity of privacy choices.[291]

Informational asymmetry is a critical issue, and when linked with intelligibility obstacles, creates an inadequately engaged data subject. Genuine informed consent has been rendered essentially impossible, due to the complicated fine print which deters users and creates social pressure to not appear awkward or confrontational.[292] Decoding vague, elastic terms about reuse that enables "improvement of customer experience" is not productive.[293] The participation deficiency stems from an overriding sense that users are "in the dark" and disabled from transparency and active engagement.[294]

Yet in terms of combatting information asymmetries, the tide is starting to turn. The establishment of New Zealand's Broadband Product Disclosure Code illustrates the drive to combat the 'fog of ignorance' that can enable unethical use.[295] This self-regulatory code, which outlines and compares broadband offerings to customers, could be used as a model to translate to the area of data

[288] Jason Millar "A Problem for Predictive Data Mining" in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, Toronto, 2005) at 110.
[289] Christopher Parsons "Putting the Meaningful into Consent" (16 October 2010) Technology, Thoughts & Trinkets <http://www.christopher-parsons.com/references-for-putting-the-meaningful-into-meaningful-consent/>.
[290] Rob Waugh "People are willing to trade private data for pistachio cookie" (2 October 2014) We Live Security <http://www.welivesecurity.com/2014/10/02/people-willing-trade-private-data-pistachio-cookies/>.
[291] Tene, above n 16 at 261 : Joseph Turow and others "The Federal Trade Commission and Consumer Privacy in the Coming Decade" 3(3) J L & Policy for Info and Soc'y (2007) 723 at 724.
[292] Chen-Wishart, above n 287.
[293] European Commission, above n 4 at 34. This refers to the recent French Consumers Group which launched legal action against three of the largest social networks, criticising them of confusing 'elliptique et pléthorique' contractual terms: Alina Tugend "Those Wordy Contracts We All So Quickly Accept" The New York Times (online edition, New York, 12 July 2013) <www.nytimes.com> : Apple Mavericks Privacy and Terms of Service (September 2 2014). This policy was accessed by the author when downloading the latest OS X (10.9.4). This policy was at least half the length of this dissertation and offered an easy way to skip reading the policy and proceed to the "I agree" phase.
[294] Yannis Bakos, Florencia Marotta-Wurgler and David Trossen *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts* (CELS 4th Annual Conference on Empirical Legal Studies Paper, 2009) : Brill, above n 10.
[295] World Economic Forum, above n 67 at 7.

protection.[296] However the fact still remains that merely forcing data controllers to notify users of the risks they are taking, could not only overwhelm them, but fail to nudge individuals into privacy-enhancing behaviours.[297]

Users may not read or understand notices about the impact of profiling, especially given the novelty, complexity and obscurity of this trend.[298] The empirical research in this field highlights how consumers remain "largely oblivious to their rights" and seldom opt in or out of privacy policies, regardless of their merits.[299] Myopia, created by a lack of knowledge, fuels this trend.[300] The concerning corollary is that users either do not understand the *quid quo pro* exchange when data is collected, or they hold inaccurate beliefs about privacy protections.

An alarming threat to user empowerment is the inconsistency between poorly optimised privacy enhancing tools by the 'privacy vulnerable', alongside the rejection of information-intensive material by 'privacy pragmatists'.[301] Yet the inefficient utilisation of privacy policies should not necessarily be rendered a market failure.[302] As privacy advocate Aquisiti asserts, offering transparent policies to users is "like bringing a knife to a gunfight".[303] To create the 'super consumer' who can capitalise on their privacy statement,[304] we must therefore look beyond conventional modes of warning, and aim for more meaningful information symmetry.

It is clear the issue of consent needs to be tackled in order to foster more effective engagement. The dangerous duo of unintelligibility and information asymmetry breeds a culture of disempowered data subjects. The DSA principles and industry-specific codes would aim to confront this situation and help advance a different business model around user-centricity. This cannot be enforced unequivocally, but must be managed though granular regulatory measures. This will aim to take

[296] New Zealand Telecommunications Forum *Broadband Product Code* (Wellington, 23 October 2013) available at <http://www.tcf.org.nz/library/d2225da1-d8b2-4e8e-8308-d025091fa2ac.cmr>.
[297] Ctrl-Shift "Mapping the Market for Personal Data Management Services" (20 March 2014) <https://www.ctrl-shift.co.uk/home/?CSRF_TOKEN=46c5c5922f666be1ab43e205168a86c64e51ec60>.
[298] Hildebrandt, above n 189 at 248.
[299] Rubenstein, above n 6 at 8 : Nissenbaum and Barocas, above n 286 at 59.
[300] Jennifer Urban and Chris Hoofnagle *The Privacy Pragmatic as Privacy Vulnerable* (Berkeley School of Law, CA, 2014) at 4. This refers to the rational choice theory explanation that it is simply not worth the consumer's time to learn about privacy issue. Following this line of reasoning, privacy becomes a less marketable value.
[301] At 3 : Alan Westin (ed) *Harris Interactive Privacy On and Off the Internet: What Consumers Want* (New York, February 2002) available at <http://www.ijsselsteijn.nl/slides/Harris.pdf> at 20.
[302] Adam Theirer "Pursuit of Privacy in a world where Information Control is Failing" (2013) 36(2) Harv J L & Pub Pol'y 410 at 446.
[303] Acquisiti, above n 32.
[304] Westin, above n 301 at 29.

account of the technical and behavioural factors underlying the interaction between data holders and data subjects.

## D. Principle Two: Data Holders must create consumer friendly privacy settings

*"We need a new commercial order in which data subjects are emancipated from systems built to control them and become free and independent agents in the marketplace.*[305] *- Doc Searls*

