EX ANTE VERSUS EX POST: REGULATING THE DIGITAL ECONOMY

Raffaele Darroch

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

October 2019

CONTENTS

Acknowledgements…… 5

Chapter 1: Challenges and Opportunities of the Digital Economy…….. 7

Introduction……. 7

A: Common themes…… 9

New Zealand and European Legislation…… 9

Organisations within the digital economy…… 10

Personal Information…… 10

The Surveillance Capitalism model…… 11

Findings of the Workshop Report…… 12

Merging areas of law…… 13

Bundeskartellamt prohibitions on Facebook…… 13

B: Opportunities…… 14

Implications for New Zealand…… 14

Benefits…… 15

C: Line of argument…… 17

Chapter 2: Market Dominance…… 20

A: Dominance in Digital Markets…… 20

Market Concentration…… 20

Zero Costs…… 21

The Importance of Data…… 23

Network and Lock-in effects…… 24

Mergers…… 27

Competing incentives…… 28

B: Summing up…… 28

Chapter 3: Personal Data Mobility…… 30

A: Moving forward…… 30

B: Data Portability…… 31

Discussion on Data Portability inclusion within the Privacy Bill…… 31

GDPR Interpretation of Data Portability…… 32
Portability in practice…… 33
Challenges…… 35
C: Data Mobility…… 36
UK Initiative…… 36
Challenges…… 37
Open Banking…… 39
Opportunities…… 40
Chapter 4: Data Protection…… 42
A: Data Protection frameworks relating to personal data disclosures… 42
Traditional approaches…… 43
Criticism of traditional collection and consent-based frameworks…… 46
B: Improper uses of personal data…… 50
Cambridge Analytica…… 50
Unknown threats…… 52
C: Modern Enforcement mechanisms…… 52
Chapter 5: Privacy By Design…… 55
A: Design importance and manipulation…… 55
Importance of design…… 55
Design methods used by digital companies…… 57
B: Setting standards for Privacy By Design…… 60
Fundamental aspects of design…… 60
Trustworthiness…… 61
Autonomy…… 63
Obscurity…… 64
Summing Up…… 64
Chapter 6: Digital Markets Unit and Adequacy…… 66

Conclusion…… 69
BIBLIOGRAPHY…… 71

ACKNOWLEDGEMENTS

To my supervisor, Associate Professor Colin Gavaghan, thank you for your guidance and patience throughout this year.

To Professor Paul Roth, for your feedback and interest in this topic.

To my friends and family for their support and encouragement.

Lastly, to all the people I have met at Otago that made my time here special.

EX ANTE VERSUS EX POST: REGULATING THE DIGITAL ECONOMY

Chapter 1: The Challenges and Opportunities of the Digital Economy

INTRODUCTION

The central research question of this paper is as follows. What is the best way to promote societies' interests through the use of their data? This is, of course, a lofty goal. My propositions merely seek to point regulators towards areas of research that previously may not have been given much thought. I will also suggest various competing interests must be accounted for when answering this question. I will elaborate upon these below. Primarily, the discussion will be concerning the digital economy and the way companies within these digital markets use the personal data of individuals. A recent joint research project by the Australian and New Zealand Productivity Commissions' defined the digital economy as the "economic activities conducted or facilitated through digital computing technologies. In modern economies … increasingly synonymous with the entire economy."[1]

Importantly, business models within the digital economy often rely on the storage and accumulation of data to achieve dominance. An increasingly seen phenomenon is that several large companies may dominate any single digital market. Frequently labelled as the 'Big Four' of the tech moguls, it is arguable that, in the future, companies like Google, Amazon, Facebook and Apple (the GAFA's) will only continue to have an increasingly powerful influence on

[1] Australian Productivity Commission and New Zealand Productivity Commission *Growing the digital economy in Australia and New Zealand.* Maximising opportunities for SMEs, Joint Research Report, (January 2019), at 9.

individuals.[2] This is in large part due to the amounts of personal data that they store for their exclusive use. Even the creator of the World Wide Web, Sir Tim Berners-Lee, has expressed concerns that their dominance has led to power imbalances. These imbalances allow these companies and others like them to act with little regard for the negative consequences their actions may have for society as a whole.[3] Of course, there is nothing new about businesses seeking to understand their customers' preferences. However, the sheer amounts of data that digital companies collect is unprecedented. Furthermore, the core feature of data's value to their business models is distinctive.[4]

It should be noted that the digital economy poses many novel issues for regulators that will not be discussed. In the future, it may need legislation dedicated solely to it. The recent Workshop report, funded by the New Zealand Law Foundation, Digital Threats to Democracy, suggested that policies should be reframed to focus upon collective impacts, as opposed to primarily protecting individual rights and privacy.[5] I would argue that the most dominant companies in the digital economy pose the greatest concerns for society. Why? Because they collect and store the largest amounts of personal data. This gives them the ability to exclude other companies and attain more users through network effects. Thus, it is this data that gives them their market power. So that when data is used for an improper purpose, it can have detrimental effects not only for any given individual's privacy but also for democracy itself.

---

[2] British and Irish Legal Education and Technology Association (BILETA) (IRN0029) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019" at 8.

[3] Sir Tim Berners-Lee "One Small Step for the Web…" <https://medium. com/@timberners_lee/one-small-step-for-the-web-87f92217d085>.

[4] Jason Furman and others *Unlocking Digital Competition* (Digital Competition Expert Panel, March 2019), at 29.

[5] Marianne Elliott and others *Digital Threats To Democracy* (The Workshop, May 2019), at 34.

