REGULATING TO SUPPORT PRIVACY DISCLOSURES

The First Step Towards Avoiding an Internet of Things Dystopia

Matthias Schorer

A dissertation submitted in partial fulfilment of the degree of Bachelor of Laws (Honours) University of Otago – Te Whare Wananga o Otago

October 2018

"You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized."

George Orwell, *1984* (1949)

TABLE OF CONTENTS

PREFACE

When future historians analyse the technological developments of the late 20th, and 21st centuries, they will undoubtedly define them as transformative – a revolution. However, as with all revolutions, whether it is defined as good or bad will depend on what is transformed, and the nature of those transformations. I believe this idea must be kept in the forefront of our minds as we continue to invite technology to transform our environment; and that is the idea that has inspired this dissertation.

To my supervisor, Associate Professor Colin Gavaghan, thank you for your guidance, feedback, and enthusiasm for my topic.

To my family, and especially my parents, thank you for your endless love, support, and encouragement.

To my friends, thanks for the good times. Olivia, a special thank you for your valuable insights. And Mitch, cheers for being a solid Junior Counsel both inside and outside the Moot Court.

REGULATING TO SUPPORT PRIVACY DISCLOSURES

Introduction

Imagine coming home and having the room automatically adjust to your ideal temperature; or, being told by your fridge what is in it and what you can make for dinner with those ingredients. Imagine feeling an unusual tightness in your chest but being reassured by your watch that it is just the flu and being told the best way to treat it, or alternatively, that you need to go to hospital immediately. These are the promises of convenience, efficiency, and enlightenment offered by a world where the Internet of Things (**IoT**) is mainstream – a world where every object you interact with is connected to the internet, with the ability "to raise awareness of some everyday circumstance to the network for analysis and response".[1]

But there is also a dark side to this hyperconnected future. Because we will interact with these objects when performing our most analogue functions, they will collect more granular information about us than other consumer facing technologies historically have. This has the potential to make us more transparent than ever before. There is evidence to show people are extremely concerned about losing control over their personal information in this environment, however, evidence also shows people are behaving in an increasingly reckless manner when disclosing personal information. People rarely make the effort to understand how their personal information can be used in the future, and rarely attempt to protect it from undesirable future uses.[2]

In a world where the IoT is mainstream this reckless oversharing of personal information will be set on a collision course with mass surveillance, and I believe this will be detrimental to individuals and society. My thesis is that

[1] Adam Greenfield *Radical Technologies* (Verso, London, 2017) at 32.

[2] Nina Gerber, Paul Gerber and Melanie Volkamer "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour" (2018) 77 Computers & Security Journal 226.

people do not want to disclose their personal information in such a potentially damaging way, but they need help to change their behaviour, which the law is currently failing to provide. The law must adapt to provide an environment where individuals are empowered to make more prudent disclosures of their personal information. I make that case through three chapters.

Chapter one describes the IoT in more detail and why, despite having nothing to hide, there are still serious consequences for an individual who discloses personal information without restricting its future use in a world where the IoT is mainstream. I also consider some worst-case scenarios for society generally.

In chapter two I consider why individuals currently disclose their personal information without restricting its future use, despite an overwhelming concern for informational privacy; and, how the law fails to provide the support individuals need to make disclosures consistent with their privacy concerns.

Finally, chapter three proposes a regulatory solution that aims to support the ability of individuals to make privacy disclosures that are consistent with their privacy concerns. First, I suggest a range of amendments to the Privacy Act 1993 that would provide protection to users of the IoT at the margins of the collector/discloser relationship, and nudge producers of IoT objects to design their technologies in ways that make it easier for disclosers to properly consider their privacy concerns at the moment of disclosure. Second, I suggest the establishment of a specialist body charged with making privacy enhancing design more accessible to technology producers.

This dissertation is not intended to be the final say on how the law should prepare for the mainstreaming of the IoT. It is not even intended to be the final say on how to fix the privacy disclosure attitudes of individuals. However, it is intended to raise awareness of the fact this is the first step towards avoiding an internet of things dystopia, and to be the beginning of the discussion as to how we should be making that step.

Chapter I: *An Internet of Things Dystopia*

A. 2022

1. The Internet of Things

The term "internet of things" was coined by Kevin Ashton in 1999.[3] When Ashton was working as a brand manager for Procter & Gamble in 1998, he was frustrated by the fact that one of his most popular products was frequently out of stock in regional shops. The problem was store workers were terrible at manually discerning when products needed to be re-ordered, in what quantity, and how often that needed to happen. Thus, in a powerpoint presentation titled "The Internet of Things", Ashton pitched the idea of learning how to automatically record how those products interacted with the supply chain.[4] Rather than manually putting information into computer databases, he had a vision "to empower computers with their own means of gathering information, so they [could] see, hear and smell the world for themselves, in all its random glory".[5]

Fast-forward 19 years; Ashton's ambition is no longer science fiction, but a present reality.[6] Wearable technologies such as Fitbit and the Apple Watch track the number of steps taken each day, distance walked, calories burned, quality of sleep, heart rate, perspiration, and skin temperature.[7] The Nest thermostat tracks motion in a room, ambient light, room temperature, and humidity to set temperatures more efficiently.[8] Products that connect to a user's car can monitor that car's health and its user's driving habits.[9]

---

[3] Kevin Ashton "That 'Internet of Things' Thing" *RFID Journal* (online ed, Melville, 22 June 2009) as cited in Irene C.L. Ng and Susan Y.L. Wakenshaw "The Internet-of-Things: Review and research directions"(2017) 34(1) IJRM 3 at 4.

[4] Jane Bainbridge "Meet Kevin Ashton, the man behind the internet of things" *Campaign* (online ed, London, 29 April 2014).

[5] Ashton, above n 3.

[6] For a comprehensive discussion of the different objects populating the IoT today, see Scott R. Peppet "Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent" (2014) 93(1) Tex L Rev 85 at 98 - 117.

[7] Peppet, above n 6, at 101.

[8] Peppet, above n 6, at 108.

[9] Peppet, above n 6, at 105.

Electricity meters can record home energy use patterns.[10] A UVeBand will monitor exposure to ultraviolet rays and notify its users if they need to reapply sunscreen.[11] A MimoBaby "onesie" shirt will monitor a baby's sleep habits, temperature and breathing patterns.[12] The list goes on: there are ovens, refrigerators, door locks, beds, sex toys, and even internet-connected vibrating underwear, "which monitor Twitter for brand mentions and shoutouts – giving you a very special feeling each time one hits".[13] From the useful, to the quirky, and the just plain weird the world is now full of connected objects that record and communicate information in a pervasive and autonomous fashion.

The IoT is not a reference to any of the aforementioned technologies in isolation. Rather, the IoT is the network of all objects connected to the internet, collecting information, locating other devices on the network, and communicating information to them and us without the direct control of people.[14] Mike Kuniavasky, an early proponent of the IoT, characterises its vision as the state of being in which "computerisation and data communication [are] embedded in, and distributed through, our entire environment".[15]

2. *A race to connect*

The scope of the IoT is increasing drastically. In 2013, the Organisation for Economic Co-operation and Development (**OECD**) estimated 2.5 devices per person were connected to the internet in people's homes. However, by

---

[10] Peppet, above n 6, at 109.

[11] UVeBand <http://www.uveband.co.uk/>.

[12] Mimo < https://www.mimobaby.com/>.

[13] Woodrow Hartzog *Privacy's Blueprint* (Harvard University Press, Massachusetts, 2018) at 260.

[14] See Ng and Wakenshaw "The Internet-of-Things: Review and research directions" above n 3; Gaochao Xu and others "Research on the Internet of Things (IoT)" (2013) 160(12) Sensors & Transducers 463; Afzal A Zaidi Sar and others "The Cognitive Internet of Things: A Unified Perspective" (2015) 20(1) Mobile Networks and Applications 72.

[15] Mike Kuniavsky *Smart Things: Ubiquitous Computing User Experience Design* (Elsevier, 2010) as cited in Greenfield, above n 1, at 31.

2022 they expect that number to grow to 12.5 devices per person.[16] Conservative estimates suggest that over 50 billion connected sensor devices will be in use by 2020,[17] offering better efficiency, more convenience, and a superior understanding of our environment through the quantification of previously immeasurable qualities.

Enabling this growth has been consistent increases in technologies' capabilities, together with consistent decreases in the costs of technology production.[18] The growth in technological capability coupled with a commensurate decrease in production costs has made it cheaper for consumers to welcome IoT products into their lives, realise the benefits associated with digitising their daily functions, and demand more internet connected products.

But it is not just consumers who are driving growth in the IoT industry. A somewhat more innocuous driver of growth has been the incentive to supply IoT products because of the value that can be generated from the personal information they collect.[19] Data is increasingly being seen by market participants as having a value comparable to money.[20] In fact, the market for data is becoming so strong that the Economist has proclaimed it to be the world's most valuable resource.[21] Companies can use data to be more efficient, by isolating cost saving opportunities; to enhance existing business

---

[16] Rudolf Van der Berg "Smart Networks: Coming Soon to a Home Near You" (21 January 2013) OECD Insights <http://oecdinsights.org/2013/01/21/smart-networks-coming-soon-to-a-home-near-you/>.

[17] Dave Evans *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything* (CISCO, April 2011) at 3.

[18] Oren Smilansky "Companies gear up for the IoT revolution: there's rising consumer demand for – and acceptance of – connected devices" (2015) 19(3) CRM Magazine 18; Alexander Wolfe "Little MEMS Sensors Make Big Data Sing" *Forbes Magazine* (online ed, New York, 10 June 2013); Shahid Ahmed "Digital Revolution Summit: The Six Forces Driving the Internet of Things" PWC <https://www.pwc.com/gx/en/technology/pdf/six-forces-driving-iot.pdf>.

[19] Albert Opher and others "The rise of the data economy and monetization" IBM < https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12367USEN>.

[20] Directive COM/2015/0634 on certain aspects concerning contracts for the supply of digital content, article (1) recital 13.

[21] "The world's most valuable resource is no longer oil but data" *The Economist* (online ed, London, 6 May 2017).

streams, through better understanding consumers and the market; to create new business streams, by identifying previously unseen opportunities; and to monetise data itself, by selling it to other businesses for the aforementioned three purposes.[22] Today, some of the biggest companies in the world are built around monetising personal data. For example, Facebook's revenue for the quarter ended 31 March 2018 was almost USD 12 billion, 98.6 percent of which was advertising revenue.[23] While Facebook is a 'free' social networking service, it is also the world's largest targeted advertising business, thanks to its personal data mine consisting of over two billion Facebook users.[24]

The growing market for data has incentivised creating businesses for the predominant purpose of collecting as much personal information as possible, and the IoT is perfectly positioned for such exploitation. Take the Amazon Dash Button, a product designed to re-order any assigned product from Amazon at the click of a button. The cost of the materials is almost certainly such that Amazon makes a loss on each $5 unit sold,[25] especially considering the full rebate offered after making a single purchase.[26] However, the data Amazon receives regarding the time and place of your need, as well as its frequency and intensity, has value that can be exploited to justify a small upfront loss.[27]

I am not suggesting all IoT products are designed to exploit personal information over user utility in the first instance. However, the incentive for producers to collect personal information provides an insight into the potential development of the IoT. First, the IoT is only going to keep

---

[22] Capgemini *Big & Fast data: The Rise of Insight-Driven Business* (Capgemini, 10 March 2015) at 8.

[23] Facebook "Facebook Reports First Quarter 2018 Results" (press release, 15 April 2018).

[24] Kathleen Chaykowski "Mark Zuckaberg: 2 Billion Users Means Facebook's 'Responsibility Is Expanding' *Forbes Magazine* (online ed, New York, 27 June 2017).

[25] Greenfield, above n 1, at 46.

[26] Amazon "Amazon Dash Button" Amazon < https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011>.