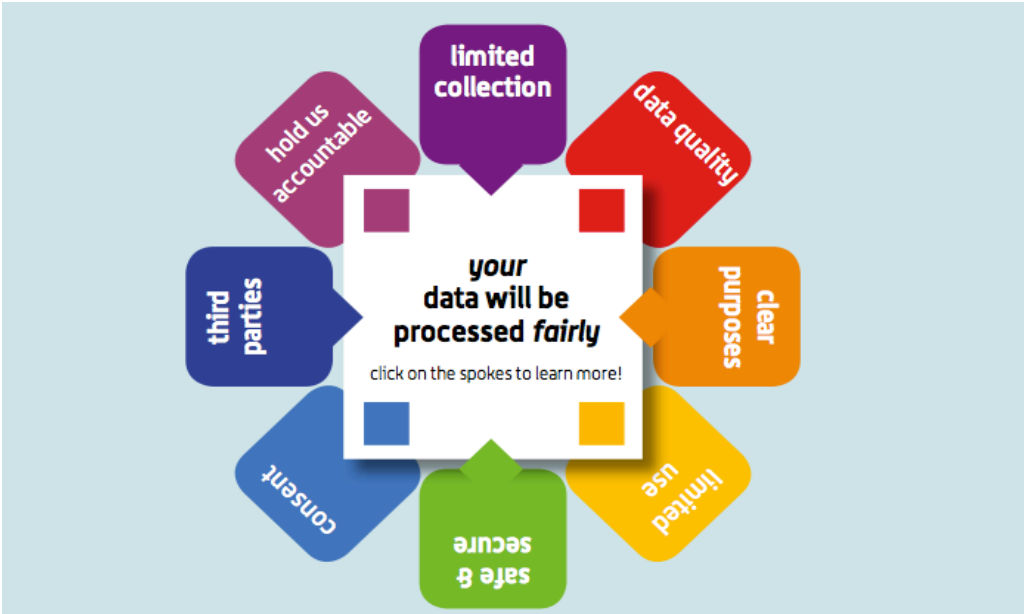
A second principle to guide the DSA is the creation of consumer friendly privacy settings. This requirement would aim to bridge the gap between ineffective command style privacy interfaces and a more desirable form of user engagement. The pivot point for this regulatory ecosystem must hinge on the concept of 'user-centricity'. [306] Opportunities do exist for liberating individuals from 'antihuman' systems that treat users as mere gadgets.[307] Provided there is a genuine shift towards a more humanised paradigm where the user becomes the nucleus in the ecosystem, then the goal of creating more consumer-friendly privacy policies may be within reach.

### i. Visualised interface: The medium is the message

This principle requires a critical examination and rethink of how privacy statements are presented to users. The aesthetic of the interface has the power to enhance or disrupt the efficacy of data stewardship. The data standards could require a minimum use of infographics within the privacy statement which organisations must comply with. Alternatively they could develop a standardised pictogram that becomes a mandatory part of the privacy policy presented to the user. If the medium is the message[308] and the medium is ill-fitting, it is little wonder that messages around data protection are slipping through the digital crevices of the web.

---

[305] Doc Searls "The Intention Economy: When Customers Take Charge" (Harvard Business Review Press, Boston, 2012) at 1: Ctrl-Shift "The New Personal Data Landscape" (22 November 2011) <www.ctrl-shift.co.uk>.
[306] Rubenstein, above n 6 at 9.
[307] Jaron Lanier "You are not a Gadget: An apocalypse of self-abdication" (Knopf, New York, 2010) at 26 : Ann Cavoukian, above n 264 at 90 : Ctrl-Shift, above n 305.
[308] Marshall McLuhan "Understanding Media: The Extensions of Man" (McGraw-Hill, New York, 1964) at 7.




This wheel was developed by Dutch researchers, based on a survey of what European citizens wanted to know about companies' data processing practices. It is based on the OECD Fair Information Principles. Users can click on the spokes of the wheel to get more information about each element.

From Bibi van den Berg and Simone van der Hof: "What happens to my data? A novel approach to informing users of data processing practices", 2012.

Privacy scholars have created images such as The Dutch Wheel to attack the issue of user detachment.[309] The endorsement of this infographic by the NZDFF signals the progression towards more visually stimulating privacy policies. The use of a similar motif to the clickable wheel, with spokes representing elements of the data relationship, could make privacy settings more consumer-friendly. Another example of interactive interfaces can be seen in the Biobanking[310] sector, where the same challenges are being faced in making sure that technical concepts are communicated and consent is meaningful.[311] Biometric data also suffers from the challenge of indeterminable future uses and a temporal distance to the individual's privacy loss. Drawing on these relevant international experiments will therefore be valuable for New Zealand's progress towards improved consumer friendly interfaces.

In finding a harmonious balance of visual and text, it is important to bear in mind the core requirement of natural language. Recent legislative changes, such as the Financial Markets Conduct Act, provide useful guidance for creating understandable interfaces. In light of the Capital Market

[309] Bibi van den Berg and Simone van der Hof "What happens to my data? A novel approach to informing users of data processing practices" (2012) 7(7) First Monday at 2.
[310] Biobanking refers to the storing of biological samples for use in future research.
[311] Whitley, above n 256 at 172 : Neil Manson and Onora O'Neill *Rethinking Informed Consent in Bioethics* (New York, Cambridge University Press, 2012) at 73.

Development Taskforce's critique of disclosure statements not being sufficiently concise, the new requirements call for word limits, concise language and the use of diagrams.[312] From a regulatory standpoint, there is also value in drawing upon the recent New Zealand 'Privacy Guidelines for App Developers'.[313] The condition in the guidelines to provide a graphical privacy dashboard, reflects the value placed on making privacy come alive. The Fair Trading Act's recent alterations similarly reinforce the focus on improved legibility and presentation.[314] These relevant legislative changes represent valuable domestic models for the DSA to take its cue from.

On this basis, privacy pictograms have the potential to enhance user experience.[315] Support from the EU Article 29 Working Party reinforces the confidence in icons capturing comprehensive information.[316] Provided the New Zealand standard avoids over-simplifying to the point that users are not truly informed and lull users into a false sense of security,[317] the stage is set for an improved interface. Although internationalising privacy symbols may be a challenge, there is scope for domestic variation around standardized key privacy concepts.[318] The aim of the DSA ought to be to create a tool that avoids exclusive use of either text or visualisations, but allows a fusion of the two.

### ii. Informed consent

A core facet of the final principle concerning user-centricity is the ability to meaningfully 'inform' the data subject.[319] To achieve this, there needs to be a shift towards conceptualising consent in a self-determinative way. The mandate to provide privacy information to users in a form that clarifies

[312] Financial Markets Authority *A Guide to the Financial Markets Conduct Act 2013 Reforms* (Wellington, 2013) at 12.
[313] New Zealand Office of the Privacy Commissioner Guidance Note for App Developers 5 Point Checklist (Wellington, 24 July 2014) at 1. These guidelines were issued following regulators from the Global Privacy Enforcement Network conducting a sweep on mobile apps earlier this year.
[314] New Zealand Fair Trading Act 1986, Subpart 3 s 36U (1) (a) (ii), (iii), (iv). The disclosure requirements relating to extended warranties agreements must be in plain language, legible and clearly presented.
[315] 'UX' is the industry term for 'user interface'.
[316] European Commission *Article 29 Working Party Opinion 10/2004 on More Information Provisions WP 100 11987/04/EN* (2004) at 8.
[317] Lorrie Cranor and others "User interfaces for privacy agents" (2006) 13(2) ACM Transactions on Computer–Human Interaction 135 at 137. See <www.privacybird.org>. Developed by W3C, Privacy Bird is a plug–in for Internet Explorer which, through the use of a small bird which dynamically changes colour depending on the (mis)match between a user's personal privacy settings and the Web site's privacy policy.
[318] Madrid Resolution, above n 180 at 31.
[319] Nissenbaum and Barocas, above n 286 at 59.