On this basis, I will propose that the objectives of competition law should also be accounted for, even when considering data protection issues. Promoting competition in markets for the long term benefit of consumers[6] can also be achieved while protecting personal data rights. The two seem to move together in the digital economy, as individuals use services that result in the exchange of personal information. As they are competing interests, regulating competition in the digital economy should also result in safer environments for the protection of data.

A: Common themes

New Zealand and European Legislation

In March of this year, the CEO of Facebook Mark Zuckerberg stated that there was a need for government and regulators to take a more active role in the regulation of the digital economy.[7] Anticipating the need for the digital economy to transition from self to co-regulation, the response of the European Union (EU) came into force one year earlier, on the 25th of May 2018, in the form of the General Data Protection Regulation (GDPR). The aim of which is to give individuals control over their personal data by enforcing stringent data protection standards. The New Zealand Government is also in the process of amending the Privacy Act 1993. The Privacy Bill is currently passing through the Committee of the Whole House.[8] It re-enacts the twelve information privacy principles, retaining its flexible nature with several notable changes (IPP's). Section 3 of the new Bill sets out its purpose, to "provide a framework for protecting an individual's right to privacy .. recognising that other rights and interests may need to be taken into account … and giving effect to

---

6 Purpose of the Commerce Act 1986, s 1(A).

7 "Mark Zuckerberg calls for stronger regulation of internet" *The Guardian* (online ed, London, 30 March 2019).

8 Privacy Bill (34-2) 2018 (as of the 18th of September 2019).

internationally recognised privacy obligations and standards in relation to the privacy of personal information."[9] It entails a more modest approach relative to the EU's direction through the GDPR. While the Bill remains focused on a principles-based approach, it does impose stricter accountability mechanisms. It also aims to support the earlier identification of privacy risks.[10]

Organisations within the digital economy

Companies or organisations within the digital economy will be referred to interchangeably. These are the companies that collect and use personal data, referred to as agencies[11] in New Zealand legislation and data controllers[12] under the GDPR respectively.

Personal Information

Throughout this paper, the discussion of "data" used by digital companies will be referenced. For the following analysis, personal data takes on the meaning given by the relevant legislation. In the Privacy Bill, personal information is defined expansively, as anything that could be referred to as personal information.[13] This scope is deliberately set out to include as many collections of information as possible, with some exceptions. Similarly, the GDPR's interpretation of 'personal data,' is any information related to an identified or identifiable natural person.[14] It should be noted that the scope of personal

[9] Privacy Bill 2018, s 3(a) and (b), Purpose of this Act.

[10] Ministry of Justice *Departmental Report - Part One, Privacy Bill* (13th March 2019), at 6.

[11] Privacy Bill 2018, s 6.

[12] General Data Protection Regulation 2018, Article 4(1).

[13] Privacy Bill 2018, s 6.

[14] General Data Protection Regulation 2018, Article 4(1).

information is itself a contested topic, but not one that will be discussed in detail within the following analysis.[15]

The Surveillance Capitalism Model

Personal data is an inherent part of the business model that dominates the digital economy. This business model has been referred to as "surveillance capitalism."[16] It was invented by Google, whose engineers found that words that were entered into search boxes by individuals could be aggregated to predict what those individuals wanted. Those predictions could then be sold to other companies. They could then target users with advertising based upon these predictions.[17] Later, this approach was extended from the parent company to its other subsidiaries, namely Gmail and YouTube.[18] It is now used by Facebook, Amazon and LinkedIn, along with many others that offer free services. Just one way of monetising that data is through advertisements that target commercial messages at users.[19]

Firstly, companies collect and store large amounts of data regarding the behaviours of individuals. Some of this data comes from personal information that is voluntarily supplied.[20] The data is then inputted into machine learning algorithms. These aim to infer insights from users as to their future

---

[15] See, for example, the obiter remarks made by Tipping J. These suggest favouring a narrower approach to the scope of personal information, made in the case of *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 at paragraph [23].

[16] Shoshana Zuboff *The Age of Surveillance Capitalism* (Hachette Book Group, New York, 2019), at 13.

[17] Jennifer Cobbe and Professor John Naughton, Trustworthy Technologies Strategic Research Initiative, University of Cambridge (IRN0031) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019" at 2.

[18] Cobbe, Naughton, above n 17, at 2.

[19] Jennifer Cobbe "Reigning in Big Data's Robber Barons" *NYR Daily* (online ed, New York, 12 April, 2018).

[20] Cobbe, above n 19, at 2.1.

behaviours.[21] Lastly, behavioural nudging through targeted advertising is used to direct user behaviour in the direction these companies desire. Facebook, for example, sells access to knowledge about users through predictive analytics and experimentation, to other companies, political parties and candidates.[22] These links are often determined algorithmically to provoke the desired behaviour from the user. Often, they make use of known shortcuts in human decisions making (or heuristics).[23] In the words of Shoshana Zuboff, "surveillance capitalists know everything about us, whereas their operations are designed in such a way to be unknowable to us".[24] She suggests that this new market form prioritises selling predictions of individuals behaviour, rather than serving the genuine needs of people.[25]

Findings of the Workshop Report

A recent report funded by the New Zealand Law Foundation argues that these companies have avoided responsibility for the impact that their business models may have, particularly concerning the collective wellbeing of society.[26] One strong conclusion was that regulators should consider the wider context in which the digital economy may harm democracy.[27] Several solutions were proposed. Policies concerning data protection were called to be revisited, particularly concerning the failures of the traditional consent-based approach.[28] Similarly, it was also suggested that antitrust and competition

[21] Cobbe, above n 19, at 2.2.