[27] Greenfield, above n 1, at 37.

proliferating and become more widespread. By 2020 it will not just be the rich who have beds, door locks, and thermostats connected to the internet for their own novelty. IoT products will become cheaper and more accessible to everyone because the value of personal information is capable of subsidising the upfront costs of a product, just like we have seen with Facebook and the Amazon Dash Button. Even products that do not have obvious consumer justifications for connectivity may become connected by default, so that more comprehensive consumer profiles can be built.

Second, when this happens, and we are walking around in a world full of connected objects, we will be haemorrhaging data – but we will not be the only ones who benefit from mopping it up.[28] Worryingly, there is very little someone else cannot do with another's personal data once they have possession of it. With endless opportunities to extract value from data, it is almost inevitable that companies will attempt to do so to the full extent their privacy policies permit. Fortunately for these companies, privacy policies are not much of an obstacle in this endeavour. Only one in four Europeans read terms and conditions in full when buying or signing up to products and services online.[29] Similarly, in Australia the proportion of people who always or often read privacy policies before providing personal information was a mere 37 percent in 2017.[30] While there is no New Zealand data on the topic, it can safely be assumed that a similar trend prevails here too. Much can be squeezed into a privacy policy without a consumer ever really knowing what they are consenting to, meaning privacy policies are virtually free licenses to collect and use data as a company wishes. But does that really matter, as long as you have nothing to hide?

---

[28] Maria Farrell "The Internet of Things – Who Wins, Who Loses?" *The Guardian* (online ed, London, 14 August 2015).

[29] Symantec *State of Privacy Report 2015* (Symantec, 2015) at 14.

[30] Jayne Van Souwe and others *Australian Community Attitudes to Privacy Survey 2017* (Office of the Australian Information Commissioner, May 2017) at 17.

B. Nothing to Hide, Everything to Lose

I will argue that despite having nothing to hide, in a world where the IoT is mainstream an individual has everything to lose from continuing to disclose personal information without limiting its future use. Attempting to describe future consequences of emerging technology use is necessarily speculative. However, the imminent threats I describe are extensions of existing technology threats and thus have a realistic grounding. The future concerns I describe while important to consider and based on academic theories are not manifested in any existing technology threats. Therefore, they are more speculative in nature and should be considered worst-case scenarios.

1. Imminent threats to personal autonomy

Autonomy is "freedom of the will".[31] That requires freedom from external control, and influence. A third party can exert control or influence over an individual by leveraging their interests, desires, and beliefs to persuade them towards, or away from, certain outcomes. Therefore, maintaining control over one's personal information to the exclusion of others is foundational to personal autonomy.[32]

The IoT collects very granular personal information because we use everyday objects to perform our most analogue functions, and connected objects provide an opportunity to digitise those functions. This has the potential to make individuals much more transparent than before. Granular information can be used, in isolation or with other information, to make incredibly accurate predictions about what an individual does, thinks, and feels.

For example, with two objects the Nest and Fitbit – it is possible to know when someone is home, as well as what their heart rate, skin temperature, and perspiration levels are.[33] If someone were to leave the house at two

---

[31] Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005) at 70, definition of "autonomy".

[32] Alan F Westin *Privacy and Freedom* (Bodley Head, London, 1970) at 33; see also Charles Fried "Privacy" (1968) 77 Yale LJ 475 at 483.

[33] Peppet, above n 6, at 101, 108.

o'clock in the morning, go somewhere and become very active, we might be able to draw certain inferences about what they are doing.[34] Or, if we restrict ourselves to a more scientific analysis: the electrical signals collected from someone's smart meter can determine with 96 percent accuracy what programme or movie someone is watching on television";[35] and, data collected from wearable technologies about biological primitives can be used to predict psycho-emotional states like stress, boredom or arousal.[36]

That level of transparency has the potential to make manipulation very effective. Late last year it was exposed some betting firms had been targeting vulnerable people with a standard online advertisement that claimed, "a gambler [had] cleared his debts and paid for his wife's medical treatment by playing online casino games".[37] Clearly this was an attempt at playing up to individuals in vulnerable positions generally. But in a world where the IoT is mainstream it will be possible for firms to know what people's real vulnerabilities are, and when they are at their most vulnerable. That provides an opportunity to create much more manipulative messages. And this deep analysis will not be restricted to the commercial industry, particularly if individuals continue to disclose their personal information without limiting its future use. Politicians, or employers may attempt to make use of the deep analysis the IoT offers to exert control or influence over individuals with an effectiveness we have not seen before.

---

[34] Scott Peppet, law professor at the University of Colorado Law School (Danny Vinik, The Agenda, 29 June 2015) transcript provided by Politico <https://www.politico.com/agenda/story/2015/06/how-to-regulate-iot-scott-peppet-interview-000112>

[35] Peppet, above n 6, at 110.

[36] Greenfield, above n 1, at 33.

[37] Rob Davies and Mark Sweney "Betting firms could be fined over ads 'targeting vulnerable people'" *The Guardian* (online ed, London, 13 September 2017).

2. *Imminent threats to individuality*

Individuality is the quality or character of a person that makes them different from others.[38] Generally, individuality requires a space for sheltered experimentation and testing of ideas, safe from ridicule or penalty.[39] Therefore, surveillance is detrimental to the freedom of an individual to express their individuality.[40]

The IoT has the potential to make surveillance a more common occurrence. The position of IoT objects makes it easier to surveil individuals who are performing their daily functions, and makes it possible to do so without physically watching them. Already, this has been taken advantage of by the insurance industry. Progressive Insurance offer discounts on premiums to customers who use small electronic monitors in their car to track total driving time, speed, and driving habits.[41] Members of this scheme have noted the effects it has had on altering their behaviour to conform with Progressive's desired standards.[42] Similarly, health insurance companies in the United States and United Kingdom have extended their customers steep discounts on the Apple Watch, together with reduced premiums for those that continue to report high and regular levels of exercise.[43]

At the moment, one can choose whether to opt into these schemes. However, some insurance companies have already begun to exclusively supply

---

[38] Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005) at 553, definition of "individual" and "individuality".

[39] Westin, above n 32, at 34; see also Edward J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYU L Rev 962 at 1003.

[40] Neil M Richards "The Dangers of Surveillance" (2013) 126 Harv L Rev 1934 at 1945 – 1952.

[41] Progressive "Snapshot" Progressive <https://www.progressive.com/auto/discounts/snapshot/>.

[42] Scott R Pepett "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future" (2011) 105 NW U L Rev 1153 at 1154.

[43] John Hancock *Vitality Active Rewards with Apple Watch* John Hancock < https://www.johnhancockinsurance.com/vitality-program/apple-watch.html>; Vitality *Vitality Active Rewards: Apple Watch* Vitality <https://www.vitality.co.uk/rewards/partners/active-rewards/apple-watch/>.

interactive insurance policies.[44] It is not difficult to imagine a time when the ability to choose is not an option, or at least opting into schemes like this is normalised so those who refuse to do so are assumed to be withholding negative information and are therefore penalised.[45] Or perhaps the individual will be bypassed in the collection process altogether, if the manufacturers of fitness trackers and automobiles begin to include the ability to sell data to insurance companies in their privacy policies. And what if surveillance begins to creep into other parts of our lives? Schools may begin to monitor extracurricular learning efforts, and employers may begin to monitor the behaviour of employees on business trips. The result will be decreased individuality in all of those domains.

3. Imminent threats to relationships

Relationships are defined and nurtured through gifts of intimacy.[46] A gift of intimacy is "the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone".[47] Exclusive control over personal information is required to parcel up gifts of intimacy and chose how to provide them to an individual in an exclusive manner.

The way individuals currently disclose personal information to companies will make it hard to maintain exclusive control over the contents of a gift of intimacy in a world where the IoT is mainstream. As I have argued, it will be possible for those with granular information about someone to make extremely accurate predictions about their actions, beliefs, and emotions. If there are no restrictions on how that information can be used in the future, it is conceivable it may be inadvertently given to an unintended recipient. In fact, this threat has already been realised in a world where the IoT is not

[44] Suzanne Barlyn "Strap on the Fitbit: John Hancock to sell only interctive life insurance" (20 September 2018) Yahoo! <https://finance.yahoo.com/news/strap-fitbit-john-hancock-sell-141135104.html>.

[45] Peppet "Unraveling Privacy", above n 42, at 1156.

[46] Charles Fried "Privacy" (1968) 77 Yale LJ 475.

[47] Fried, above n 46, at 484.

mainstream. Recently, Target predicted a woman was pregnant based off her in store purchasing habits.[48] They then started sending personalised pamphlets for baby clothes and cribs to the woman's home address, which were seen by her father. Her father confronted her about this material, and as a result, the daughter was forced to tell her father she was pregnant.

This could have had a negative effect on the relationship in any number of different scenarios. First, the daughter may have intended to tell her father she was pregnant at some point, however this confrontation would have limited her choice of when and how to gift him that knowledge. Instead of being able to make an event out of it with the involvement of her partner, she was forced to tell him in an unexpected, inquisitory environment. The gift was undoubtedly less relationship enhancing as a result. Secondly, the pamphlet may have been seen by someone else – perhaps her father's friend, or the pamphlet deliverer. This would ruin "the quality of exclusivity intimacy requires of a gesture of love or friendship".[49] A gift undoubtedly feels less sentimental if it has already been shared with someone else, especially if you would expect to have been the first told. Finally, and most harrowingly, there is the possibility she did not want her father to know at all, for any number of reasons. Often it is the case that there are thoughts whose expression to friend, family or lover would be a hostile act, though the entertaining of them is completely consistent with friendship or love.[50] That hostile act has the potential to not only ruin that particular gift of intimacy, but the relationship in its entirety.

In a world where the IoT is mainstream, situations like this will not be odd or newsworthy. Granular data collection will lead to more opportunities for organisations to acquire the contents of people's intimate gifts, and the increase in objects capable of interacting with people in their homes will lead to more insensitive and inopportune digital suggestions. Whether it be

---

[48] Kashmir Hill "Hot Target Figured Out a Teen Girl Was Pregnant Before Her Father Did" *Forbes Magazine* (online ed, New York, 16 February 2012).

[49] Fried, above n 46, at 490.

[50] Fried, above n 46, at 485.

learning about a partner's proposal plans, or a family member's undisclosed sexuality, more gifts of intimacy will be ruined, with flow-on effects for the ability of individuals to define and nurture relationships.

4. Future threats to society

At a greater level of abstraction, continuing to disclose personal information without restricting its future use could have detrimental impacts on society. While these ideas are much more speculative and future orientated, they are no less necessary to consider even if only to raise awareness about the very worst-case scenarios of maintaining the status quo in a world where the IoT is mainstream.

First, the IoT may frustrate liberal democracies through enabling more effective manipulation. I have already outlined why the IoT will enable more effective manipulation. However, I have not discussed how this may blunt societies' liberal capacities. The primary condition for a liberal democracy is citizens who possess the capacity for democratic self government; the liberal self and the liberal democracy are symbiotic ideas.[51] At the most basic level, the liberal self is someone who makes independent decisions formed through robust open debate.[52] Personal autonomy is an important cornerstone to the liberal self, because to make independent decisions one must be capable of autonomous thought.

The IoT's contribution to more effective manipulation will make it harder for individuals to generate independent political ideas. This is not just due to the capacity for intended political manipulation,[53] but more subtle modulation too. Julie Cohen has described how as search and social networking become more seamlessly integrated, individuals move within personalised filter bubbles.[54] These bubbles conform an individual's

[51] Julie E Cohen "What is Privacy For" (2013) 126 Harv L Rev 1904 at 1918.

[52] Cohen, above n 51, at 1917.

[53] Which I have described as possible, above in *Immediate threats to personal autonomy*; and which we have seen manifested earlier this year in the infamous Facebook/Cambridge Analytica scandal, see below n 67.

[54] Cohen, above n 51, at 1917.

informational environment to the political and ideological commitments they are predicted to affiliate with. Therefore, individuals are mostly exposed to political ideas they like and that look unchallenged by other like-minded individuals in their filter bubble. In turn, although not the end goal of the modulators, this will have the flow-on effect of entrenching biases.