the nature of the data capture, reuse and downstream sharing is becoming increasingly critical.[320] In recognising that informed consent may no longer be a match for the challenges posed by big data, the DSA measures should be more than just operationally-focused.[321] In pursuing this objective, we ought to transcend the notion that 'shedding sunlight' on personal data arrangements is adequate, and instead strive towards ensuring the user's 'ammunition' is more fitting for what Aquisiti hails the 'data gunfight'.[322]

It is absurd to believe that notice and consent can fully specify the terms of data interactions in the face of unpredictable data challenges and opportunities. In lieu of radically abandoning consent as a core privacy concept, the DSA could instead promote informed consent that spotlights on the purposes of data practices, and how these behave with ethical, political and context-driven interests.[323] On this basis, it would be prudent for the second sub category of informed consent to be rooted in the idea of contextual integrity.[324] In accordance with the industry-specific codes, this concept frames privacy solutions according to contextual circumstances.[325] By contextualising consent, the DSA could bring the background of rights, obligations and legitimate expectations into focus so that notice and consent "can do the work for which it is best suited".[326]

One way in which informed and contextually-driven consent could display more granularity is through sliding scales.[327] In this respect, how the data is protected needs to be weighted against the sensitivity of the information collected. For the privacy settings to capture the texture of data stewardship, the decisional criteria behind data management choices also ought to be elucidated, including perhaps the disclosure of algorithms.[328] Greater exposure of how decisions are weighed

[320] Simone Fischer-Hübner "Online Privacy - Towards Informational Self-Determination on the Internet" in Hildebrandt, above n 134 at 134.
[321] Nissenbaum and Barocas, above n 286 at 63. The distinction between operationalising informed consent and informed consent itself ought to be recognised.
[322] Rubenstein, above n 6 at 8 : Acquisiti, above n 32.
[323] Nissenbaum and Barocas, above n 286 at 67.
[324] Helen Nissenbaum *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, California, 2009) at 129.
[325] Ohm, above n 283 at 103. Ohm refers to Helen Nissenbaum's concept of contextual integrity, specifically regarding the study of cities, and framing privacy problems in appropriately sized contexts as opposed to broader privacy solutions.
[326] Nissenbaum and Barocas, above n 286 at 66. : Carolyn Nguyen, above n 161 at 231.
[327] Paul Ohm, above n 283 at 105.
[328] Fischer-Hübner, above n 320 at 133.

would help users gain trust in the entities they interact with, and greater insight into the variables that influence data-sharing.[329]

Achieving true informed consent also requires evaluation of downstream sharing agreements. The challenges posed by the chain of data stakeholders involved in the data enterprise, make this an important practice to bring to the attention of users.[330] Delving further into this issue prompts the question of when the data controller's obligation to inform should end. Should the duty to provide 'informed consent' be rendered complete in terms of the data that is explicitly recorded? Or should the data controller adopt a more encompassing approach, explaining what further information the organisation may glean? There appears to be a strong case for arguing that consent should not only cover the information that can be directly derived from it, but also information from sophisticated analysis, including aggregation with other contextual or personal data.

In response to the trend towards increased downstream sharing, the Privacy Commission recently released privacy policy Guidelines for App Developers.[331] The guidelines place emphasis on integrating privacy from day one, which entails raising awareness of whether the data is being 'funnelled' to downstream third parties.[332] Whilst recognising the correlations between app developers, users and data miners, the announcement of these standards foreshadows the potential extension of the privacy benchmarks beyond the app domain, to wider instances of data collection and manipulation.

By implementing measures that increase understanding of sharing, users can attain greater informational self-awareness. By providing users with guidance on the implications of their data decisions, the ecosystem will accord more with the first principle's focus on PbyD.[333] It is only when users are properly informed of the risks of their participation in the lifecycle of big data, can they achieve a true sense of the ultimate aim of user centricity.

---

[329] Nguyen, above n 161 at 231.
[330] Nissenbaum and Barocas, above n 286 at 60.
[331] Kate Fay "Fitness Apps Can Help You Shred Calories and Privacy" (May 2014) Adage <www.adage.com>.Recent studies by the US Federal Trade Commission reveal the extent of downstream sharing, with the sample study of 12 health and fitness apps disseminating personal data with 76 third parties.
[332] New Zealand Office of the Privacy Commissioner, above n 313.
[333] Jennifer Golbeck "The Curly Fry Conundrum: Why Social Media 'likes' Say More than You Might Think" (podcast, October 2013) TEDtalk <https://www.ted.com/playlists/56/making_sense_of_too_much_data>.

### iii. Live consent

A final feature of Principle 2 that will help foster a culture of user-centricity is the aspect of 'living informed consent'.[334] Identified as a key strategy by privacy commentators and industry bodies, the submission from Spark to the NZDFF also highlights the need for dynamic privacy.[335] Rethinking privacy settings towards creating a living conversation between data holder and data subject, re-envisions the traditional notion of rigid preferences. As emphasised in the preceding section, accessible consent is crucial, and a dynamic process would place the user at the heart of the data protection matrix. It is vital for the DSA to recognise the value of a more intuitive process, so the DSA standards can sway the stakeholders involved.

To respond to the need for consent measures that value the dynamic pace at which data is being 'upcycled' and disseminated, the DSA ought to focus on the preference functions around personal data. Although data rights ultimately reside with the individuals, data subjects do not practically own their data and in most cases cannot prevent the processing of it.[336] Since the real objective of data protection measures is to protect against unjustified interventions in personal life, offering the right protective choices to the user is critical. Various options exist for ways that consent could be tendered to the data subjects in less static forms.

Firstly, it is plausible for coverall consent to be offered at the beginning of the data stewardship process.[337] Advocates for consent regimes of this genre challenge the prioritisation of active permissions, arguing that the value in live consent is overstated. The contention from data evangelists is that more data being used in unrestricted ways will always be beneficial, if only for reasons to be determined at a later date.[338] Privacy scholar Omer Tene argues an over-emphasis on consent may stifle innovation, and that neglecting to solicit consent actually results in more positive

[334] Greenwood and others "The New Deal on Data: A framework for Institutional Controls" in Lane and others, above n 178 at 201.
[335] Spark, above n 52 at 8.
[336] Gutwirth and others, in Hildebrandt and others, above n 134 at 2 : NZDFF, above n 202 at 68. This point is exemplified by the 2014 Terms and Conditions that state users do not generally own their content and grant substantial latitude to Linkedin to commercialize their data now or in the future, without any further consent, notice or compensation. See Appendix 1 for the Terms and Conditions. Until online platforms that enable data trading from a consumer perspective become more mainstream, users are disempowered from gaining stronger ownership rights over their data.
[337] Whitley, above n 256 at 172.
[338] Diaz and others, above n 270 at 959.

outcomes for all parties involved.[339] He cites examples such as Facebook's proactive News Feed Feature launch, and Google's 'wardriving'[340] to map out Wi-fi networks as evidence of this. In the case of Google's geo-location orientated exploits, had they provided the choice for users to opt their routers out of the wardriving campaign, it is doubtful that many would have done so, considering the recognised value of Google's data use.[341] These cases highlight the potentially regressive effect of consent-based processing, which may ultimately result in less utility for data users.