[22] Cobbe, above n 19, at 2.3.

[23] Cobbe, above n 19, at 2.3.

[24] Zuboff, above n 16, at 11.

[25] Zuboff, above n 16, at 93.

[26] Elliott and others, above n 5, at 23.

[27] Elliott and others, above n 5, at 12.

[28] Elliott and others, above n 5, at 61.

regulation should also be refreshed.[29] While these conclusions are the first step towards reigning in some of the negative aspects of the digital economy, the report itself did not detail how these changes should be brought about. Or more importantly, what they should entail.

Merging areas of law

Another complicating feature of the digital economy is the interplay it creates between areas of law that are traditionally treated separately. Usage of business models where individuals gain 'free' online services in exchange for their personal data, highlights the often competing objectives of data protection and privacy on the one hand, with competition policy on the other.[30] Throughout this paper, I will endeavour to show how these areas of law are often intertwined when seeking to address the issues posed by the digital economy.

Bundeskartellamt prohibitions on Facebook

A recent decision by the German national competition regulator highlights some of these concerns. The conclusion of the body was to prohibit Facebook combining user data from different sources for profit-making.[31] The decision suggested that Facebook's access to data was competitively relevant. This access coupled with network effects was seen to constitute another barrier to market entry. It was also found to enhance their ability to monetise their products.[32] Additionally, the decision also accounted for another competing interest that is usually a subject within competition law, that of dynamic

---

[29] Elliott and others, above n 5, at 56.

[30] Furman and others, above n 4, at 124.

[31] Furman and others, above n 4, at 124.

[32] Bundeskartellamt Case Summary *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for data processing* (B6-22/16, 15th February 2019), at 7.

efficiency.[33] They were dismissive of that interest, stating that the internet's innovative power should not be taken into account as an argument against a digital companies market power.[34] For reasons I will elaborate on below, I believe this interest should also be accounted for when discussing the issues the digital economy brings.

More importantly for this paper, the Bundeskartellamt examined the relationship between competition law provisions and the harmonised data protection principles of the GDPR together. It was stated that it was necessary, to examine the conduct of dominant companies both in terms of their data processing procedures and also from the lens of competition law.[35] As it was noted, the "violation of data protection standards is a manifestation of Facebook's market power."[36] Meaning that both the aspect of market dominance and the violation of data protection requirements could perhaps be linked by causality. Of course, it is clear the two areas of law necessarily remain distinct. However, it seems that one interpretation that can be drawn from the decision concerning the digital economy is that both areas can be relevant. It may be the case that both competition and data protection policy have to evolve together to deal with the challenges the digital economy poses.[37]

B: Opportunities

Implications for New Zealand

[33] This can be defined as the benefits to the economy from innovation and technological research, see Whish, *Competition Law* 6th ed (Oxford University Press, Oxford, 2009), at 4.

[34] Bundeskartellamt, above n 32, at 7.

[35] Bundeskartellamt, above n 32, at 8.

[36] Bundeskartellamt, above n 32, at 11.

[37] Renato Nazzini *Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision* (Competition Policy International, March 2019) at 8.

The challenges and benefits posed by the digital economy are a global phenomenon. New Zealand has itself, certain distinguishing characteristics. The 'curse of distance' along with the relatively high proportion of primary industries in international trade are two such features.[38] Remoteness from international markets 'might contribute negatively to GDP per capita by as much as 10% in Australia and New Zealand.'[39] This distance may constrain income growth in several ways. It may act as a barrier to investment, knowledge spill-overs and technology diffusion. Additionally, it may also increase the costs of supplying goods and services to the markets where they are demanded.[40]

Of course, while digital technologies have not eliminated distance as a barrier to economic growth, they still provide new opportunities. There is some reason to suggest the development and expansion of digital technologies may reduce the impact of borders and distance.[41] For example, individuals may have an improved ability to trade across borders using platforms such as Amazon Marketplace. It seems therefore that regulators must be careful not to underemphasise some of the benefits of the digital economy to individuals, society and the economy generally. Careful regulation could allow New Zealand to also realise its potential.

Benefits

---

[38] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 19.

[39] Herve Boulhol, Alain de Serres and Margit Molnar "The contribution of economic geography to GDP per capita," (2008) OECD Journal, Economic Studies, vol. 2008, issue 1, 1-37, at 6.

[40] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 19.

[41] Thomas Friedman *The world is flat: a brief history of the twenty-first century* 1st ed (Farrar, Straus and Giroux, New York, 2005), at 11.

While this paper focuses primarily on the challenges digital markets pose in their use of individuals data, it is also necessary to note some of the benefits. As New Zealand is affected by the "curse of distance," the cross border nature of online platforms may also create new opportunities.

For example, research from the National Bureau of Economics has shown that the average adult in the United States values digital services at several thousand dollars a year.[42] Typically, these services are also provided at no cost. Around the world, it is clear that the digital economy is quickly becoming a growth area within national economies. In the United Kingdom (UK), the number of jobs in the digital technology sector increased at approximately 5 times the rate of other areas of the economy in 2017.[43] It also contributed around £184 billion value to the UK economy in 2017, £14 billion more than in 2016.[44] Companies are increasingly using digital technology to innovate within areas of existing services. For example, Uber in transportation, Airbnb in hotel and hospitality, along with Uber Eats and Delivereasy in food delivery, are just some examples. These digital companies also seem to have the capacity to avoid regulation in the short-term. Perhaps this is due to the novel nature of services they can provide, in contrast with traditional counterparts. Research also suggests that New Zealand businesses are underutilising the benefits that arise from the use of data analysis by both private and public sector organisations.[45] A report has claimed that while New Zealand shared approximately $2.4 billion in gross value added in 2014 through data-driven innovation, Australia's figure at that time was already

---

[42] Erik Brynjolfsson, Felix Eggers and Avinash Gannamaneni *Using massive online choice experiments to measure changes in well-being* (National Bureau of Economic Research, C82, I30, O40, April 2018), at 35.