This modulation is a form of manipulation. Core drivers are being leveraged to decide what information will keep individuals in a comfortable environment. With the addition of the IoT to this technology cocktail, the amount of granular information will make individuals' filter bubbles narrower, while also making it easier to keep individuals within them. Liberal democracies are enabled by individuals whom, acting as their liberal self, perform functions such as voting and debating on public issues.[55] If individuals become less able to act as their liberal selves then liberal democracies will be weakened.

This is the most relevant societal threat for a country like New Zealand. However, a more radical problem may await those who do not start with a liberal democratic system. A totalitarian state, for example, relies on secrecy for the regime and high surveillance of all other groups.[56] I have already discussed how the position of IoT objects in everyday life will make it easier for companies to surveil individuals for their own benefit. What if the public sector had access to this information too? If a government were to have access to all of this information then they could have the kind of large-scale surveillance required to support and entrench an undemocratic regime. Some governments already buy and borrow private sector data for the purpose of surveillance.[57] Furthermore, companies with large troves of personal information have shown a willingness to assist unliberal regimes where there is a commercial benefit involved for them.[58] Therefore, it is not

[55] Cohen, above n 51, at 1912.

[56] Westin, above n 32, at 23.

[57] See Robert O'Harrow *No Place to Hide* (Free Press, New York 2005).

[58] Alex Hern "Google 'working on censored search engine' for China" *The Guardian* (online ed, London, 2 August 2018).

completely beyond the realms of possibility to suggest that in a world where the IoT is mainstream, disclosing personal information without imposing limits on its future use could give totalitarian states the kind of high surveillance they need to thrive.

Governments may not even need to monitor every aspect of an individual's life to maintain an authoritarian regime. It has been argued the possibility of being consistently watched produces conformity even if an individual is not being watched in fact. This is called the Panoptic effect.[59] The Panopticon is a surveillance structure that was designed by Jeremy Bentham in the late 18th century.[60] The design consists of a circular exterior wall with a detached inspection house at the centre. Individuals are stationed in cells that line the exterior wall and face inwards to the inspection house. Critically, individuals in the cells cannot see into the inspection house and thus have no idea whether they are actually being watched at any given moment. Because of this, individuals act in conformity even when they are not being watched at all, because they fear being caught acting out at any moment.[61] In an authoritarian regime, by continuing to surrender personal information to the IoT without imposing limitations on its future use, citizens will be forced to assume every moment of their life may be observed and scrutinised by the government. Provided they are sparingly disciplined for acting out of conformity this mere possibility of being watched may be enough to support an authoritarian regime even if the government cannot watch every aspect of an individual's life in fact.

5. Unknown future threats

There are additional unknown consequences of disclosing personal information without limiting its future use. Outcomes are imbedded within collected data, which are only unknown because exploiting data in a way that would produce them has not been discovered yet.

---

[59] See Ronald Bailey "Your Cellphone is Spying on You" (3013) 44(8) Reason 35 at 36.

[60] Jeremy Bentham, *The Works of Jeremy Bentham* (William Tait, Edinburgh, 1843).

[61] See generally Richards, above n 40, at 1948.

The best way to illustrate the fact unknown consequences exist within already collected data is through a case study presented by Adam Greenfield. He explains that:[62]

> In 1936 it became mandatory for each Dutch municipality to maintain a demographic record of its inhabitants … This information was maintained on Hollerith Cards, the most advanced data storage and processing system at the time … Both the Hollerith cards on which the civil registry of 1936 was tabulated, and the machines necessary to sort and read them, immediately fell under German control after the invasion of 1940. The same data that was innocuous when provided to the Bureau of Statistics turned out to be lethal in the hands of the Gestapo …

Greenfield uses this case study to show that there is a risk the data we shed onto the IoT will be dangerous if it falls into the wrong hands. That is true, but I would argue the risk is not isolated to a change in data controller. The risk is caused by an enlightenment to the idea that a data set has a hidden outcome within it. There are many variables that may result in such an enlightenment; changes in social attitudes, market conditions, the political environment, and technology. Therefore, the unknown outcomes are not dependent upon a change in data controller. The risk is dependent upon the mere fact that we do not know every purpose to which data we collect can and will be used for in the future.

In a world where the IoT is mainstream very little data will be left uncollected. The more granular information surrendered to the IoT the larger the data base with unknown future outcomes imbedded within it will become. By not only submitting to the siphoning of this information, but also failing to place caveats on its future uses, that data base will be ripe for exploitation when someone is enlightened as to any of its hidden outcomes; and as Greenfield's case study illustrates, some of those hidden outcomes can shape the world in terrifying ways.

---

[62] Greenfield, above n 1, at 61.

Chapter II: The Law's Problem

A. Why Worry? It's a Free Choice, Right?

In the previous chapter, I argued there will be serious consequences for individuals and society if current disclosure behaviours persist in a world where the IoT is mainstream. In this chapter, I consider an obvious counter argument. If users of the IoT are freely choosing to hand over their personal information, why should this be a concern for anyone else? And in particular, why should it be a concern for the law? I will argue that current disclosure behaviours are a concern for the law because users of the IoT are not necessarily 'freely' choosing to hand over their personal information.

Despite the relaxed disclosure behaviour of individuals, the overwhelming consensus from empirical research is that people are becoming more concerned about their privacy. In New Zealand, two thirds of respondents to a 2018 survey conducted by the Privacy Commissioner's Office declared concern about their privacy, and 55 percent of respondents said they were more concerned about issues with their individual privacy than in the last few years.[63] Similar sentiments can be found in the results of surveys carried out in Australia,[64] the European Union,[65] and the United States.[66]

The results from these surveys attribute increasing concerns about privacy to a variety of perceived internet related threats. In all of the countries there is an overwhelming distrust of online companies *vis-a-vis* offline companies. People are most uncomfortable with that sector tracing and storing information about them, sharing or otherwise using information without their permission, and being targeted in personalised ways.

Even public activity reflects a concern for informational privacy. In this year's Facebook and Cambridge Analytica scandal it came to light that

---

[63] Privacy Commissioner "Privacy concerns on the rise – public survey" (press release, 7 May 2018).

[64] Van Souwe and others, above n 30.

[65] Symantec, above n 29.

[66] Mary Madden and others *Public Perceptions of privacy and security in a psot-snowden era* (Pew Research Center, 2014).

Cambridge Analytica had used Facebook to collect the personal information of more than 50 million Facebook users. That information was used to create psychographic profiles of data subjects so politicians who hired Cambridge Analytica could determine what kind of advertisement would be most effective to influence a particular person in a particular location.[67] After this was exposed, Facebook CEO Mark Zuckerberg issued a public apology,[68] US Congress condemned the activity,[69] class actions were filed against the two companies,[70] Facebook suffered a $50 billion drop in market capitalisation,[71] public outrage fuelled countless media reports, and there were revived calls for stronger data protection regulation.[72] Collectively, these responses show the community at large found something inherently wrong with the collection and use of personal information in this way.

Why then, do people readily disclose personal information without attempting to restrict its future use? When individuals' disclosure behaviours are juxtaposed against this overwhelming concern for informational privacy, their behaviour appears nonsensical. For the last ten years, privacy researchers have attempted to explain this dichotomy of privacy attitude and actual privacy behaviour, known as the 'privacy paradox'.[73] No comprehensive explanation has been found.[74] However, most theorists agree humans have a natural inability to make rational

---

[67] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr "How Trump Consultants Exploited the Facebook Data of Millions" *The New York Times* (online ed, New York, 17 March 2018); Carole Cadwalladr and Emma Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" *The Guardian* (online ed, London, 17 March 17 2018).

[68] Julia Carrie Wong "Mark Zuckaberg apologises for Facebook's 'mistakes' over Cambridge Analytica" *The Guardian* (online ed, London, 22 March 2018).

[69] Cecilia Kang "Facebook Faces Growing Pressure Over Data and Privacy Inquiries" *The New York Times* (Online ed, New York, 20 March 2018).

[70] Owen Bowcott and Alex Hern "Facebook and Cambridge Analytica face class action lawsuit" *The Guardian* (online ed, London, 10 April 2018).

[71] Cecilia Kang, above n 69.

[72] Cecilia Kang, above n 69.

[73] Gerber, Gerber and Melanie, above n 2, at 227.

[74] Gerber, Gerber and Melanie, above n 2, at 227.

decisions about privacy self-management.[75] It seems we are not built to properly consider privacy concerns at the moment we are asked to disclose personal information. Thus, when we disclose personal information it does not reflect true intent as it exists in the abstract.

While the law might not have a legitimate mandate to make decisions for individuals, it should create an environment that allows individuals to make decisions that reflect their true intent. The first part of this chapter will discuss how individuals decide whether or not to disclose personal information, and more specifically, why they find it difficult to properly consider their privacy concerns in that process. The second part of this chapter will analyse the relevant legal framework and explain how it fails to create an environment to help individuals make decisions that reflect their true intent.

B. The Decision-making Process

1. Privacy calculus

The dominant theory for explaining how individuals decide whether to disclose personal information is privacy calculus.[76] This theory extends from an economic idea;[77] a rational consumer makes decisions that are all driven by an attempt to maximise their benefit. Applied to the privacy context, it is postulated that when individuals are asked to disclose a piece of personal information, they perform a calculation between the expected loss of privacy and the potential gain of disclosure.[78] If the anticipated

[75] See Peppet "Regulating the Internet of Things", above n 6, at 160; Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880; Ryan Calo "Code, Nudge, or Notice?" (2014) 99 Iowa L Rev 773 at 788-789 (reviewing critiques of privacy notice).

[76] Gerber, Gerber and Melanie, above n 2, at 229.

[77] Gerber, Gerber and Melanie, above n 2, at 229.

[78] Spyros Kokolakis "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon" (2017) 64 Computers & Security 122 at 128.

benefits outweigh the costs, the individual will disclose that piece of personal information.[79]

This theory is supported by empirical research. One of the earliest studies to reveal "something of a 'privacy paradox'" discovered that individuals who expressed concerns about their privacy being infringed were still willing to give away personal details to online retailers as long as they had something to gain in return.[80] Similarly, a later interview and experiment found that users actively share personal information despite their concerns because they consider the expected benefits of sharing in addition to the risks.[81] Most recently, a 2018 study of various data variables and personal information disclosures found possible benefits that a user can gain through data disclosure was among the best predicters for disclosure.[82]

It is not paradoxical to care about opposing things, and seek to balance them. In fact, privacy calculus is a perfectly rational decision-making process. However, its rationality assumes a rational agent.[83] Currently, individuals are not capable of acting rationally when performing privacy calculus because of constraints on their ability to access and process information about privacy risks.

2. *Limited information*

The circumstances an individual usually finds themselves in when required to perform privacy calculus make it hard to access information about all the risks of disclosure. First, individuals are still relatively naive about the quality of personal information companies are capable of collecting and how that information can be used. For example, the surprised reactions to the

[79] Kokolakis, above n 78, at 128.

[80] Barry Brown *Studying the Internet Experience* (HP Laboratories Bristol, Technical Report HPL-2001-49, 26 March 2001).

[81] Haein Lee, Hyejin Park and Jinwoo Kim "Why do people share their context information on Social Network Services? A qualitative study and an experimental study on user's behaviour of balancing perceived benefit and risk" (2013) 71(9) Int J Hum Comput Stud 862.

[82] Gerber, Gerber and Melanie, above n 2, at 252.

[83] Kokolakis, above n 78, at 129.

Facebook and Cambridge Analytica scandal show society is generally unaware about data linkage, profiling, and how that can be used to manipulate them. Second, disclosure decisions are often made hastily as they represent an obstacle to the acquisition of some desired benefit. Therefore, there is a lack of practical opportunity to discover the full extent of what is not already within the general knowledge of the consumer. Finally, there is an incentive for data collectors to make it hard for disclosers to access information about the negative implications of disclosure. As I have argued in chapter one, there is great motivation for companies to collect as much personal information as possible. Drawing attention to the risks of that activity would be self-defeating, which is why privacy policies have historically been expressed in such an indigestible manner.