Nonetheless the coverall approach has been condemned as excessive. Requiring data subjects to be 'stuck' with the initial choices would fly in the face of a living dialogue and emasculate the concept of informed consent.[342] This wholesale attitude diminishes the value of informed consent because it requires notice that fails to delimit future uses of data and its possible consequences.

Conversely, live consent would enable users to engage in real time through privacy triggers, an element that the NZDFF focused on in their final recommendations paper.[343] This system could use appropriate notification standards from the recent New Zealand App Guidelines. For instance, if a user wanted to change privacy settings themselves, they should be provided with information regarding who will be able to view their data after the change.[344] Since the timing of notification is also critical, icon-based notifications to indicate when vital attributes like geo-location data is being mined, could be useful. This is currently being explored through the 'VRM Project' at Harvard's Berkman Centre for Internet and Society. This project is pursuing a vision where an individual is in "complete control of her digital persona and grants permissions for vendors to access it on her own terms without vendor lock in".[345] This echoes the NZDFFs aim of more fine-grained control over personal profiles to achieve mutual gain in data exchanges. Striking the balance between open and active communication channels, and respect for an appropriate level of distance in the data relationship is challenging, and cuts to the core of achieving live consent.

---

[339] Tene and Polonetsky, above n 16 at 262.
[340] "Wardriving" refers to the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant.
[341] Kevin O'Brien "Google Allows Wi-Fi Owners to Opt Out of Database" New York Times (online ed, New York, 15 November 2011) <http://www.nytimes.com/2011/11/16/technology/google-allows-wi-fi-owners-to-opt-out-of-database.html>.
[342] Mayer-Schönberger and Cukier, above n 6 at 154.
[343] NZDFF, above n 202 at 20.
[344] Privacy Commission App Guidelines, above n 313.
[345] Tene, above n 16 at 266.

Given the possibility that consent-based data acquisitions may not have been fully 'informed', updated prompts seem desirable. Looking at models of consent in the health sector, the Ministry of Health 'Guidelines on the Use of Human Tissue for Future Unspecified Purposes' provides useful insight into promising methods.[346] The option to "recontact the donor in order to gain further consent" is indicative of the 'living consent' approach. This mode of consent, combined with providing practical insights in real time, is a suitable cross-industry impulse for the DSA to draw upon.[347] Just as the guidelines offer indications about the nature of research carried out on tissue samples and implications for the donor, the live consent standards imposed by the DSA could require data holders to be notified on a similar basis. Empowering the user to know the types of proactive upcycling from the beginning could lead towards a more informed user base.

In response to concerns surrounding the intrusiveness of a live notification-based consent model, opt-out options must also be explored. To avoid initial bad bargains having long-term consequences, users should be able to retract consent and halt future use of their data at any point they feel is appropriate. Although we may presume the ability to opt-in and out is a reality, the harsh truth is that most privacy policies operate on a model of endurance. Apple's approach to the use of their Operating Systems (OS) is one relevant example. In response to the latest Mavericks OS 10.9.4 offering, users are presented with the option of termination, upon which the license becomes redundant. However the express limitation enabling downstream sharing to survive such termination, allows Apple to ensure that the dissemination of user's data is a permanent one.[348] This kind of agreement highlights the current artificiality of consent to data-sharing. Moreover it reaffirms how genuine consent is being constrained by the mainstream acceptance of wholly submitting to these less than desirable privacy policies.

It is against this backdrop that the NZDFF have recommended bolstering the right to opt-out. There is an obvious need for more clarity surrounding consent arrangements. The NZDFF suggests incorporating the right to opt-out in standard terms and conditions for consent to data services. While there are technical limitations to this, opting out could also be accompanied by 'best-efforts provisions' to delete all the relevant data.[349] Whilst it is not in the ambit of this dissertation to

[346] Ministry of Health Guidelines on the Use of Human Tissue for Future Unspecified Purposes (Ministry of Health, Wellington, March 2007) at 9.
[347] NZDFF, above n 202 at 6.
[348] Apple Mavericks, above n 293.
[349] NZDFF, above n 202 at 71.

investigate the related issue of the 'Right to be Forgotten', this is a pertinent question that warrants serious discussion regarding its impact on information privacy law.

### iv. Conclusion

The degree to which consumer friendly privacy settings can prevail as the norm which data holders must abide by, depends to a large extent on the self-awareness of users. Once appropriate standards are in place, the responsibility is on users to maximise the dynamic interface that has the capacity to stimulate a living dialogue. Companies can extensively visualise, clarify and inform users, but if the data subject remains disengaged, then consumer friendly privacy settings will fail to get traction. For consent to be truly 'live', the continuing conversation must be valued. Like any fruitful relationship, this requires active listening to ascertain what each stakeholder wants out of the data exchange. Thus, the new guidelines must be founded on user-centric principles that balance regulatory certainty with flexibility so the dynamism of data can be accounted for.

# PART VII

## CONCLUSION

*"In God we trust. All others must bring data."* [350]

Big data has come. And it is trampling all over privacy law. The nuanced ways in which data analytics operate and the vigour with which the technological landscape is changing, presents a unique time in societal development. In grappling with the question of how data can operate for us, and not upon us, this dissertation set out to explore how to shift New Zealand's privacy landscape towards more progressive legal tools.

The regulation around data stewardship is critical. This is evidenced by the national conversation which has already begun. Discussion papers from the NZDFF and the PC are offering support for changes in the data protection sphere. This dissertation has identified a fresh regulatory framework. With this body in mind, New Zealand's ability to navigate the information industry through relevant privacy protections is more assured. In light of the current power imbalances between data holders and users, a Data Standards Authority could be truly valued. This body would be well placed to provide a baseline of best practices for data stewards and downstream 'upcyclers', whilst offering robust accountability measures to encourage organisations to engage in a more responsible and responsive data-use ecosystem.

Paying heed to the notion that "cyberspace has no intrinsic nature. It is as it is designed,"[351] the strategy for overcoming the inadequacies of New Zealand's data protection law has focused on the formulation of guiding principles. I have suggested several that the proposed amendment to the Privacy Act could encompass, and which would lay the groundwork for the formulation of industry-specific codes. These not only stress the operational side of data protection and effective PbyD techniques, but also the behaviour-driven elements concerning user empowerment and engagement models. New Zealand need not only rely on regulatory reform to achieve its data protection goals. It can, and should, take advantage of emerging business models in which firms decide to empower consumers and enhance individual control over personal data.

[350] Hastie and others *The Elements of Statistical Learning* (2nd ed, Springer, New York, 2009) at vii.
[351] Lessig, above n 241 at 317.