[43] Furman and others, above n 4, at 19.

[44] Nick Ismail, "Tech Nation 2018 report: UK tech expanding faster than the rest of the economy," <https://www.information-age.com/tech-nation-2018-report-uk-tech-faster-economy-123471982/> (17 May 2018).

[45] Ministry of Business, Innovation and Employment *Business Information and Communication Technology (ICT) use and productivity growth in New Zealand* (October 2017), at 8.

three times greater than our own.[46] They also suggested the reason for this was organisations' rates of adoption concerning data driven processes, as opposed to the sizes of the two countries populations respectively.[47]

C: Line of Argument

Traditionally, most competition and data protection policies necessarily act in an ex-post, after the fact manner. Of course, frameworks usually have some balance between these and ex-ante approaches. The latter are approaches that deal with problems as they arise. For example, the Commerce Commission may vigorously scrutinise business mergers before they occur in markets to mitigate issues of collusion.[48] Similarly, one of the functions of the Privacy Commissioner is to "undertake research into, and to monitor developments in, data processing and technology to ensure that any adverse effects of the developments on the privacy of individuals are minimised."[49] The Commissioner has also pushed for further powers, one example being that agencies should have to demonstrate ongoing compliance with the Privacy Act.[50] This would enable the Privacy Commissioner to proactively recognise issues. A conclusion I believe is necessary is to continue rebalancing frameworks with a greater focus upon these ex-ante approaches, particularly when assessing issues based on the digital economy.

The Elliot report has also suggested that policies should be reframed to address not only individual rights but also to account for collective

---

[46] Hayden Glass and others *Data Driven Innovation in New Zealand* (Sapere Research Group & Covec, 2015), at 6.

[47] Glass and others, above n 46, at 6.

[48] Matt Sumpter *New Zealand Competition Law and Policy* (CCH, Auckland, 2010) at 41.

[49] Privacy Bill 2018, Subpart 2, Functions of the Privacy Commissioner, section 14(j).

[50] Paul Roth, *Privacy Law in Practice*, John Lulich (ed) *Privacy Commissioner makes recommendations for Privacy Act reform,* Judith Collins (looseleaf ed, Lexis Nexis) at [CD. 1], 2017.

dynamics.[51] I would suggest that the dominant companies within the digital economy are those that can pose these collective threats. They control the largest datasets for their exclusive use. If such a company uses data for an improper purpose, the effects are more widespread throughout society generally.

A mark of a successful data protection system could be providing individuals with the trust and confidence to use new digital services. Thus, in a competitive market where services are offered for 'free,' privacy standards can themselves become a relevant assessment of quality.[52] Furthermore, there are opportunities that the digital economy poses for economies around the globe. New Zealand could be a forerunner in this area with careful regulation, that also allows for innovation and technological progress. There are ways for data to be used that allow new opportunities for individuals, not just for digital companies.

This leads me to suggest several propositions that summarise the position:

1. Regulators should aim to ensure informed choice for individuals when they disclose personal data. Once this is achieved, regulators should be wary not to over-extend individual rights.
2. Digital companies who control datasets should be held to higher standards concerning the protection of personal data.
3. Uses of data by digital companies that collectively threaten democratic processes or societal welfare should be those prioritised in frameworks.
4. If we can be confident that this informed choice is achieved and uses of personal data by digital companies are regulated to a satisfactory degree, legislation could also facilitate dynamic efficiency. Frameworks could then also maximise the benefits of the digital economy that use personal data.

---

[51] Elliott and others, above n 5, at 25.

[52] Furman and others, above n 4, at 124.

A way competition could potentially be fostered while giving individuals more control over their data is a data mobility provision, as has been suggested for further research in the UK.[53] Large digital companies would then be moved towards shared data systems, lowering some of the barriers to entry in digital markets. One way to facilitate informed choice for individuals, while placing more responsibility on collectors of data, could be an ethical design provision. This would enforce standards of compliance for companies in the design of their information technologies. It would also allow individuals to better understand the consequences that disclosures of information could have, but perhaps more importantly, in a manner that could be easily understood. Additionally, this approach could supplement traditional frameworks based upon notice, consent and collection. Both of these provisions were discussed in submissions to the Select Committee on the Privacy Bill. Neither were recommended to be adopted into the Bill by the Ministry of Justice's report.[54]

As similar provisions to these are included within the GDPR, regulatory bodies could work alongside EU authorities. This may play a part in easing some of the concerns surrounding transnational issues of enforcement. Where New Zealand bodies may not themselves be able to hold these large digital companies to account, the EU might be able to play a more active role. Within this analysis will also be a discussion on the creation of a digital markets unit. Effective and timely policy-making relies on decision-makers being fully informed. The speed at which the digital world develops poses a serious

---

[53] See the commentary on data mobility in the following reports, Jason Furman and others *Unlocking Digital Competition* (Digital Competition Expert Panel, March 2019), House of Lords Select Committee on Communications *Regulating in a digital world* (9th March 2019), and Ctrl-Shift Department for Digital, Culture, Media and Sport *DATA MOBILITY: The personal data portability growth opportunity for the UK economy* (2018).