Consequently, individuals are not usually fully informed about the risks of disclosing their personal information when they are asked to do so. Making a privacy calculation based on incomplete information prevents individuals from acting rationally.[84] From their subjective point of view disclosure may appear to be the utility maximizing option. However, that is because within their limited boundaries of reasoning they cannot apply the concerns they have for privacy to the facts they do not know about. Therefore, from the objective point of view of someone who has complete information, disclosure is cost-neglecting and irrational.

3. Cognitive biases

The rationality of an individual's privacy calculus is further disrupted by cognitive biases.[85] All decisions are affected by these biases to a degree.[86] However, because individuals have trouble accessing information when

[84] Christian Flender and Gunter Muller "Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited" in Jerome R Busemeyer and others (eds) *Quantum Interaction: 6th International Sympnosium* (Springer-Verlag Berlin, Heidelberg, 2012) 148 at 151.

[85] Gerber, Gerber and Melanie, above n 2, at 229; Kokolakis, above n 78, at 128.

[86] Alessandro Acquisti and Jens Grossklags "What can behavioural economics teach us about privacy" in Acquisti and others *Digital Privacy: theory, technology, and practices* (Auerbach Publications, 2007) 363.

performing privacy calculus, they tend to rely on heuristics, which make biases even more influential.[87]

'Availability bias' leads individuals to overestimate the probability of events they can easily recall.[88] Most people have not personally suffered from privacy invasions,[89] or if they have, are unaware of that fact. Therefore, they are likely to recall only positive experiences associated with the disclosure of personal information, disassociated from negative consequences. Although infamous privacy breaches raise a general awareness about the risks of disclosure, 'optimism bias' leads individuals to believe they are at less risk of experiencing negative privacy compared to others.[90] Therefore, when an individual is asked to disclose their personal information these biases are likely to cause them to neglect some privacy risks.

Furthermore, the 'affect heuristic' leads people to make judgements based on their affective impression when forced to decide something quickly.[91] This tends to lead individuals to underestimate the risks associated with things they like.[92] Consumer facing objects are designed to elicit enjoyment from individuals, and IoT objects are no exception. Therefore, the risks that are recognised by a potential discloser are likely to be discounted by the haze of convenience and enjoyment these novel internet-connected devices cast.

Perhaps the most influential bias on an individual's privacy calculus is the 'immediate gratification bias', which leads individuals to value present benefits or risks more than those that lie in the future.[93] The decision about

---

[87] Gerber, Gerber and Melanie, above n 2, at 229.

[88] Norbert Schwartz and others "Ease of Retrieval as Information: Another Look at the Availability Heuristic" (1991) 61 J Person Social Psychol 195.

[89] Gerber, Gerber and Melanie, above n 2, at 230.

[90] Hichang Cho, Jae-Shin Lee and Siyoung Chung "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience" (2010) 26 Comput Hum Behav 987.

[91] Paul Slovic and others "The Affect Heuristic" in Thomas Gilovich and others *Heuristics and Biases* (Cambridge University Press, Cambridge, 2002) 397.

[92] Paul Slovic and others, above n 91 as cited in Gerber, Gerber and Melanie, above n 2, at 230.

[93] Alessandro Acquisti and Jens Grossklags "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior" Proceedings

whether to disclose personal information is usually presented as a barrier to access some benefit – tick the box to begin tracking your step count and heart rate in real time - thus the benefit always appears immediate, tangible, and highly valuable. This is to be contrasted with the risks of disclosure, which usually lie in the distant future, are predominantly unknown, and often very abstract. The result is the already discounted risks of disclosure are rarely a match for the inflated benefits they are pitted against.

When faced with a decision about whether to disclose personal information, individuals intend to employ a rational process that weighs the benefits of disclosure against the privacy costs to determine the most valuable outcome for that individual. However, humans are not equipped to act rationally when faced with these types of decisions. The circumstances these decisions are usually put to individuals in limit their access to information about the risks of disclosure, which leads to decisions that are prone to the influence of cognitive biases. The result is individuals often overestimate the value of disclosure and underestimate the privacy risks, which means they stand no chance of making a decision that accurately reflects the intention they had when beginning their privacy calculus.

C. Lack of Legal Empowerment

In New Zealand, privacy law is a complex mesh of legislation, common law and equity. Some of this law has the concept of privacy as its central focus;[94] other law has the ancillary consequence of protecting privacy while pursuing different goals.[95] The patchy protection afforded to privacy by the law reflects the fact privacy is an amorphous concept with many different and sometimes incompatible elements.[96] Fortunately, we are only concerned

---

of the second annual workshop on economics and informational security (WEIS, 2003) at 16.

[94] For example: Privacy Act 1993; the privacy tort of public disclosure of private facts, *Hosking v Runting* [2005] 1 NZLR 1 (CA); and the privacy tort of intrusion upon seclusion, *C v Holland* [2012] 3 NZLR 672 (HC).

[95] Such as the equitable tort for breach of confidence, or civil and criminal trespass.

[96] *Marfart v Television New Zealand* [2006] 3 NZLR 534 (CA) at [60]; For a summary of the different definitions of privacy see Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008) at 31 – 47.

with one particular element – informational privacy –[97] and specifically the rules that govern the moment individuals give their personal information to somebody else. This regulatory domain is governed by the Privacy Act 1993 (**the Act**). The Privacy Bill which will repeal and replace the Act is currently with the Select Committee,[98] but is not set to make any amendments relevant to the following discussion.

1. Relevant purpose and scope of the Act

The relevant purpose of the Act is to "establish certain principles with respect to the collection … by public and private sector agencies, of information relating to individuals".[99] This must be understood in the context of the Act's purpose to promote individual privacy in accordance with the Recommendation of the Council of the OECD Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (**OECD Guidelines**).[100] The OECD Guidelines recommend placing limits on the collection of personal data, that such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (the **Collection Limitation Principle**).[101]

There is nothing in this purpose that ostensibly recognises individuals need to be supported through the decision-making process of disclosing personal information. In fact, there is an assumption that by giving individuals the opportunity "where appropriate" to know and consent to the collection of their personal information, that they will be able to make that decision in their own interests. As I have argued, this is a false assumption. Individuals are in a vulnerable position when making decisions about the disclosure of their personal information. Legislation grows up around its purpose,

---

[97] Law Commission *Privacy Concepts and Issues*, above n 96, at 57: "At its core, informational privacy is concerned with control over access to private information or facts about ourselves".

[98] Privacy Bill 2018 (34-1).

[99] Privacy Act 1993, long title.

[100] Privacy Act 1993, long title.

[101] Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), article 7.

therefore by failing to recognise this fundamental vulnerability the Act takes off on the wrong trajectory from the outset. The negative implications of this will become apparent when I come to discuss *principles two and three of the Act: notice and consent*, and *remedies under the Act*.

The Act carries out its objective through four principles, which all centre around two concepts: personal information, and agencies. Personal information is defined broadly, as any information about an identifiable individual,[102] including information in which the individual can have no expectation of complete privacy;[103] and an agency refers to persons and organisations in the public, and private sector.[104] Therefore, the scope of the principles catch almost every collection of any individual's personal information, with the notable exclusions of collection for personal use,[105] and by the news media.[106] This is a legitimately broad scope because it represents the need to scrutinise every disclosure, leaving no room for an organisation to circumvent that scrutiny. The proper point to limit the scrutiny is through the operative principles.

2. *Principles two and three of the Act: notice and consent*

Under principle two, personal information must be collected directly from the individual concerned, subject to exceptions.[107] Some of the relevant exceptions include a reasonable belief that: (a) the information is publicly available; (b) the individual authorises collection from someone else; or (c) compliance is not reasonably practicable in the circumstances.

Principle three provides an agency must take such steps as are reasonably necessary, before information is collected, to make an individual aware of a

---

[102] Privacy Act 1993, s 2.

[103] *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR 710 at [132].

[104] Privacy Act 1993, s 2. There are some exceptions from the definition of "agency", but for all practical purposes, an "agency" includes nearly every person and organisation.

[105] Privacy Act 1993, s 56.

[106] Privacy Act 1993, s 2. An "agency" does not include "in relation to its news activities, any news medium".

[107] Privacy Act 1993, s 6.

number of relevant facts. Some of those relevant facts include: (a) the fact information is being collected; (b) the purpose for which the information is being collected; and, (c) the intended recipients of the information.[108] This principle is subject to exceptions that are similar to those set out under principle two.

While consent is not explicitly mentioned in principles two and three, the Chief Justice has observed the scheme of the Act is such that informed consent is central to collection.[109] Informed consent is a popular mechanism in data protection law, designed to give an individual control over the disclosure of their personal information.[110] The idea is to ensure the data collector gives an individual the necessary information and opportunity for that individual to make a decision in their best interests. However, this mechanism is flawed. Mere notice and consent does not actually give individuals the control it promises. First, I have argued individuals are naturally flawed at making decisions about privacy self-management; notice and consent does nothing to ameliorate this difficulty.

Secondly, the notice and consent regime can be manipulated by data collectors to take advantage of individuals' limited ability to make disclosure decisions in their interests. This is because collectors are left a very broad discretion over how to design the way they give notice and obtain consent. In his book *Privacy's Blueprint*, Woodrow Hartzog explains the function of design and how design can be used to manipulate individuals' privacy decisions.[111] The function of design is two-fold: first, design communicates information about how something is to be understood; and second, design enables or hinders activities.[112]

In the notice and consent regime, the quintessential design collectors use to manipulate individuals is the privacy policy. First, these policies can be

---

[108] Privacy Act 1993, s 6.

[109] *R v Alsford*, above n 103, at [138].

[110] Peppet "Regulating the Internet of Things", above n 6, at 140.

[111] See generally Hartzog, above n 13, at 21 – 56.

[112] Hartzog, above n 13, at 26.

designed to make certain things hard for individuals. For example, policies are often tucked away in locations external to the request for disclosure making them hard to access.[113] Even if accessed, the quantity and complexity of the information makes it difficult for a layperson to understand. Ultimately, design is used to make it hard for individuals to obtain the information they need to properly understand what they are purporting to agree to. Concomitantly, it is not uncommon to find a pre-checked "I accept the Privacy Policy" box,[114] which makes it easier for individuals to consent to the policy they have been deterred from attempting to understand.

Secondly, a data collector can use certain signals to communicate how this policy ought to be understood. An example of a trust enhancing signal is the padlock icon. "[E]ach padlock icon invites reliance upon a technology or service. It signals safety … [and] can affect peoples' expectations regarding their relationship with a company".[115] Of course displaying a padlock icon in the vicinity of a request for personal information does not physically protect your information from anything, but it is capable of leading people to believe there is some sort of limit on how their information can be collected and utilised. Signals may be heavily relied upon by people who have already been deterred from finding out the truth.

Perhaps a red flashing exclamation mark would be a more accurate signal to provide. However, given the broad discretion collectors are given by the Act to design the way they give notice and obtain consent, there is the flexibility to use virtually whatever signal they want in order to convey a message about how the policy should be understood. Together with the ability to make certain things harder or easier, this makes the notice and consent regime a dangerously malleable tool for collectors of personal information.

---

[113] See Peppet "Regulating the Internet of Things", above n 6, at 141 – 144 for a discussion about the way 20 popular internet of things devices utilize the privacy policy.

[114] So much so that Regulation (EU) 2016/279 on General Data Protection Regulation [2016] OJ L119/1, recital 32 now prohibits this activity. However, the law in New Zealand does not prohibit this activity.

[115] Hartzog, above n 13, at 28.