We would be wise to avoid a tragedy of the data commons,[352] in which individualistic and exploitative pursuits by data holders override and deplete the potential value of the data resource. Not only would this be contrary to individual privacy rights and the orientation of data protection towards providing transparency, it would also be contrary to the long-term interests of society. There is little doubt that data is a highly strategic asset that has the power to be the new engine of our increasingly digitalised economy.

The cultural commentator McLuhan recognised that "we shape our tools, and our tools shape us".[353] Careful carving of this privacy toolkit, and close attention to the form our privacy messages take, will enable a sharper, more robust data ecosystem. The chosen tools to govern personal data will have a profound impact on New Zealand's capacity to be a world leader in delivering a trusted digital environment where the big data benefits can be realised. Big data can be harnessed to serve the public good. The only limitation will be deciding to what extent we want our digital future to be guided by an ever-changing petabyte-driven compass.

[352] Jane Yakowtiz "Tragedy of the Data Commons" (2011) 25(2) Harvard J L & Tech at 4.
[353] McLuhan, above n 308 at xi.

Appendix 1

License and warranty for user submissions to LinkedIn

"You still own what you own, but you grant us a license to the content and/or information you provide us. As between you and LinkedIn, you own the content and information you provide LinkedIn under this Agreement, and may request its deletion at any time, unless you have shared information or content with others and they have not deleted it, or it was copied or stored by other users. Additionally, you grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including, but not limited to, any user generated content, ideas, concepts, techniques and/or data to the services you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties".

# PART VII
# BIBLIOGRAPHY

## LEGISLATION & BILLS

New Zealand Bill of Rights Act 1990.

New Zealand Broadcasting Act 1989.

New Zealand Commerce Act 1986.

New Zealand Crown Entities Act 2004.

New Zealand Fair Trading Act 1986.

New Zealand Financial Markets Conduct Act 2013.

New Zealand Human Rights Act 1993.

New Zealand Legislation Act 2012.

New Zealand Privacy Act 1993.

Summary Proceedings Act 1957.

## CASES

### *NEW ZEALAND*

*R v Jefferies* [1994] 1 NZLR 290 (CA).

*Taylor v Beere* [1982] 1 NZLR 81.

*Commerce Commission v Telecom* (2011) 13 TCLR 270.

## BOOKS & CHAPTERS IN BOOKS

Colin Bennett and Christopher Parsons "Privacy and Surveillance" in William Dutton *The Oxford Handbook of Internet Studies* (Oxford University Press, Oxford, 2013).

Jeremy Bentham *Panopticon; Or, The Inspection-House: Containing The Idea of a New Principle of Construction applicable to any Sort of Establishment, in which Persons of any Description are to be kept under Inspection: And in Particular To Penitentiary-Houses, Prisons, Houses of Industry, Workhouses, Poor*

*Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals, And Schools: With a Plan Of Management adapted to the principle: in a series of letters, written in the year 1787, from Crecheff in White Russia* (T Payne, London, 1791).

Ian Brown *Regulating Code* (MIT Press, Cambridge, 2013).

Jacques Bus and Carolyn Nguyen "Personal Data Management - A Structured Discussion" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Lee Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002).

Ann Cavoukian "Personal Data Ecosystem (PDE) - A Privacy by Design Approach to an Individual's pursuit of Radical Control" in Hildebrandt and others *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Noam Chomsky *Manufacturing Consent: The Political Economy of the Mass Media* (Pantheon, New York, 1988).

Ronald Deibert and Rafal Rohozinski "Beyond Denial" in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds) *Access Controlled, The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MIT Press, 2010).

Usama Fayyad and others (eds)*Advances in Knowledge Discovery and Data Mining* (MIT Press, Cambridge, 1996) at 37 as cited in Tal Zarsky "Mine your own! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion" (2003) 5 Yale J L & Tech 2.

Simone Fischer-Hübner "Online Privacy - Towards Informational Self Determination on the Internet" in Mireille Hildebrandt, Kieren O'Hara and Micahel Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Lisa Gitelman (ed) *Raw Data is an Oxymoron* (MIT Press, Cambridge, 2013).

Trevor Hastie and others *The Elements of Statistical Learning* (2nd ed, Springer, New York, 2009).
Heath William "Mydex, and restoring control over Personal Data to the Individual" in Mireille Hildebrandt, Kieren O'Hara and Micahel Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Mirielle Hildebrandt "The Value of Personal Data" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Mirielle Hildebrandt "Who is Profiling Who?" in Gutwirth and others (eds) *Reinventing Data Protection* (Springer, Amsterdam, 2009).

Aldous Huxley *Brave New World* (Harper Collins, New York, 2000).

Bert-Jaap Koops "Should ICT Regulation be Technology-Neutral" in Bert-Jaap Koops and others *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (TMC Asser, The Hague, 2006).

Julia Lane and others (eds) *Privacy, Big Data and the Public Good* (Cambridge University Press, Cambridge, 2014).

Jaron Lanier *You are not a Gadget: An apocalypse of self-abdication* (Knopf, New York, 2010).
Lawrence Lessig *Code 2.0* (Basic Books, New York, 2006).

David Lyon *The Surveillance Society* (Open University Press, Philadelphia, 2001).
Manson Neil and Onora O'Neill *Rethinking Informed Consent in Bioethics* (New York, Cambridge University Press, 2012).

Viktor Mayer-Schonberger and Kenneth Cukier *Big Data: A Revolution That Will Transform the Way We Live, Work and Think* (1st ed, Eamon Dolan, New York, 2013).

Marshall McLuhan *Understanding Media: The Extensions of Man* (McGraw-Hill, New York, 1964).

Jason Millar "A Problem for Predictive Data Mining" in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, Toronto, 2005).

Carolyn Nguyen "A User-Centered Approach to the Data Dilemma" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Helen Nissenbaum and Solon Barocas "Big Data's End Run around Anonymity and Consent in Julia Lane and others (eds) *Privacy, Big Data and the Public Good* (Cambridge University Press, Cambridge, 2014).

Helen Nissenbaum *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, California, 2009).

Doc Searls *The Intention Economy: When Customers Take Charge* (Harvard Business Review Press, Boston, 2012).

Daniel Solove *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, New York, 2006).

Daniel Solove *Understanding Privacy* (Cambridge University Press, Cambridge MA, 2008) at 117.

Bernard Stiegler "Die Aufklärung in the Age of Philosophical Engineering" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook* (IOS Press, Amsterdam, 2013).

Nassim Taleb *Antifragile: Things that Gain from Disorder* (Penguin Books, New York, 2012).

Stephen Todd (ed) *The Law of Torts in New Zealand* (4 ed. Brookers, Wellington, 2005) 1190-1200.

Sive Vaidhyanathan *The Googlization of Everything (And Why We Should Worry)* (University of California Press, Berkeley, 2011).

## JOURNAL ARTICLES

Arnold Bruce Baer "Ending the OIAC and new frameworks for privacy law" (2014) 11(5) Privacy Law Bulletin 66.

Ryan Calo "Digital Market Manipulation" Geo Wash L Rev (2014) (forthcoming).