[54] Ministry of Justice, above n 10, at 42 and 44.

challenge to this. The body could be tasked with providing the public, Government and Parliament with the latest information.[55]

Chapter 2: Market Dominance

A: Dominance in Digital Markets

Market Concentration

Companies like Google, Amazon, Facebook and Apple have grown at incredible rates. Over time, the internet has quickly evolved into a system where small numbers of large companies dominate and control separate digital markets.[56] Of course, it is necessary in business that by being the most innovative and responsive to consumers wishes, some firms may gain incumbent positions.[57] While this may be true, it is a different story when companies can influence the information flows of billions of users data.[58] Given this, these companies can then implement policies that go relatively untested in terms of how users access and interact with online information. All of the aforementioned companies have a market value of over $400 billion.[59] Facebook alone has 2.7 billion monthly users globally.[60]

Indeed, even where competition does exist within these digital markets, it is usually between a subset of these five large companies. For example, online

---

[55] House of Lords Select Committee on Communications *Regulating in a digital world* (9th March 2019) at 6.

[56] Dr. Shehar Bano (IRN0114) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

[57] Whish *Competition Law* 6th ed (Oxford, Oxford University Press, 2009) at 15.

[58] Bano, above n 56.

[59] House of Lords Select Committee on Communications, above n 55, at 34.

[60] Markets Insider '"2.7 billion people can't be wrong: Here's what Wall Street is saying about Facebook earnings" (31 January 2019), <https://markets.businessinsider.com/news/stocks/facebook-stock- price-earnings-revenuewall-street-2019-1-1027913555>.

searches are dominated by Google, with some competition from Bing. Worldwide, over 92% of online searches were estimated to come from Google's search engine.[61] Social media is dominated by Facebook and the services it owns, albeit with some competition from Snapchat and Twitter. Online advertising revenues are largely controlled by Google and Facebook. Of the £11.55 billion spent on digital advertising in the UK in 2017, the two companies earned 54%.[62] Downloads of mobile apps are shared in a duopoly format between Apple (App Store) and Google (Google Play). Lastly, e-commerce through online marketplaces is dominated by Amazon, with eBay providing some competition.[63]

There are concerns that traditional analyses are ineffective in responding to the fast-paced nature of digital markets. Strong network effects often result in the rapid acquisition of significant market shares by these dominant companies. Businesses can use data to differentiate between customers. This can raise the risk of market abuse. Furthermore, the fast-moving nature of online markets means that enforcement can come too late to address the harms of anti-competitive practices.[64]

Zero Costs

One of the essential first steps in evaluating competition is assessing the "market." This is set out in the Commerce Act as a "market in New Zealand and Australia for goods or services as well as other goods or services that, as a

---

[61] statcounter GlobalStats "Search Engine Market Share Worldwide," August 2019, <https://gs.statcounter.com/search-engine-market-share#monthly-201808-201908>.

[62] eMarketer "Digital Duopoly to Remain Dominant in UK Ad Race," (September 2017) <https://www.emarketer.com/Article/Digital-Duopoly-Remain-Dominant-UK-Ad-Race/1016481>.

[63] Furman and others, above n 4, at 31.

[64] Competition and Markets Authority (IRN0100) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

matter of fact, and commercial common sense, are substitutable for them."[65] Activity outside New Zealand, involving foreign firms will still apply if it affects a market within New Zealand.[66] Once the specific market is defined, market power can then be assessed against the level of effective competition.[67] Some critics of the market-defining process suggest that it should already be regarded as impossible.[68] It is true that in many cases the Commission do not need to precisely define the boundaries of a market in determining a particular issue. One reason for this is that there may not be a clear distinction between what products fall inside and outside any given market.[69] Further difficulties arise in determining the specific market categories that befit areas within the digital economy. Many digital services, like for example, Google Maps and Facebook, are free of cost. Individuals are usually not charged for searching on the internet, or connecting with friends on social networks. The absence of a quantifiable price to be measured provides a challenge for competition policy analysis.[70]

These online services that have no monetary price are usually funded either through a commission by users of platforms, or advertising. One example of this is sellers on Amazon paying commissions to sites such as YouTube for advertising space.[71] For services funded through advertising, individuals essentially pay through the provision of their personal data. Digital platforms are thus known as operating in the "attention market," providing services in

---

[65] Commerce Act 1986, s 3(1C).

[66] Commerce Act 1986, s 4(1).

[67] Diane Coyle *Practical competition policy implications of digital platforms* (University of Cambridge, March 2018) at 3.

[68] Maureen Brunt *Economic Essays on Australian and New Zealand Competition Law* (The Hague, Kluwer Law International, 2003) at 363.

[69] Commerce Commission New Zealand *Mergers and Acquisitions Guidelines* (July 2013) at 23.

[70] Jason Furman and others, above n 4, at 22.

[71] Furman and others, above n 4, at 22.

exchange for individuals attention and data.[72] One way to profit from this time is to sell access to this data to companies for targeted advertising. The exchange often is not consciously participated in by individuals, who do not appreciate the value of the attention they are providing.[73] Individuals having zero costs is, therefore, a distinctive feature of digital platforms.