Design is particularly effective at manipulating individuals because people react to design in predictable ways.[116] All a company has to do is make it hard for individuals to access information, and predictably they will disregard that offer choosing instead to rely on heuristics. This makes cognitive biases more influential, which with the addition of some design signals will pull them strongly towards consent. Just like that, the notice and consent mechanism intended to give disclosers control can be leveraged by collectors to manufacture the permission they need to collect whatever information they want. This effectively puts control in the collectors' hands, rather than the hand of the disclosers.

In the context of the IoT, notice and consent is even more problematic. IoT objects are often small, screenless, and lack an input mechanism to register responses.[117] Where, for example, is the mechanism for an open dialogue about the risks of disclosure between a consumer and their smart bed? While privacy notices could be included in or on the packaging of IoT products, this does nothing for individuals who buy their products second-hand. Some products offer notice and consent through a set-up function in a phone application.[118] However, this just brings us back to the existing problems with privacy policies; and, how are consumers of these products to be re-notified if that policy changes?

Principles two and three of the Act only require the taking of steps that are reasonably necessary, and offer an exception where compliance is not reasonably practicable in the circumstances. Therefore, producers have no incentive to overcome the unique obstacles the IoT provides for notice and consent regimes. The principles do not require them to invent better ways to obtain quality informed consent. As long as notice is given and consent obtained, data collectors have fulfilled their obligations. Thus, while the IoT

[116] See Hartzog, above n 13, at 34 for a discussion about the long history governments and industry have of leveraging design to influence behavior.

[117] Peppet "Regulating the Internet of Things", above n 6, at 140; Howard W Waltzman and Lei Shan "The Internet of Things" (2015) 27(7) Intellectual Property & Law Journal 19 at 20.

[118] Peppet "Regulating the Internet of Things", above n 6, at 141.

is being granted more regular access to our intimate moments than any technology has had before, its ability to ask for permission to do so could not be more dysfunctional.[119] The loser in all of this is the consumer who is left to fight their own cognitive obstacles, and the obstacles provided by those who want to collect their personal information before they can hope to make a decision that is truly consistent with their privacy concerns.

3. Principles one and four of the Act: protection at the margins

Under principle one, personal information must be collected for a lawful purpose, connected with a function or activity of the agency; and, be necessary for that purpose.[120] This principle is important for two reasons. First, the purpose of collection provides a limit for what uses the information can be put, and to whom information can be subsequently disclosed.[121]

Second, by limiting the legitimate purposes of collection the Act strives to prohibit the indiscriminate collection of personal information, which reflects the Collection Limitation Principle in the OECD Guidelines. The OECD was concerned about the collection of sensitive information.[122] However, it is hard to define sensitive information because information often takes on its character of sensitivity from the circumstances of its intended use.[123] Therefore, instead of prohibiting the collection of "sensitive information" the OECD Guidelines attempt to mitigate the risks associated with that collection through limiting the collection of personal information generally.[124] By only permitting the collection of information for a legitimate purpose, individuals are arguably protected from the negative consequences of sensitive information collection. Sensitive information can

---

[119] Hartzog, above n 13, at 264.

[120] Privacy Act 1993, s 6.

[121] Privacy Act 1993, s 6. Principles 10 and 11 provide that personal information is only to be used or disclosed for the purposes for which it was obtained.

[122] Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum* (1980) at [50].

[123] Organisation for Economic Co-operation and Development, above n 122, at [50].

[124] Organisation for Economic Co-operation and Development, above n 122, at [51].

still be collected, but because it has to be put to a legitimate purpose it is less likely for that collection to result in negative consequences for the individual concerned.

This principle recognises the power imbalance between data collectors and disclosers exists, and manifests that concern in an attempt to protect the discloser from being taken advantage of. That idea is consistent with the need to assist individuals with disclosing personal information in line with their interests, as it can safely be assumed nobody wants to disclose sensitive information about themselves for unknown future purposes. Therefore, by effectively prohibiting this behaviour the Act provides some protection to individuals at the margins of the data collection process.

However, the effectiveness of the means the Act has employed to fulfil this purpose is unclear. On a plain reading of principle one, it is possible to cast the collection of personal information itself as a function of the agency, especially for technology companies that want to experiment with how they can leverage information for an increasing number of obscure uses. Because the concept of "purpose" is supposed to operate as a limitation on the collection of personal information, it would be self-defeating to allow collection itself to constitute a legitimate purpose.[125] However, the Act is silent on the level of detail required for describing purpose and therefore the position is unclear.

Under principle four, personal information shall not be collected by means that, in the circumstances: are unlawful; are unfair; or, intrude to an unreasonable extent upon the personal affairs of the individual concerned.[126] This represents another paternalistic effort at bridging the power imbalance between information collectors and disclosers. However, principle four has not been used to mitigate the ostensibly unfair way companies leverage the

[125] Paul Roth "Report on Aspects of Privacy Compliance & Practice of NZ Post Lifestyle Survey 2009 Privacy Act Perspective" (20 June 2011) Office of the Privacy Commissioner <privacy.org.nz/reports-on-aspects-of-privacy-compliance-and-practice-of-the-nz-post-lifestyle-survey-200/>.

[126] Privacy Act 1993, s 6.

notice and consent regime in principles two and three. It is conceivable that principle four could be used as the way privacy policies effectively operate as antiprivacy policies seems "unfair" and principle four is cast very broadly. However, until this is tested the ability for principle four to provide protection to consumers of the IoT in this way, is unclear.

4. The Act's definition of "collect"

Even if the operative principles did empower individuals to make decisions consistent with their intentions, there is still scope for individuals to be left without that assistance in some circumstances. That is because the principles are only engaged when information is "collected"; and there is uncertainty as to whether some types of information are caught by that definition.

Collection is defined to exclude the receipt of unsolicited information.[127] While extraordinarily broad, this still raises questions because of the uncertainty about what "unsolicited" means.[128] Some types of information are clearly unsolicited, for example: information provided to an agency without asking for it; or, information provided to an agency by mistake. However, other types of information are not as clear cut. Of particular relevance to the IoT is internally generated information. In *Boyle v Manurewa RSA Inc*,[129] the Human Rights Review Tribunal found that the outcome of a disciplinary process was not information that had been collected by the RSA.[130] By extension it could be argued that predictions about individuals, which are based on granular data that has been collected, would not be deemed to be collected for the purposes of the Act. The information has not been asked for, and thus it is unsolicited in the ordinary sense of the word. Furthermore, it does not necessarily come from the individual. Instead, it has been extrapolated from requested information.

---

[127] Privacy Act 1993, s 2.

[128] Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2010) at [3.89].

[129] *Boyle v Manurewa RSA Inc* [2003] NZHRRT 16.

[130] *Boyle v Manurewa RSA Inc*, above n 129, at [31].

I have argued IoT predictions can approximate facts about an individual with great accuracy, and lead to some of the most serious consequences for individuals and society. Yet individuals may not even be afforded control over that information under the scheme of the Act.

5. Remedies under the Act

Liability is incurred under the Act when an agency breaches an information privacy principle,[131] and the individual concerned has suffered or may suffer harm as a result:[132] The relevant harm can take three general forms, which appear to be categorised by level of abstraction: loss, determent, damage, or injury; an adverse effect to rights, benefits, privileges, obligations, or interests; or, significant humiliation, loss of dignity, or injury to feelings.

The Act looks for concrete harm, or a very close approximation of it, before it will offer an individual its assistance. This ignores the fact that many privacy breaches do not manifest in such harm. Particularly when it comes to having personal information collected in an unfair way, it is very difficult to articulate a clear and recognisable injury. We might find it harder to trust others in the digital space, or be forced to watch our back and cover our traces[133] but it is unlikely we will suffer tangible damage or injury, or an emotional effect demonstrable to the significance the Act requires. Individuals may not even discover they have had information collected from them contrary to the privacy principles in the first place.

Because the Act only lends support when quantifiable harm has been done, it saddles individuals with the entire burden of recovering from the most common harms they will suffer. Concomitantly, it gives data collectors little incentive to abide by the collection principles. Ultimately, this gives the Act a narrow remedial scheme, which does nothing to help individuals make disclosures that are more consistent with their privacy concerns.

---

[131] With the exception of principles 6 and 7, which relate to access and correction of one's personal information.

[132] Privacy Act 1993, s 66(1).

[133] Hartzog, above n 13, at 71.

Chapter III: *Taking the First Step*

A. A Principled Approach to Regulation

In the previous chapter, I argued individuals disclose personal information without limiting its future use because they need support making decisions consistent with their privacy concerns, and the law fails to give them that support. In this chapter I offer a regulatory solution. The chapter concentrates on what the regulations might look like, and not the processes or operational practices regulators should follow in creating those regulations. That is not to say the regulatory process is unimportant. Transparency, independence, consistency, and consultation between regulators and regulatees is fundamental to legitimate and effective regulation. However, a detailed exploration of this area is beyond the scope of this dissertation.

For the purposes of this chapter I use the term 'regulation' in the same sense Roger Brownsword used it in his book *Rights, Regulation, and the Technological Revolution*;[134] regulation encompasses whatever measures regulators take to control and channel conduct in a desired way.[135] From education campaigns, to legislation, and everything in-between, as long as the action is taken for the purpose of altering conduct the tool is in the regulator's toolbox. Conceptualising regulation in this way is necessarily broad because regulating technology is a multifaceted issue. A regulator must have great flexibility to address these Rubik-like issues appropriately.

However, it does not follow that a regulator should use whatever tool or tools they desire. A builder does not randomly decide to use a square, handsaw and/or sledgehammer to beat in a nail because that might be a fun, new, or interesting way of fulfilling their duty. If a regulator acts in an arbitrary fashion they risk creating regulation that is at best ineffective, and at worst

---

[134] Roger Brownsword *Rights, Regulation, and the Technological Revolution* (Oxford University Press, New York, 2008) at 7.

[135] This is in line with the generally accepted definition of regulation: see Roger Brownsword & Han Somsen "Law, Innovation and Technology: Before We Fast Forward – A Forum for Debate" (2009) Law, Innovation, and Technology 1 at 8.

harmful. To avoid falling into this trap, I draw on part of Bert-Jaap Koop's *Ten Dimensions of Technology Regulation*.[136] The *Ten Dimensions of Technology Regulation* are a list of relevant issues one can consider in order to better understand their regulatory environment and target.

1. The regulatory problem

While not the first of the *Ten Dimensions of Technology Regulation*, the logical starting point for us is defining the regulatory problem.[137] Most of the heavy lifting required to consider this issue has been done in chapters one and two. In chapter one I argued there will be serious consequences for individuals and society if current disclosure behaviours persist in a world where the IoT is mainstream. The hypothesised consequences can be thought of as symptoms, and disclosure behaviours as the problem.

However, that general problem is not the same as our regulatory problem. In chapter two, I identified the law only has a legitimate interest in regulating disclosure behaviours to the extent that behaviour is contrary to individuals' underlying intentions. Individuals' disclosure behaviours are generally inconsistent with their underlying intentions when they do not properly reflect their privacy concerns. Thus, our regulatory problem can be framed as: what is the best way to help individuals disclose personal information in a manner consistent with their privacy concerns?

2. Normative outlooks

The normative outlooks of a regulator provide the substrata on which regulation is cultivated.[138] As regulation is developed it will reflect those normative assumptions. In turn, those who are affected by the regulation will be influenced by the regulator's normative assumptions. Our regulatory

[136] Bert-Jaap Koops "Ten Dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline" in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds) *Dimensions of Technology Regulation* (Wolf Legal Publishers, 2010).

[137] Koops, above n 136, at 319.

[138] Koops, above n 136, at 317.

problem is directly concerned with behaviour modification, therefore it is critical these assumptions are well-considered.

Our assumptions should be consistent with those that led us to view the symptoms in chapter one, and problem in chapter two, as undesirable. This will help us achieve optimal coordination between the symptoms and regulations charged with preventing them. There are three key assumptions in this respect. First, exclusive control over personal information is fundamental to human autonomy and dignity – a lack of control over personal information is the catalyst for the symptoms discussed in chapter one. Second, individuals need help making rational decisions about their privacy disclosures. This was the subject of the second chapter. Finally, individual liberty is of central importance. This is at the crux of our regulatory goal ensuring individuals are free to make privacy disclosures that accurately reflect their intentions – and the common denominator of all the symptoms described in chapter one.