Lorrie Cranor and others "User interfaces for privacy agents" (2006) 13(2) ACM Journal of Transactions on Computer–Human Interaction 135.

Claudia Diaz, Omer Tene and Seda Gurses "Hero or Villian - the Data Controller in Privacy Enhancing Technologies" (2013) 74 Ohio St L J.

Isaace Ehrlich and Richard Posner "An Economic Analysis of Legal Rulemaking" (1974) 3 J Leg Stud 257.

Katrine Evans, Deputy Privacy Commissioner, "The Case for Exemplary Damages, Show me the Money: Remedies under the Privacy Act" (2005) 36 VUWLR 475.

Neil Gunningham "Environmental Management Systems and Community participation: Rethinking Chemical Industry Regulation" (1998) 16 UCLA J Envtl L and Pol'y 319.

Paul de Hert "Identity Management of e-ID, privacy and security in Europe. A Human Rights view" (2008) 13(2) Informational Security Technical Report 71.

Dennis Hirsch "Achieving Global Privacy Standards through sector based codes of conduct" (2011) Ohio St L J 24.

Michael Kirby "Legal Aspects of Transborder Data Flows" (1991) 11(3) Computer L J 233.

Christopher Kuner "The Challenge of 'Big Data' for Data Protection" (2012) 2 International Data Privacy Law 47.

Aleecia McDonald and Lorrie Cranor "The Cost of Reading Privacy Policies" (2008) 17(1) J L & Policy for Info Society 540.

Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701.

Paul Ohm "The Underwhelming Benefits of Big Data" (2013) 161 U PA L Rev Online 339.

Jules Polonetsky and Omer Tene "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11(5) Nw J Tech & Intell Prop 239.

Carol Rose "Crystals and Mud in Property Law" (1988) 40 Stan L Rev 577.

Ira Rubenstein “Big Data - The End of Privacy or a New Beginning?” 2013 3(2) International Data Privacy Law 74.

Ira Rubenstein, Ronald Lee and Paul Schwartz “Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches” (2008) U Chicago L Rev 261.

Paul Schwartz “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination” (1989) 37(4) Am J Comp L 674.

Paul Schwartz and Daniel Solove “The PII Problem: Privacy and a New Concept of Personally Identifiable Information” (2011) NYU L Q Rev 1814.

Daniel Solove “A Taxonomy of Privacy” (2006) 154 Penn St L Rev 477.

Omer Tene “Symposium Issue: Privacy in the Age of Big Data: A Time for Big Decisions” (2012) 64 Stan L Rev 63.

Joseph Turow et al “The Federal Trade Commission and Consumer Privacy in the Coming Decade” (2007) 3(3) J L & Policy for Info and Soc’y 723.

Fan Wei and Albert Bifet “Mining Big Data: Current Status, and Forecast to the Future” (2012) 14 ACM at 9.

Tal Zarsky “Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society” (2004) 56(13) Me L Rev.

## PARLIAMENTARY & GOVERNMENTAL MATERIALS

Cabinet Social Policy Committee “Government Response to Law Commission Report: Review of the Privacy Act” (12 March 2012) SOC Min (12) 3/1.

Financial Markets Authority *A Guide to the Financial Markets Conduct Act 2013 Reforms* (Wellington, 2013).

Legislation Advisory Committee “LAC Guidelines: Principles of the Treaty of Waitangi” <http://www.lac.org.nz/guidelines/lac-guidelines/chapter-5/>.

Ministry of Health Guidelines on the Use of Human Tissue for Future Unspecified Purposes (Ministry of Health, Wellington, March 2007).

Ministry of Justice Infringement Notice Guidelines available at <http://www.justice.govt.nz/publications/global-publications/i/infringement-guidelines/guidelines-for-new-infringement-schemes>.

New Zealand Law Commission “Questions and Answers to the Law Commission Review 2011” (Wellington, August 2011) available at

<http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/questions_and_answers_-_for_report_release.pdf>.

New Zealand Law Commission "Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 Issues Paper" (Wellington, 2010).

New Zealand Office of the Privacy Commissioner Guidance Note for App Developers 5 Point Checklist (Wellington, 24 July, 2014).

New Zealand Telecommunications Forum *Broadband Product Code* (Wellington, 23 October 2013) available at <http://www.tcf.org.nz/library/d2225da1-d8b2-4e8e-8308-d025091fa2ac.cmr>.

Regulations Review Committee "Inquiry into the oversight of disallowable instruments that are not legislative instruments" (July 2014) I.16H <http://www.parliament.nz/resource/en-nz/50DBSCH_SCR56729_1/2dd6b5922847c918b02457adfb7e83f055a20f35>.

Privacy Commission Privacy Commission Guidance Note on Code Creation (New Zealand, June 2008) available at <http://www.privacy.org.nz/news-and-publications/guidance-notes/guidance-note-on-codes-of-practice-under-part-vi-of-the-privacy-act/ >.

## REPORTS

### *NEW ZEALAND*

Bell Gully Submission to Law Commission - Issues Paper on Civil Pecuniary Penalties (February 2013).

Joy Liddicoat *Association for Progressive Communications New Zealand Digital Freedoms Report* (Wellington, 2014) available at <https://www.apc.org/en/irhr/i-freedom-nz/about>.

New Zealand Data Futures Forum (NZDFF) *Full Discussion Paper* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/first-discussion-paper_0.pdf>.

New Zealand Data Futures Forum (NZDFF) *Second Discussion Paper* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/first-discussion-paper_0.pdf>.

New Zealand Data Futures Forum (NZDFF) *Third Discussion Paper: Harnessing the economic and social power of data* (New Zealand, 2014) available at <https://www.nzdatafutures.org.nz/sites/default/files/NZDFF_harness-the-power.pdf>.

Statistics New Zealand The Digital Divide (Wellington, 2013) available at <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/digital-divide/introduction.aspx>.

*INTERNATIONAL*

Yannis Bakos, Florencia Marotta-Wurgler and David Trossen *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts* (CELS 4th Annual Conference on Empirical Legal Studies Paper, 2009).

Fred Cate and Viktor Mayer-Schönberger *Notice and Consent in a World of Big Data: Global Privacy Summit Report and Outcomes* (Washington, 2012).

Ann Cavoukian and Daniel Castro *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (Information and Privacy Commissioner, Ontario, 2014) <www.itif.org/2014-big-data-deidentifaction.pdff>.

Ann Cavoukian and El Emam *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (Ontario, June 2014) available at <http://www2.itif.org/2014-big-data-deidentification.pdf>.

Cisco *Cisco Visual Networking Index: Global Mobile Data Traffic forecast Update 2012-2017* (Cisco, 2013) available at <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf>.

Committee on the Elimination of Racial Discrimination *CERD Report on New Zealand* CERD/C/NZL/CO/17 (2007).