The Importance of Data

Within the digital economy, data is an increasingly important business input. Due to this, it can also be regarded as a source of market power. While this is true, data access issues are often treated separately under privacy law, for example, as opposed to competition policy. Access to individuals' personal data enables companies to engage in data-driven innovation processes. These improve their understandings of customers' habits and in doing so, cements their advantage. For example, some studies claim to have shown that companies who use data-driven innovation experience 5 - 10% faster productivity growth than those who do not.[74]

Economies of scale and scope are particularly prevalent in the accumulation and use of data relating to individuals' behaviour. As a digital companies user base rises, average costs gradually fall. Geographical barriers are also largely irrelevant to digital markets. Thus, economies of scale support concentration on a global level.[75] Sharing data from one market to another can also reduce costs or increase the quality of services provided. This may be one reason why small numbers of digital companies have found success across many separate digital markets. I share the view of Rubinfeld and Gal, that the amounts of

---

[72] Furman and others, above n 4, at 22.

[73] Furman and others, above n 4, at 22.

[74] Organisation for Economic Co-operation and Development *Big data: bringing competition policy to the digital era* (November 2016) at page 8.

[75] Furman and others, above n 4, at 32.

data held by incumbent firms may be the largest barrier to entry in the digital economy.[76] The data using mechanism that provides these large companies with a competitive advantage is known as a feedback loop.[77] Two distinct types of feedback loop exist. One is user feedback loops.[78] They occur when companies collect data from individuals that they then use to improve the quality of their product or service. This then draws in more users. The second is monetisation loops.[79] These refer to revenues generated from users, that are then reinvested into improving the quality of the services provided.

There are clear implications from digital companies exclusively possessing data. Combined with a lack of engagement from individuals after disclosure, this can lead to low competitive pressure within digital markets. Advantages for digital companies can arise across many different markets. For example, in searching online, a rival with fewer queries to process will generate less accurate results.[80] Therefore, users are more likely to use the incumbent platform, exacerbating the competition problem. The dominance of Google over Bing seems to give some support for this theory.[81] It is advantageous for companies with large amounts of data to maintain their existing position and further increase their market share. Inevitably, this will pose barriers to new entrants.[82]

Network Effects

[76] Daniel Rubinfeld, Michal Gal "ACCESS BARRIERS TO BIG DATA" Arizona Law Review, (2017) VOL. 59:339, at 43.

[77] Organisation for Economic Co-operation and Development, above n 74, at 10.

[78] Organisation for Economic Co-operation and Development, above n 74, at 10.

[79] Organisation for Economic Co-operation and Development, above n 74, at 10.

[80] Marc Bourreau, Alexandre de Streel and Inge Graef *Big Data and Competition Policy: Market power, personalised pricing and advertising* (Cerre, 16 February 2017) at page 49.

[81] Furman and others, above n 4, at 34.

[82] Furman and others, above n 4, at 35.

These effects refer to the increase in value of a service as its user network increases. Digital companies are typically loss-making until they reach a critical amount of users. Before large incumbent firms began to control digital markets, other digital companies could become dominant in short periods through these effects.[83] The Entrepreneurs Network and Adam Smith Institute argue in the alternative, that these tech companies' heavy investment in research and development highlights that they are in intense competition with one another.[84] Indeed, Amazon, Google, Microsoft and Apple all were in the list of the top 10 companies for spending on research in 2018.[85] It should be noted, however, that the areas of research these companies invest in are unknown. The threat of competition may also encourage them to invest in areas targeted towards further solidifying their position. This could make successful entry into markets less likely, rather than being aligned with strategies that maximise consumer welfare.

As digital markets can show these network effects, incumbents can become entrenched in markets known as "winner-takes-most."[86] Statistics suggest arguments that digital companies are in intense competition with one another may be erroneous. For example, Facebook has 2.3 billion active users and in the UK in 2018, was visited monthly by 95% of the adult internet audience. For Google, the figure was 99%.[87] This reflects that buyers want to use the platform that has the most sellers, and vice versa.[88] Furthermore, having more

---

[83] Doteveryone (IRN0028) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019" at 22.

[84] The Entrepreneurs and Adam Smith Institute (IRN0070) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019" at 5.4.

[85] Furman and others, above n 4, at 20.

[86] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 39.

[87] Furman and others, above n 4, at 18.

[88] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 43.

users and data creates other competitive advantages, such as better predictions and personalised marketing advice. One example of these effects is Google overtaking rivals such as AltaVista and Yahoo as the leading search engine. Why was this possible? Google could offer users faster and more relevant search results. The position has now been solidified by user and monetisation feedback loops, that smaller competitors cannot match.[89]

Lock-In Effects

Individuals can also be locked to using the services of digital companies. These effects are particularly strong in the digital sector due to the aggregation of services companies can provide. The lock-in effect refers to a situation whereby individuals are dependent on a single producer and cannot move to another without substantial costs or inconvenience.[90] Individuals get used to services they use daily and often become less willing to switch. Particularly this is true when a user's experience of a service also depends on others. For example email, geolocation services or social media services. One example would be switching between the clouds of Apple and Microsoft.[91] Additionally, these digital companies have an incentive to move away from interoperability, or the exchange of information between services. Raising the costs of switching once they have accumulated large amounts of personal information is also in their interest. A lack of interoperability helps large platforms to maintain their market position by maintaining the barriers that result from these network and lock-in effects.[92]

---

[89] Furman and others, above n 4, at 38.

[90] Markus Eurich, Michael Burtscher *The Business-to-Consumer Lock-in Effect* (University of Cambridge, August 2014), at 2.