3. Competing policy considerations

Analysing the policy considerations competing against regulation is not listed as one of the *Ten Dimensions of Technology Regulation*, however it is still an important part of understanding the regulatory environment. While the risks I described in chapter one may lead one interest group to desire regulatory intervention, other stakeholders will be sceptical about the negative effects such intervention could have on their interests. Any regulatory response should be tailored to avoid the perceived risks of regulation from alternative viewpoints as much as possible to ensure more proportional and legitimate regulatory responses.

The potential for regulation to stifle innovation is a juggernaut in the camp against regulation because innovation is incredibly important to virtually everyone. Innovation, particularly with reference to technology, is a driving force behind our species.[139] For example, the Industrial Revolution and all

[139] Morag Goodwin "Introduction. A Dimensions Approach to Technology Regulation" in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds) *Dimensions of Technology Regulation* (Wolf Legal Publishers, 2010) at 1.

of its technological innovations created the shift from a slow-moving world to a modern world "where populations, output and real incomes per head of population [have grown] very quickly".[140]

Regulation directly stifles innovation when it predetermines permissible outcomes of emerging technologies. An active regulator may also discourage investment into research and development within the sector they are focused on because there is a risk of future regulation preventing developed products from being allowed in the marketplace.

However, there is clearly a need to regulate innovation in some instances. From "the first use of a stone as a hammer …the use of tools to adapt and control our environment … has always presented human beings with the possibility of" hammering others, ourselves and the broader environment.[141] Thus, these regulatory efforts must always seek a balance between encouraging and curbing innovation.[142]

At an individual level, companies for whom collecting personal information is a vital part of their business may be concerned about the additional costs of complying with new regulation. Or depending on the nature of the regulation, they may be concerned about how new limitations on their ability to collect personal information will affect their business model. Again, there is precedent for limiting corporate liberty, such as those regulations that prohibit anti-competitive behaviour, and fraud. However, there is always a justifiable reason for prioritising the interests of another over corporate liberty. Therefore, a proportional and legitimate regulatory response will be cautious of limiting this interest where it does not need to, or where it is unjustified.

---

[140] Peter Lane *The Industrial Revolution* (Harper & Row Publishers, New York, 1978) at 5.

[141] Goodwin, above n 139, at 1.

[142] Goodwin, above n 139, at 1.

4. Time and knowledge

The dimension of time is predominantly used to draw attention to different regulatory issues that arise depending on where a technology is in its life-cycle.[143] The IoT is at a relatively early stage in its life-cycle. This has implications for our knowledge about the effects of its large-scale use. I have hypothesised what the risks will be if we do not regulate, in chapter one. However, it will not be until the IoT reaches maturity that we know what the risks to humanity truly are. Regulating now means operating at the edge of evidenced-based decision-making, which makes balancing competing policy considerations difficult. This raises the question: how cautious should our regulatory response be to risks that might not manifest?

As a starting point it is not impermissible or unconstitutional to regulate in advance of material risks. The precautionary principle is recognised as justification for regulatory authorities imposing preventative restrictions where there is still a lack of full scientific certainty about the existence of suspected risks.[144] Our regulatory problem does not require preventative restrictions to be placed on the IoT in the ordinary sense of that phrase; we are not seeking a ban of the IoT. We are merely seeking to ensure individuals are better placed to make decisions consistent with their intentions when asked to disclose personal information in the course of using IoT objects. However, this still represents an intervention in the natural development of the relationship between people and the IoT, and to that extent we should fall back on the core of good sense in the precautionary idea that our interests are not always best served by waiting until the evidence of serious and irreversible damage is overwhelming before we intervene.[145] In other words, we are allowed to be risk-averse.

---

[143] Koops, above n 136, at 315.

[144] See generally Roger Brownsword and Morag Goodwin *Law and the Technologies of the Twenty-First Century* (Cambridge University Press, New York, 2012) at 137 – 167.

[145] Roger Brownsword and Morag Goodwin *Law and the Technologies of the Twenty-First Century*, above n 144, at 166.

In fact, the nature of information technologies means we *should* be risk-averse.[146] Once a technology is well-developed intervention might become expensive or be perceived as drastic.[147] Information technologies generally have fast innovation cycles and consumer uptake,[148] therefore there is a relatively small window of opportunity to regulate in advance of a time that will be met with considerable pushback.

Furthermore, the hypothesised risks in chapter one are serious; autonomy, individuality, and the ability to define and nurture relationships are fundamental human values. The adverse effects on these qualities will potentially be irreversible once we get to a position where there are massive amounts of granular personal information populating private archives with no caveats on future use. This is not an outcome that can be tolerated.

Understanding how the dimensions of time and knowledge have an effect on our regulatory environment raises our awareness to a potential regulatory obstacle; the difficulty of balancing competing policy considerations with incomplete information. However, as the risks associated with our regulatory problem are large and we are not required to respond in an overly intrusive manner it is still reasonable to regulate in advance of those risks materialising. In doing so we must merely remain cognisant that we are at a greater risk of getting the balance wrong and therefore any regulatory approach will need to be innovative enough to respect that risk.[149]

5. Technology, and regulatory location

The location of a technology, together with the location of any regulatory attempt, must be taken into account when determining how to regulate that

[146] The type of technology is another dimension that should be considered: see Koops, above n 136, at 312.

[147] Koops, above n 136, at 315.

[148] Koops, above n 136, at 315.

[149] Koops, above n 136, at 315.

technology.[150] Relevant factors associated with a place will determine what types of regulation are permissible, feasible, and effective.

IoT objects are available globally; however, it is important to note that the place we are attempting to regulate them, New Zealand, makes up a very small portion of the global market's demand for IoT products. That means New Zealand may lack the market power to justify regulation that makes compliance for IoT producers radically different from, and more difficult than, global standards. Producers may perceive it as more efficient to not supply New Zealand with their products, instead of complying with an unusual regulatory regime.

While digital technology is generally a product of virtual space, the IoT is unique because it manifests in tangible objects. For our purposes especially, the IoT only exists in physical space because we are concerned about how people interact with and surrender personal information to physical IoT products. This eliminates the jurisdictional concerns about regulatory targets that operate in the borderless virtual world.[151]

Finally, New Zealand data protection regulation exists within an international context.[152] This international context encourages adherence to a minimum set of standards.[153] As those minimum standards relate to the collection of personal information, collection should generally be fair and lawful. [154] Failure to provide adequate data protection may prevent New Zealand from receiving personal information from other

---

[150] Koops, above n 136, at 314.

[151] Law Commission *Privacy Concepts and* Issues, above n 96, at [6.41].

[152] See Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS 108 (opened for signature 28 January 1981, entered into force 1 October 1985); *The United Nations Guidelines for the Regulation of Computerised Personal Data Files* GA Res 45/95 (1990).

[153] *The United Nations* Guidelines, above n 152, are not legally binding, but asks that governments take them into account in their legislation and administrative regulations; OECD *Guidelines*, above n 152, at [6] are "minimum standards" that should be adopted in each member state's domestic legislation.

[154] OECD *Guidelines*, above n 152, at [7].

jurisdictions,[155] however that does not relate to the collection of personal information within New Zealand. The international instruments are intended to harmonise data protection laws from individual municipalities for the purpose of continuity in cross-border information flows; but this does not have any bearing on the collection of personal information within New Zealand. Therefore, provided any new regulation of personal information collection does not drop below current standards, the international regulatory context is not a regulatory obstacle.

6. Regulation type

We started with a very broad definition of regulation; any measure taken to channel behaviour in a desired way. Now, drawing on my evaluation of the regulatory environment and target, that conception can be narrowed by making some preliminary conclusions about the type of regulation that is or is not consistent with those elements.

A logical starting point is to decide who to regulate. There are two choices; the individual that discloses their personal information, and the agency that collects that personal information. While our regulatory problem is about the modification of disclosing behaviour, it is not about *regulating* disclosing behaviour because it is not our desire to channel that behaviour towards a specific outcome. Rather, our intention is to empower individuals to act in any way they desire, as long as it is consistent with their true intentions. Thus, to regulate the individual would conflict with our regulatory problem, and our normative assumption about the importance of individual liberty. The logical focus of regulation should be the collector of personal information.

Next, it is important to consider how regulators should engage with regulatees – termed regulatory pitch by Rodger Brownsword.[156] Essentially, this relates to what sense of reasoning regulators try to appeal to, and what

[155] Regulation (EU) 2016/279 on General Data Protection Regulation [2016] OJ L119/1, part 9 imposes restrictions on the transfer of personal data from EU states to states outside the EU that lack adequate data protection safeguards.

[156] Brownsword *Rights, Regulation, and the Technological Revolution*, above n 134, at 16.

sense of reasoning is the basis for the regulatee's conformation. Given the conflicting policy consideration of corporate liberty, the most appropriate regulatory pitch is to appeal to the ideas of what makes practical sense to companies. This forces a basic commitment from regulators to act in both parties' libertarian interests.

Closely related to regulatory pitch, is regulatory range. The regulatory range describes how regulation seeks to channel conduct: so that x is done (positive channelling), so that x is not done (negative channelling), or so that agents have a choice between doing x or not doing x as they prefer (neutral channelling).[157] It is clear neutral channelling is inappropriate, because the incentive for companies to collect personal information is too great. After all, organisations already have a broad discretion over how to collect personal information and, I have argued, use that discretion to elicit personal information in ostensibly unfair ways. Negative channelling would also be inappropriate, given that preventing conduct creates a greater risk of stifling innovation. Positive channelling is the most ideal form of regulatory range, because it nudges conduct in the desired direction without closing any doors to innovation. However, any positive channelling will need to be soft, because creating additional compliance measures that are too burdensome will deter businesses from bringing their products to the New Zealand market.

Regulatory tilt refers to the default position set by regulators [158] The options for regulatory tilt are binary in this instance, either: collection is permissible until it is not; or, collection is prohibited unless regulatory obstacles are overcome. It is clear the tilt should be towards the latter option, because our normative assumptions put a premium on exclusive control over personal information.

The last preliminary conclusion to be drawn from my evaluation of the relevant regulatory environment is that regulation needs to be soft and

[157] Brownsword *Rights Regulation, and the Technological Revolution*, above n 134, at 19.

[158] Brownsword *Rights, Regulation, and the Technological Revolution*, above n 134, at 21.

incredibly flexible. Regulation needs to be soft because of the lack of knowledge we have about the risks of failing to regulate. However, the IoT's fast innovative cycle and consumer uptake means that knowledge about those risks should grow exponentially. Regulation needs to be sufficiently flexible to cater to these changing circumstances. To this extent, a classic command and control type regulation is unlikely to be suitable on its own; innovative solutions should be pursued.

7. Smart regulation

I offer three classes of suggestion that are intended to operate in conjunction. The first two classes are suggested amendments to the Act. The third is for a specialist body dedicated to informing the producers of IoT objects about privacy enhancing design. This follows the "smart regulatory" approach advocated for by Neil Gunningham and Peter Grabosky.[159] They argue single instrument "approaches [to regulation] are misguided, because all instruments have strengths and weaknesses; and because none are sufficiently flexible and resilient to address all … problems in all contexts".[160] Instead, "a better strategy will seek to harness the strengths of individual mechanisms while compensating for their weaknesses by the use of additional and complimentary instruments".[161] This multi-layered approach to regulation is especially necessary where we have such a complex regulatory environment and target.

B. Paint Over the Cracks

The first aspect of my suggested regulatory solution involves ameliorating the elements of the Act I identified in chapter two as having become disconnected from the IoT. These are all elements that either affect the operation of the Act, or provide safety to individuals at the margins of the

[159] Neil Gunningham and Peter Grabosky *Smart Regulation: Designing Environmental Policy* (Oxford: Clarendon Press, New York, 1998).