Barbara Daskala and Ionnis Maghiros *Digital Territories : Towards the Protection of Public and Private Space in a Digital and Ambient Intelligence Environment* (Institute for Prospective Technological Studies, Seville, 2007).

European Commission *Article 29 Data Protection Working Party Opinion 05/2014 on Anonymisation Techniques* (Brussels, April 2014).

European Commission *Article 29 Working Party Opinion 10/2004 on More Harmonised Information Provisions* WP 100 11987/04/EN (Brussels, October 2004).

European Commission *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Region: Towards a Thriving Data Driven Economy* (Brussels, July 2014) available at<http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6216>.

European Commission *Directorate of General Justice Opinion 11/2011 on the level of protection of personal data in New Zealand* (Brussels, 2011) available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf#h2-13>.

European Commission *Privacy and Competitiveness in the Age of Big Data: the interplay between data protection, competition law and consumer protection in the Digital Economy* (Brussels, March 2014).

Executive Office of the President *Podesta Report: Big Data: Seizing Opportunities, Preserving Values* (Washington, May 1 2014) available at <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf>.

International Conference of Privacy Commissioners *Madrid Resolution: Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* (Madrid, November 2009).

McKinsey Global Institute *Big Data: The New Frontier for Innovation, Competition and Productivity* (1 May 2011) available at <http://www.mckinsey.com/client_service/telecommunications/latest_thinking>.

OECD *OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data* (Geneva, 1980) available at <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

OECD *Thirty Years After: The OECD Privacy Guidelines* (OECD, 2011) available at <http://www.oecd.org/sti/ieconomy/49710223.pdfAddress>.

Price Waterhouse Coopers *PWC Big Data: Big Benefits and Imperilled Privacy* (United States, June 2014).

Omer Tene *The Future of Privacy Forum White Paper: The Definition of Personal Data: Seeing the Complete Spectrum* (United States, 30 January 2013).

The White House *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, February 2012).

United Kingdom Office of the Information Commissioner *Big Data and Data Protection* (London, July 2014) <http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf>.

United Kingdom Information Commissioner's Office *Data Protection Technical Guidance Determining What is Personal Data* (2007) <http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx>.

Jennifer Urban and Chris Hoofnagle *The Privacy Pragmatic as Privacy Vulnerable* (Berkeley School of Law, CA, 2014).

Alan Westin (ed) *Harris Interactive Privacy On and Off the Internet: What Consumers Want* (New York, February 2002) available at <http://www.ijsselsteijn.nl/slides/Harris.pdf>.

World Economic Forum *Rethinking Personal Data* (Geneva, May 2014) available at < http://reports.weforum.org/rethinking-personal-data/>.

World Economic Forum *Unlocking the value of Personal Data: From Collection to Usage* (Geneva, 2013) available at <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf>.

Bendert Zevenbergen *Ethical Privacy Guidelines for Mobile Connectivity Measurements* (Oxford Internet Institute, 2013).

## NEWSPAPER & MAGAZINE ARTICLES

Charles Duhigg "How Companies Learn Your Secrets" *The New York Times* (online edition, New York, 16 February 2012).

Tom Fox-Brewster "Londoners give up eldest children in public Wi-Fi security horror show" (29 September 2014) *The Guardian* <http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>.

Quentin Hardy "Rethinking privacy in an Era of Big Data" *The New York Times* (4 June 2012) available at <http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?_php=true&_type=blogs&_r=0>.

Ian Katz "Tim Berners-Lee: demand your data from Google and Facebook" *The Guardian* (online ed, London, 18 April 2012) <http://www.theguardian.com/technology/2012/apr/18/tim-berners-lee-google-facebook>.

Andrew McAfee "Big Data: The Management Revolution" *Harvard Business Review* (online ed, Boston, December 2012).

Kevin O'Brien "Google Allows Wi-Fi Owners to Opt Out of Database" *The New York Times* (online ed, New York, 15 November 2011) <http://www.nytimes.com/2011/11/16/technology/google-allows-wi-fi-owners-to-opt-out-of-database.html>.

Alexandra Suich "Special Report Advertising and Technology: Getting to Know You" *The Economist* (September 13th 2014).

Alina Tugend "Those Wordy Contracts We All So Quickly Accept" *The New York Times* (online edition, New York, 12 July 2013) <www.nytimes.com>.

## INTERNET MATERIALS

Australia National Statistical Service "Confidentiality Information Series" <http://www.nss.gov.au/nss/home.nsf/pages/Confidentiality+-+the+obligation+to+protect+identity+and+privacy>.

Ann Cavoukian "Privacy by Design: The 7 Foundational Principles" (Ontario, 2011) Privacy by Design <www.privacybydesign.ca>.

Andrew Couts "Senator Promises Bill to Block Invasive Employer Facebook Checks" Digital Trends (23 March 2012) <http://www.digitaltrends.com/social-media/senator-promises-bill-to-block-invasive-employer-facebook-checks/>.

Ctrl-Shift “Mapping the Market for Personal Data Management Services” (20 March 2014) <https://www.ctrl-shift.co.uk/home/?CSRF_TOKEN=46c5c5922f666be1ab43e205168a86c64e51ec60>.

Ctrl-Shift “The New Personal Data Landscape” (22 November 2011) <www.ctrl-shift.co.uk>.

EU Data Protection Law “EU Data Protection Regulation Timeline” (13 May 2014). <www.eudataprotectionlaw.com>.

Facebook <http://www.facebook.com/help/promotee>.

Kate Fay “Fitness Apps Can Help You Shred Calories and Privacy” (May 2014) Adage <www.adage.com>.
Fitbit “The Fitbit Story” <http://www.fitbit.com/nz/story>.

Andy Green “Personally Identifiable Information Hides in Dark Data (13 April 2013) Varonis <http://blog.varonis.com/personally-identifiable-information-hides-in-dark-data/>.

Green Party Internet Rights and Freedoms Bill available at <https://home.greens.org.nz/misc-documents/internet-rights-and-freedoms-bill>.

Larry Hardesty “Algorithm recovers speech from vibrations of potato-chip bag filmed through soundproof glass”(August 4, 2014) Phys.org <http://phys.org/news/2014-08-algorithm-recovers-speech-vibrations-potato-chip.html>.

Hunton Williams “Privacy Law Update” (podcast, 16 September 2014) <www.hunton.com/media/20140916_privacy/20140916_privacyupdate2_Mono2.mp3>.

Thorin Klosowski “How Websites Vary prices Based on your Information (and what you can do about it)” LifeHacker (July 2013) <http://lifehacker.com/5973689/how-web-sites-vary-prices-based-on-your-information-and-what-you-can-do-about-it>.

Dr Kathleen Kuehn “Media Technologies and Surveillance” (Victoria University of Wellington, 2014) available at <http://www.victoria.ac.nz/seftms/about/news#a248532>.

Eric Markowitz “Meet a Startup with a Big Data Approach to Hiring” (September 2013) INC <www.inc.com/eric-markowitz>.