[91] Directorate General For Internal Policies Policy Department A: Economic and Scientific Policy, *Challenges for Competition Policy in a Digitalised Economy* (IP/A/ECON/2014-12 July 2015 PE 542.235) at 33.

[92] Directorate General For Internal Policies Policy Department A: Economic and Scientific Policy, above n 91, at 26.

Mergers

The data digital companies possess can enter their production process in several ways, as noted by some of the above analysis. After a merger, the creation of larger or more diverse datasets is capable of providing those digital companies with further competitive advantages.[93] Companies within the digital economy are very active in acquiring and merging with other smaller counterparts. Over ten years spanning from 2008 to 2018, Amazon, Google and Facebook have acquired 299 companies collectively.[94] One main conclusion of the Lear report is that these acquisitions by digital companies usually target companies whose services are complementary to those supplied by incumbent firms.[95] Often these companies are relatively new to the market, so it is difficult for authorities to determine whether they will become a competitive force. These acquisitions of companies with complementary products may stop potential or direct competitors from improving their products to better challenge incumbents. Strong network effects mean that often competition is "for" the market, as opposed to "in" the market.[96] Thus, the threat exerted by potential entrants is crucial to constraining market power.

Mergers can also move these companies into separate niche areas. One notable example was Amazon's purchase of Whole Foods Market.[97] As many services and sectors are yet to become digitalised, these large tech companies may gain further advantages in these emerging markets. Of course, many of these acquisitions were likely benign and beneficial to consumers. Why might this

---

[93] Elena Argentesi and others *Ex-post Assessment of Merger Control Decisions in Digital Markets* (Lear, June 2019), at 10.

[94] Argentesi, above n 93, at 9.

[95] Argentesi, above n 93, at 9.

[96] Argentesi, above n 93, at 31.

[97] House of Lords Select Committee on Communications, above n 55, at 39.

be the case? Small numbers of firms may make for more efficient transactions for consumers and businesses. That may be because they facilitate for companies who grow because they offer better, more innovative products.[98] A minority, however, of these mergers are likely to be anti-competitive. The research of the Furman report suggests at least some of these acquisitions are problematic.[99]

Competing Incentives

Where firms have these dominant positions, rather than compete to build individuals' trust in their businesses, they can also devise more effective ways of exploiting consumers. Competing incentives may occur when the digital company running the platform also produces goods and services sold on that marketplace. These may give preference in its rankings to its products in the placement of advertising.[100] One example of this was the EU fining Google €2.4 billion in June 2017, following an investigation that found the company had favoured its services in internet search results. The Commission found that Google had displayed its comparison-shopping service in its general search results pages and had exempted its service from penalties applied to competitors.[101]

B: Summing Up

Digital markets do provide considerable benefits for individuals and society generally. While this is the case, many digital markets are dominated by one or

---

[98] Furman and others, above n 4, at 10.

[99] Furman and others, above n 4, at 100.

[100] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 39.

[101] Nick Statt *Google appeals record €2.4 billion antitrust fine over manipulated search results*, The Verge <https://www.theverge.com/2017/9/11/16291482/google-alphabet-eu-fine-antitrust-appeal>.

two large companies. The position of these companies can lead to privacy and data protection issues. Additionally, the barriers to entry that exist in established markets suggest they may not be freely contestable. Thus, dominant companies can exert significant market power over users. In large part, the impacts of this may be benign to societal welfare. While this may be true, a serious misuse of data from a company containing a large and diverse dataset may have detrimental implications that go further than affecting a given individual or groups privacy. A preliminary report from the Australian Competition and Consumer Commission released a worrying conclusion. Facebook and Google may be insulated from competition due to factors such as their barriers to entry and acquisition strategy.[102] The fact that these two companies hold some of the largest tracts of personal data does not seem to be a coincidence.

Irrespective of the way platforms and digital companies have come to assert their dominance, it is largely the case that several companies in certain markets have high degrees of control and influence over relationships between consumers and producers.[103] This gives them some distinct forms of power relative to other market forms. Research suggests the position of the largest firms is getting stronger. This coincides with increased profitability over time. The pricing within these digital markets shows a significant likelihood that none of the currently successful companies will lose a battle for the market in the foreseeable future.[104]

While individuals can access services with no costs, it is in the interests of digital markets to provide them in this way. Even though these free services have positive outcomes, they often do not tell the full story. Specifically, they

---

[102] Australian Competition and Consumer Commission *Digital Platforms Inquiry – Preliminary Report* (December 2018) at 8.

[103] Furman and others, above n 4, at 42.

[104] Furman and others, above n 4, at 47.

may not show the amount of data given in exchange for a service. Or the advertising it is used for, or the privacy by which personal data is treated in its use. While it may be difficult, these are factors that should also be measured when assessing the digital economies' impact.[105] Situations like the Facebook and Cambridge Analytica scandal that will be discussed below, show that some digital companies have not taken issues of privacy and treatment of consumer data as seriously as regulators and individuals desire.[106] One statement of the Furman report was that misuses of data, along with harms to privacy, are perhaps causally related to low quality caused by low levels of competition.[107] It may be true that the large collections of data held by digital companies are a way of achieving monopolistic power in markets. This aligns with conclusions of the House of Commons report concerning 'Fake News,' whereby scrutiny was invited over whether Facebook was unfairly using its position in the market to determine whether businesses could succeed or fail.[108] It seems clear that antitrust enforcement in this area is crucial. Traditionally, however, it acts in a predominately ex-post, after the fact manner. The intention of which is to resolve issues that narrowly focus on specific cases. Thus, it seems that traditional approaches may need to evolve to become more compatible with digital markets. So far, frameworks have not established set rules and principles to give businesses certainty regarding the boundaries of acceptable competitive conduct.[109]

Chapter 3: Personal Data Mobility

A: Moving Forward

[105] Furman and others, above n 4, at 42.