[160] Neil Gunningham and Peter Grabosky, above n 159, at 14.

[161] Neil Gunningham and Peter Grabosky, above n 159, at 14.

collector/discloser relationship. This aspect does not address the mechanics of the decision to disclose personal information.

1. *Fixing the definition of "collect"*

In chapter two, I explained that it is uncertain whether the definition of "collect" includes predictions based off data that has been collected. I suggest the definition of "collect" in the Act should be amended to explicitly include this situation.

2. *Fixing protection at the margins*

In chapter two, I explained the requirement to collect personal information for a legitimate purpose may not limit the collection of personal information, because under the current construction of principle one it is possible to offer collection itself as a legitimate purpose of collection. It is important that this limitation operates as an effective constraint on indiscriminate collection by the IoT because of the difficulty the IoT creates for giving information to its users. More robust protection at the margins is required to make up for that deficiency. I suggest for the IoT, legitimate purposes should only be those that are necessary to make the particular IoT product function.

I also identified the possibility of interpreting the prohibition on unfair collection practices in principle four to include a prohibition on the manipulation of notice and consent regimes. I suggest a best practice guideline should be developed about how to give notice to, and obtain consent from users of IoT products. While failure to comply with this guideline would not make collection unfair and in violation of principle four *per se*, it would create a certain base to judge alternative collection practices against. The further a collection practice strays from the guideline, the more likely it is to be considered unfair and in breach of principle four. This would make unfair manipulation more certainly within the scope of principle four's protection.

Adherence to this guideline could also qualify organisations to certify themselves as compliant with fair information collection practices. The guideline would act as an incentive for companies to adhere to fair

information collection practices so they can identify as transparent and trustworthy entities.

3. *Fixing remedies under the Act*

In chapter two, I identified that it is very rare for harm as it is defined in the Act to result from a breach of principles one to four. Therefore, the Principles are largely aspirational, and do not have the teeth to protect individuals from breaches in most instances. It is important to recognise the intangible harm that can be done by collecting personal information against an individual's free will, and to provide a deterrent from causing that harm. Therefore, I suggest conduct which breaches the first four privacy principles should not require any related harm element to trigger enforceable rights under the scheme of the Act.

Where possible, my suggestions have incorporated the type of regulatory tools that best reflect the regulatory environment we are operating within. For example, in regards to clarifying what is unfair for the purposes of principle four I could have suggested a mandatory definition. However, a best practice guideline is more suitable because it is not a form of negative channelling. Furthermore, it appeals to the practical sensibilities of organisations.

One place I did use negative channelling is in my suggested amendment to principle one. The effect of this recommendation, together with an expanded definition of "collect", is that an organisation would no longer be able to make predictions about individuals for any reason they want. This does limit future innovation to an extent. However, the approach I have taken does not completely stifle innovation. Organisations are still free to make predictions about individuals as long as those predictions relate to the function of the particular IoT product the original data was collected from. Such predictions may relate to the improvement of that product, and user experience. Therefore, this solution represents a balance between the competing policy considerations of innovation and protecting individuals from disclosing information that conflicts with their privacy concerns.

C. Redesign Notice and Consent

This aspect of my suggested regulatory solution relates more directly to the mechanics of personal information collection. It involves rethinking how companies can use the notice and consent regime, with the goal of trying to prevent them from leveraging cognitive biases to take advantage of that scheme. That contributes to solving our regulatory problem because it will remove some of the obstacles individuals face when trying to make disclosures that are consistent with their privacy concerns.

Clearly we need to prevent companies from using manipulative design, however there are challenges to preventing manipulative design within this regulatory environment. The first challenge is our commitment to positive channelling. It is particularly important to respect this commitment here, because prohibiting certain designs has direct implications on corporate liberty and innovation. Secondly, positive channelling in the context of mandating certain designs comes with the risk of creating regulatory obstacles that deter producers from bringing their products to the New Zealand market.

In light of these boundaries, the best way to approach the issue of preventing manipulative design is through positive nudging – that is to say, not mandating good design procedures, but encouraging them. My suggestion is two-fold. First, we should remove the application of principles two and three to the IoT and replace them with a model based on the EU General Data Protection Regulation, which simply requires consent as a lawful basis for collecting personal information.[162] This new requirement would read:

> Without limiting principle one, using the Internet of Things to collect personal information shall be lawful only if and to the extent that the individual has given consent to the collecting of his or her personal information.

[162] Regulation (EU) 2016/279 on General Data Protection Regulation [2016] OJ L119/1, article 6. It is acknowledged consent is not the only lawful basis for data collection under article 6. However, for the purposes of this regulatory suggestion I only rely on article 6 as a model to the extent that consent is a lawful basis for collection.

Second, we should define what consent means in this context. Currently, there is no guidance as to what constitutes an agreement between collector and discloser. In determining what promise has been made to a discloser it is normal to only look to the terms of use agreement or to the privacy policy.[163] This ignores the function of design. I have argued there are many design features that signal privacy expectations to a discloser. Thus it is critical design signals and transaction costs are considered to be part of any promise a discloser is said to have consented to, and this should be incorporated into the definition of consent.

This two-fold suggestion reflects the desired regulatory tilt against collection, until collection is permissible. The suggestion is also grounded in soft positive channelling. Producers are nudged towards using design that accurately reflects what information will be collected from an individual and how that information will be collected because design features are reconceptualised as part of the promise made to consumers. At the bare minimum, it prevents design being used to undermine or mislead privacy expectations.

D. Establish a Specialist Technology and Design Body

Earlier I suggested a best practice guideline should be developed for how to give notice to, and obtain consent from users of IoT products, and that an associated certification for compliance with that guideline should be created. This suggestion is that a specialist body should be established to control that guideline, and perform other regulatory functions that make privacy enhancing design more accessible to technology producers.

1. Oversight of the best practice guideline

It is necessary that there is continuous regulatory oversight of the best practice guideline. First, there is uncertainty as to how those affected by it will initially respond. If the guideline does not induce the desired response from producers of IoT objects, or if it does but it transpires the guideline is

[163] Hartzog, above n 13, at 169.

not strong enough to empower consumers with better control over their privacy disclosures, then the standard needs to be responsive to those issues in the first instance. Secondly, as the technology evolves, and certain market players or researchers come up with innovative ideas about how to deliver notice to, and obtain consent from users of IoT products, the concept of best practice will change. The standard needs to be responsive to those ongoing developments too.

2. *The provision of education*

Over and above having responsibilities for maintaining that guideline, the specialist body should have the mandate to perform research, and offer education to companies on how to implement better notice and consent practices. A similar function is carried out by the Federal Trade Commission (**FTC**) in the United States. Speaking on the role of the FTC in consumer privacy protection David Vladeck, former Director of the FTC Bureau of Consumer Protection, outlined how they have been encouraging "companies to design innovative ways – apart from privacy policies – to inject greater transparency in their interactions with consumers".[164] This represents part of the FTC's commitment "to increasing transparency for consumers … so that they will have the tools necessary to make meaningful, informed choices".[165]

Education is a necessary function for the specialist body to perform because the incentive for companies to come up with better ideas themselves for giving notice to, and obtaining consent from individuals, is small. By reinventing consent I have attempted to provide some positive channelling towards giving better quality notice to consumers of IoT products. However, the challenge of how to do this in practice is still a difficult one that will require companies to commit resources towards coming up with a solution they do not really want to provide. By offering existing solutions that can

[164] David Vladeck, Director FTC Bureau of Consumer Protection "The Role of the FTC in Consumer Privacy Protection" (Washington DC, 8 December 2009).

[165] David Vladeck, above n 164.

be easily implemented the specialist body can break down some of the barriers companies face in this mission.

Even by simply keeping an eye on international trends the specialist body could provide innovative suggestions about how to deliver better notice to consumers of IoT products. At one point, California's Senate Bill 327 would have required manufacturers who sell connected devices to design those devices to indicate through audio or visual signals when they are collecting information.[166] This could be easily adapted into an implementable suggestion, such as that manufacturers design their products with a small LED light that turns on when the device is collecting personal information. One can imagine how this might be effective in resolving some of the privacy paradox's issues by increasing the accessibility to, and tangibility of privacy warnings; I am sure most people would be alarmed to see the light on their Alexa never turn off.[167]

3. The provision of resources

In addition to providing education to manufacturers of IoT products, this specialist body could further break down the barriers companies face in their mission to provide better notice to consumers by offering them resources. For example, a website that technology manufacturers could plug their software into could be developed. That website could have a dedicated page for each IoT object, accessible only through a unique code on each object, which displays a simple list of information that has been collected from that object in descending order of sensitivity. By not only offering suggestions, but resources too, the specialist body can guide companies towards providing users of the IoT with better quality information that will help them make decisions consistent with their privacy concerns.

---

[166] Information Privacy: Connected Devices 2017-2018 (SB-327, version: 17 May 2017), s 1(2)(a); for a description of that version of the Bill, see Douglas Bonner and Womble Carlyle "California Bill Mandates Privacy By Design for IoT Devices" *Mondaq Business Briefing* (online ed, Washington, 27 April 2017). The Bill does not include this requirement, in its current form.

[167] Alexa is a virtual assistant designed by Amazon, which exists within a portable speaker; see Geoffrey A Fowler "Hey Alexa, come clean about how much you're really recording us: *The Washington Post* (online ed, Washington, D.C., 24 May 2018).

4. *Oversight of the remedial process*

Finally, the specialist body should also be responsible for making damages recommendations to the Human Rights Review Tribunal in the event an interference with privacy occurs. They should have the discretion to reduce the penalties for companies that have implemented privacy enhancing design suggestions, promise to implement them in the future, or otherwise contribute to the privacy by design discussion. This creates a practical pitch to companies to engage with and utilise the specialist body.

.

Conclusion

The IoT is expanding at a phenomenal rate. Its reach into various aspects of human life is growing ever greater, and the information it gathers increasingly comprehensive. Underpinning this growth is the lucrative data economy, which is motivating producers of the IoT to collect as much personal information as possible through their products.

The benefits of the IoT are all too tangible. We lead increasingly busy and complex lives; the appeal of products that help us to save time, access information and more generally benefit our quality of life is undeniable. However, as I have discussed, the price we pay for immediate gratification and convenience by tapping into the IoT may be greater than we think.

In chapter one I discussed some of the various risks that the IoT poses to individuals and society. The most imminent of those risks are to personal autonomy, individuality, and the ability to define and nurture relationships. I also discussed the worst-case scenario, which is a world in which societies' ability to maintain strong liberal democracies, or any liberal government at all, is severely compromised. And these are only the risks that have been identified to date; there will inevitably be as yet unknown risks.

These risks are caused by the current behaviour of individuals, who disclose personal information without attempting to limit its future use. In chapter two I argued that this is not a product of individuals' free will, but rather an inability to properly take into consideration privacy concerns in the moment of making these decisions. Both the context in which these decisions are made, and cognitive biases contribute to that dilemma.

While the law may not (and most would agree should not) have the mandate to ensure individuals make more sensible disclosure decisions, at the very least it ought to create an environment that enables individuals to do so if they wish. The law is currently failing in this regard. As it stands, the Act fails to recognise individuals need help to make disclosures that are consistent with their privacy concerns; is too narrow to catch some of the most damaging information collection; provides illusory support at the

margins of the collector/discloser relationship; utilises an archaic notice and consent regime which is open to manipulation, unfit for the IoT and deficient at helping individuals with disclosures; and only lends support where harm has been done. Consequently, individuals are left with the responsibility of protecting their privacy while being ill-equipped to handle that burden, and manufacturers of IoT products are left free to package privacy information in a way that takes advantage of individuals' myopic tendencies.