Richard Metzger “Facebook: I want my friends back” Dangerous Minds (24 October 2012) <www.dangerousminds.net>.

New Zealand Office of the Privacy Commissioner “NZ Data Protection gets tick from EU Committee” (13 April 2011) <http://privacy.org.nz/news-and-publications/statements-media-releases/nz-data-protection-law-gets-tick-from-eu-committee/>.

New Zealand Parliament “Judith Collins Press Statement Privacy Act Changes ” Beehive (Wellington, 28 May 2014) available at <http://www.beehive.govt.nz/release/privacy-law-changes-strengthen-protection>.

Office of the Australian Information Commissioner <www.oiac.gov.au>.

Drew Olanoff “Google wants to serve you ads based on the background noise on your phone calls” (21 March 2014) The Next Web <http://thenextweb.com/google/2012/03/21/google-wants-to-serve-you-ads-based-on-the-background-noise-of-your-phone-calls/>.

Christopher Parsons “Putting the Meaningful into Consent” (16 October 2010) Technology, Thoughts & Trinkets <http://www.christopher-parsons.com/references-for-putting-the-meaningful-into-meaningful-consent/>.

Pruhealth “Vitality Health Programmes” <http://www.pruhealth.co.uk/>.

Sensing Cities “Project to Create Sensing Cities Launches in Christchurch” (4 September 2014) Sensing City <http://www.sensingcity.org/stay-informed/project-to-create-%E2%80%98sensing-cities%E2%80%99-launches-in-christchurch>.

Statistics New Zealand “The Digital Divide” (Wellington, 2013) <www.stats.govt.nz>.

Omer Tene “Privacy: For the Rich or for the Poor?” (July 26 2012) Concurring Opinions <http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html>.

Alice Truoing “How Google searches can predict the next stock market crash” (July 24 2014) Fast Tech Company <http://www.fastcompany.com/3033661/fast-feed/how-google-searches-can-predict-the-next-stock-market-crash>.

United Kingdom Anonymisation Network <www.ukanon.net>.

United Kingdom Department for Business Innovation and Skills “Plans for World Class Research Centre in the UK” (United Kingdom Government, 19 March 2014) available at <https://www.gov.uk/government/news/plans-for-world-class-research-centre-in-the-uk>.

Rob Waugh “People are willing to trade private data for pistachio cookie” (2 October 2014) We Live Security <http://www.welivesecurity.com/2014/10/02/people-willing-trade-private-data-pistachio-cookies/>.

## INTERVIEWS

Interview with Dele Atanda, founder of the Universal Declaration of Digital Rights and Digitterra (Mahoney Turnbull, 30 July 2014).

Interview with Cyrus Facciano, General Manager Qrious (Mahoney Turnbull, July 25th 2014)

Interview with Hon Michael Kirby (Mahoney Turnbull, August 5th 2014).

Interview with Vikram Kumar, Chief Executive Internet Party (Mahoney Turnbull, 25 April, 2014).

Interview with Paul Roth, University of Otago Law Professor (Mahoney Turnbull, 7 August, 2014).

Interview with John Steadman, Legal counsel at Spark (Mahoney Turnbull, 8 July 2014).

## PRESENTATIONS

Alessandro Acquisiti "Why Privacy Matters" (podcast, October 18 2013) TEDtalks <http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters>.

Jonathan Boston "A New Global Climate Change Treaty – Can Humanity Deliver? Our Challenge after Durban for 2015" (paper presented at University of Otago, Dunedin, 14 March 2012).

Julie Brill, United States Federal Trade Commissioner, "Reclaim your name" (speech presented at NYU Sloan Lecture Series: Privacy in the World of Big Data, NYU, October 2013) available at <http://engineering.nyu.edu/sloanseries/reclaim-your-name.php>.

Mindy Chen-Wishart "Contract Law and Uncertain Terms" (Staff Seminar given to University of Otago Law Faculty, 25 July 2014).

David Currie, Chairman of UK Competition and Markets Authority "Big Data and UK Competition" (Speech presented in Beesley Lecture Series, 7th November 2013) available at <https://www.gov.uk/government/speeches/the-new-competition-and-markets-authority-how-will-it-promote-competition>.

John Edwards, New Zealand Privacy Commissioner "Exploring Privacy over the next 25 years: The Right to be Forgotten" (speech presented to New Zealand Nethui Summit, Auckland, July 2014).

John Edwards, New Zealand Privacy Commissioner "New Zealand's Data Future: A View from the Privacy Commissioner" (Wellington, 4 July).

John Edwards, New Zealand Privacy Commissioner "Privacy and Big Data" (speech presented to Ministry of Social Development, Wellington, 2 September 2014).

Jan Eliasson, Deputy Security General "Remarks on a Data Revolution for Sustainable Development" (Speech presented to the United Nations Independent Expert Advisory Group for Big Data, 24 September 2014) available at <http://www.undatarevolution.org/2014/09/26/deputy-secretary-generals-data-revolution/>.

Juan Enriquez "How to think about digital tattoos" (podcast, December 2012) TedTalks <https://www.ted.com/talks/juan_enriquez_how_to_think_about_digital_tattoos>.

Ian Fletcher Director Government Communications Security Bureau "Privacy and Security: Identity, society and the state in the internet age" (speech presented at NZ Privacy Forum Week, Wellington, 7 May 2014).

Jennifer Golbeck "The Curly Fry Conundrum: Why Social Media 'likes' Say More than You Might Think" (podcast, October 2013) TEDtalks <https://www.ted.com/playlists/56/making_sense_of_too_much_data>.

Edith Ramirez, Chair of the US Federal Trade Commission "Data Brokers: A Call for Transparency and Accountability: Opening Remarks" (speech presented to Federal Trade Commission, May 2014).

Viviane Reding, Vice Commissioner European Commission "Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" (speech presented to the Digital Age Innovation Conference, DLD Munich, January 2012) available at <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm>.

Bruce Schneier, Chief Security Technology Officer, British Telecom "Privacy in the Age of Big Data" (speech presented to the New Zealand Privacy Forum, Wellington, May 2012) available at <https://www.youtube.com/watch?v=L_UIdkbp3xo>.

## MISCELLANEOUS

Apple Mavericks Privacy and Terms of Service (2 September 2014).
Lars Backstron "Wherefore art thou r3579x? Anonymised social networks hidden patterns, and structural steganography" (paper presented at the 16th International Conference on the World Wide Web, Canada, 2007).

Email from Mia Garlick, Head of Policy, Facebook Australia and New Zealand to Mahoney Turnbull regarding data governance structures (8 August 2014).

Spark (Arvind Narayanan and Edward Felten "No silver bullet: De-Identification Still Doesn't Work" (unpublished manuscript, Princeton University, 2014).

Spark "Submission to the New Zealand Data Futures Forum" (Wellington, July 2014).

Interview with Swannanoa Primary School Principle (Guyon Espiner, Morning Report, National Radio, 31 July 2014).