The law needs to better support individuals to make privacy disclosures that are consistent with their true intentions. However, given the nature of this issue an appropriate regulatory solution cannot be radical. The IoT is still early in its product-cycle, there is a risk harsh regulation will stifle innovation and corporate liberty, and the potential to deter manufacturers from bringing their IoT products to the New Zealand market if compliance is too burdensome. Therefore, regulation must be principled, flexible and straightforward. My proposed solution is to fix the problems with the current law, redesign notice and consent, and create a specialist body that can be a resource to support privacy enhancing design.

The mainstreaming of the IoT will be revolutionary. It has the potential to make enormous and positive transformations to our homes, businesses, cities, and planet. However, if we continue to disclose personal information without limiting its future use then the IoT may also result in negative transformations to human nature, and our political system. At the speed the IoT is developing the implications of the IoT must be considered now rather than later. Early engagement and robust discussion will allow us to shape and harness the power of the IoT before it has the opportunity to shape us.

To return to the quote that began this dissertation, in George Orwell's *1984*, Winston Smith was unable to turn off the telescreen that observed every aspect of his life. We are choosing not to, and changing that behaviour now is the first step towards avoiding an IoT dystopia.

BIBLIOGRAPHY

A. Cases

1. New Zealand

Boyle v Manurewa RSA Inc [2003] NZHRRT 16.

C v Holland [2012] 3 NZLR 672 (HC).

Hosking v Runting [2005] 1 NZLR 1 (CA).

Marfart v Television New Zealand [2006] 3 NZLR 534 (CA).

R v Alsford [2017] NZSC 42, [2017] 1 NZLR 710.

B. Legislation

1. New Zealand

Privacy Act 1993.

2. Europe

Directive COM/2015/0634 on certain aspects concerning contracts for the supply of digital content.

Regulation (EU) 2016/279 on General Data Protection Regulation [2016] OJ L119/1.

3. Bills

New Zealand

Privacy Bill 2018 (34-1).

United States of America: California

Information Privacy: Connected Devices 2017-2018 (SB-327, version: 17 May 2017).

C. Treaties

The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS 108 (opened for signature 28 January 1981, entered into force 1 October 1985).

D. Books and Chapters in Books

Adam Greenfield *Radical Technologies* (Verso, London, 2017).

Alan F Westin *Privacy and Freedom* (Bodley Head, London, 1970).

Alessandro Acquisti and Jens Grossklags "What can behavioural economics teach us about privacy" in Acquisti and others *Digital Privacy: theory, technology, and practices* (Auerbach Publications, 2007) 363.

Bert-Jaap Koops "Ten Dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline" in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds) *Dimensions of Technology Regulation* (Wolf Legal Publishers, 2010) 309.

Christian Flender and Gunter Muller "Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited" in Jerome R Busemeyer and others (eds) *Quantum Interaction: 6th International Sympnosium* (Springer-Verlag Berlin, Heidelberg, 2012)

Jeremy Bentham, *The Works of Jeremy Bentham* (William Tait, Edinburgh, 1843).

Mike Kuniavsky *Smart Things: Ubiquitous Computing User Experience Design* (Elsevier, 2010).

Morag Goodwin "Introduction. A Dimensions Approach to Technology Regulation" in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds) *Dimensions of Technology Regulation* (Wolf Legal Publishers, 2010) 1.

Neil Gunningham and Peter Grabosky *Smart Regulation: Designing Environmental Policy* (Oxford: Clarendon Press, New York, 1998).

Paul Slovic and others "The Affect Heuristic" in Thomas Gilovich and others *Heuristics and Biases* (Cambridge University Press, Cambridge, 2002) 397.

Peter Lane *The Industrial Revolution* (Harper & Row Publishers, New York, 1978).

Robert O'Harrow *No Place to Hide* (Free Press, New York 2005).

Roger Brownsword and Morag Goodwin *Law and the Technologies of the Twenty-First Century* (Cambridge University Press, New York, 2012).

Roger Brownsword *Rights, Regulation, and the Technological Revolution* (Oxford University Press, New York, 2008).

Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (Oxford University Press, Melbourne, 2005).

Woodrow Hartzog *Privacy's Blueprint* (Harvard University Press, Massachusetts, 2018).

E. Journal Articles

Afzal A Zaidi Sar and others "The Cognitive Internet of Things: A Unified Perspective" (2015) 20(1) Mobile Networks and Applications 72.

Charles Fried "Privacy" (1968) 77 Yale LJ 475.

Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

Edward J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYU L Rev 962 at 1003.

Gaochao Xu and others "Research on the Internet of Things (IoT)" (2013) 160(12) Sensors & Transducers 463.

Haein Lee, Hyejin Park and Jinwoo Kim "Why do people share their context information on Social Network Services? A qualitative study and an experimental study on user's behaviour of balancing perceived benefit and risk" (2013) 71(9) Int J Hum Comput Stud 862.

Hichang Cho, Jae-Shin Lee and Siyoung Chung "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience" (2010) 26 Comput Hum Behav 987.

Howard W Waltzman and Lei Shan "The Internet of Things" (2015) 27(7) Intellectual Property & Law Journal 19.

Irene C.L. Ng and Susan Y.L. Wakenshaw "The Internet-of-Things: Review and research directions"(2017) 34(1) IJRM 3.

Julie E Cohen “What is Privacy For” (2013) 126 Harv L Rev 1904.

Neil M Richards “The Dangers of Surveillance” (2013) 126 Harv L Rev 1934.

Nina Gerber, Paul Gerber and Melanie Volkamer “Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour” (2018) 77 Computers & Security Journal 226.

Norbert Schwartz and others “Ease of Retrieval as Information: Another Look at the Availability Heuristic” (1991) 61 J Person Social Psychol 195.

Oren Smilansky “Companies gear up for the IoT revolution: there’s rising consumer demand for – and acceptance of – connected devices” (2015) 19(3) CRM Magazine 18.

Roger Brownsword & Han Somsen “Law, Innovation and Technology: Before We Fast Forward – A Forum for Debate” (2009) Law, Innovation, and Technology 1.

Ronald Bailey “Your Cellphone is Spying on You” (3013) 44(8) Reason 35.

Ryan Calo “Code, Nudge, or Notice?” (2014) 99 Iowa L Rev 773.

Scott R. Peppet “Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent” (2014) 93(1) Tex L Rev 85.

Scott R Pepett “Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future” (2011) 105 NW U L Rev 1153.

Spyros Kokolakis “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon” (2017) 64 Computers & Security 122.

F. Parliamentary and Government Materials

Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008).

Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2010).

G. Papers and Reports

Albert Opher and others "The rise of the data economy and monetization" IBM <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12367USEN>.

Alessandro Acquisti and Jens Grossklags *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior Proceedings of the second annual workshop on economics and informational security* (WEIS, 2003).

Barry Brown *Studying the Internet Experience* (HP Laboratories Bristol, Technical Report HPL-2001-49, 26 March 2001).

Capgemini *Big & Fast data: The Rise of Insight-Driven Business* (Capgemini, 10 March 2015).

Dave Evans *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything* (CISCO, April 2011).

Jayne Van Souwe and others *Australian Community Attitudes to Privacy Survey 2017* (Office of the Australian Information Commissioner, May 2017).

Mary Madden and others *Public Perceptions of privacy and security in a psot-snowden era* (Pew Research Center, 2014).

Symantec *State of Privacy Report 2015* (Symantec, 2015).

H. *International materials*

Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

The United Nations Guidelines for the Regulation of Computerised Personal Data Files GA Res 45/95 (1990).

I. Newspaper and Magazine Articles

Alex Hern "Google 'working on censored search engine' for China" *The Guardian* (online ed, London, 2 August 2018).

Alexander Wolfe “Little MEMS Sensors Make Big Data Sing” *Forbes Magazine* (online ed, New York, 10 June 2013).

Carole Cadwalladr and Emma Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" *The Guardian* (online ed, London, 17 March 17 2018).

Cecilia Kang “Facebook Faces Growing Pressure Over Data and Privacy Inquiries” *The New York Times* (Online ed, New York, 20 March 2018).

Douglas Bonner and Womble Carlyle “California Bill Mandates Privacy By Design for IoT Devices” *Mondaq Business Briefing* (online ed, Washington, 27 April 2017).

Geoffrey A Fowler “Hey Alexa, come clean about how much you’re really recording us: *The Washington Post* (online ed, Washington, D.C., 24 May 2018).

Jane Bainbridge “Meet Kevin Ashton, the man behind the internet of things” *Campaign* (online ed, London, 29 April 2014).

Julia Carrie Wong “Mark Zuckaberg apologises for Facebook’s ‘mistakes’ over Cambridge Analytica” *The Guardian* (online ed, London, 22 March 2018).

Kashmir Hill “Hot Target Figured Out a Teen Girl Was Pregnant Before Her Father Did” *Forbes Magazine* (online ed, New York, 16 February 2012).

Kathleen Chaykowski “Mark Zuckaberg: 2 Billion Users Means Facebook’s ‘Responsibility Is Expanding’ *Forbes Magazine* (online ed, New York, 27 June 2017).

Kevin Ashton “That ‘Internet of Things’ Thing” *RFID Journal* (online ed, Melville, 22 June 2009).

Maria Farrell “The Internet of Things – Who Wins, Who Loses?” *The Guardian* (online ed, London, 14 August 2015).

Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr "How Trump Consultants Exploited the Facebook Data of Millions" *The New York Times* (online ed, New York, 17 March 2018).

Owen Bowcott and Alex Hern “Facebook and Cambridge Analytica face class action lawsuit” *The Guardian* (online ed, London, 10 April 2018).

Rob Davies and Mark Sweney “Betting firms could be fined over ads ‘targeting vulnerable people’” *The Guardian* (online ed, London, 13 September 2017).

"The world's most valuable resource is no longer oil but data" *The Economist* (online ed, London, 6 May 2017).

J. Internet Resources

Amazon “Amazon Dash Button” Amazon < https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011>.

John Hancock *Vitality Active Rewards with Apple Watch* John Hancock < https://www.johnhancockinsurance.com/vitality-program/apple-watch.html>.

Mimo < https://www.mimobaby.com/>.

Paul Roth “Report on Aspects of Privacy Compliance & Practice of NZ Post Lifestyle Survey 2009 Privacy Act Perspective” (20 June 2011) Office of the Privacy Commissioner <privacy.org.nz/reports-on-aspects-of-privacy-compliance-and-practice-of-the-nz-post-lifestyle-survey-200/>.

Progressive “Snapshot” Progressive <https://www.progressive.com/auto/discounts/snapshot/>.

Rudolf Van der Berg “Smart Networks: Coming Soon to a Home Near You” (21 January 2013) OECD Insights <http://oecdinsights.org/2013/01/21/smart-networks-coming-soon-to-a-home-near-you/>.

Shahid Ahmed “Digital Revolution Summit: The Six Forces Driving the Internet of Things” PWC <https://www.pwc.com/gx/en/technology/pdf/six-forces-driving-iot.pdf>.

Suzanne Barlyn “Strap on the Fitbit: John Hancock to sell only interctive life insurance” (20 September 2018) Yahoo!

<https://finance.yahoo.com/news/strap-fitbit-john-hancock-sell-141135104.html>.

UVeBand <http://www.uveband.co.uk/>.

Vitality *Vitality Active Rewards: Apple Watch* Vitality <https://www.vitality.co.uk/rewards/partners/active-rewards/apple-watch/>.

K. *Interviews*

Scott Peppet, law professor at the University of Colorado Law School (Danny Vinik, The Agenda, 29 June 2015) transcript provided by Politico <https://www.politico.com/agenda/story/2015/06/how-to-regulate-iot-scott-peppet-interview-000112>.

L. *Speeches*

David Vladeck, Director FTC Bureau of Consumer Protection "The Role of the FTC in Consumer Privacy Protection" (Washington DC, 8 December 2009).

M. *Press releases*

Facebook "Facebook Reports First Quarter 2018 Results" (press release, 15 April 2018).

Privacy Commissioner "Privacy concerns on the rise – public survey" (press release, 7 May 2018).