[106] Furman and others, above n 4, at 43.

[107] Furman and others, above n 4, at 43.

[108] House of Commons Digital, Culture, Media and Sport Select Committee *Disinformation and 'fake news'*: *Final Report* (February 2019), at 42.

[109] Furman and others, above n 4, at 57.

When the characteristics of a market mean they gravitate towards several firms taking incumbent positions, policy interventions beyond those considered standard are necessary. Digital markets based upon data-driven business models seem to show these tendencies. The Furman report proposed that pro-competition policy tools should be implemented to create more competition in these markets.[110] Some of the proposed positives of moving towards such frameworks are as follows. They would facilitate entry, helping smaller businesses find new market niches. Another goal would be to provide predictability for the standards that they should apply. Perhaps most importantly, they would benefit individuals by incentivising companies to compete with one another over guarantees in terms of personal data treatment.[111]

A benchmark of this pro-competition approach is data mobility. Effective implementation could help mitigate network and lock-in effects, pushing systems to use open and standardised formats.[112] Individuals could then move their data between networks. Smaller companies could then also have the opportunity to access the data sets of larger companies. This could have the effect of opening up new business opportunities to use, manage or combine datasets.

B: Data portability

Discussion on Data Portability inclusion within the Privacy Bill

Data portability refers to the right of individuals to transfer their personal data from one digital company to another. Thus, it could enhance competition by

[110] Furman and others, above n 4, at 56.

[111] Furman and others, above n 4, at page 57.

[112] Furman and others, above n 4, at 57.

allowing individuals to switch between services, while also empowering individuals by providing them with more control over their data.[113] Twenty-six submissions were made on the provision. The majority favoured inclusion of some form of the right, primarily to promote consumer rights so that they are not "locked-in" to existing providers.[114] There were some other comments of note within some of the submissions. One was from Trade Me, submitting that it would prefer to learn from the EU's experience with data portability before implementation in New Zealand.[115] Progressive Enterprises Ltd also suggested that implementation costs might outweigh any benefit to New Zealanders.[116] The Ministry of Justice recommended that while the right could be considered as part of future work, it should not be inserted into the Bill.[117] These comments may have merit, as the area is a largely novel one without much in the way of application. Many issues come with implementing such a provision. Only some will be discussed in the analysis below. Although this may be the case, working alongside international partners in formulating the basis for such a right may be worthwhile. I will endeavour to show that further research into the area should be made by regulators.

GDPR Interpretation of Data Portability

Article 20 of the GDPR refers to the right of a data subject to receive data they have provided to a controller, along with the ability to transmit that data to another controller without hindrance from the controller to which the data has been provided.[118] In contrast to the principle-based approach of the EU,

---

[113] Ministry of Justice *Departmental Report - Part Two, Privacy Bill* (13th March 2019), at 41.

[114] Ministry of Justice, above n 113, at 41.

[115] Ministry of Justice, above n 113, at 42.

[116] Ministry of Justice, above n 113, at 42.

[117] Ministry of Justice, above n 113, at 42.

[118] General Data Protection Regulation 2018, Article 20(1) Right to data portability.

Australia is taking a detailed sectoral approach including standards infrastructure. An incremental approach will be applied, with implementation beginning in the banking sector. It will include complemented powers of the Privacy Commissioner through the Australian Competition and Consumer Commission.[119]

The GDPR interpretation of the right intends to give individuals several new abilities when it comes to personal data they may have disclosed. Firstly, it seeks to enable individuals with more control over their personal data, as it facilitates their ability to move their data from one organisation to another.[120] This is intended to provide consumer empowerment by preventing lock-in effects.[121] Individuals are then also entitled to receive a subset of their personal data that is processed by a collector of that data.[122] This is to be provided in a structured, commonly used and machine-readable format.[123] That individual can also exercise his or her rights to manage or reuse their personal data so long as the controller processes it. This is a key change, whereby individuals become active participants in the digital economy, as opposed to being treated as passive subjects.[124] Giving individuals these rights seeks to create the basis of initiatives promoting the wider beneficial economic and societal use of data.

Portability in practice: United Kingdom (UK) original midata programme

---

[119] Ministry of Justice, above n 113, at 41.

[120] Article 29 Data Protection Working Party *Guidelines on the right to data portability* (16/ EN WP 242 rev.01, 5th April 2017), at 4.

[121]Article 29 Data Protection Working Party, above n 120, at 4.

[122] Article 29 Data Protection Working Party, above n 120, at 4.

[123] Information Commissioners Office, 'Right to data portability,' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>.

[124] Ctrl-Shift, Department for Digital, Culture, Media and Sport *DATA MOBILITY: The personal data portability growth opportunity for the UK economy* (2018) at 32.

In 2011, the midata programme was initiated in the UK by the then Department of Business, Innovation and Skills. Essentially, individuals could download their current transactional data from banks. It could then be placed into comparison tools that would help individuals find the best provider.[125] This was the first proposed concept of data portability. The programme sought voluntary engagement from 25 different organisations to make data available to individuals.[126] One challenge was the cost to businesses of making that data available and the incentive or opportunity for those businesses themselves. After doing so, the midata innovation lab (miL) was then designed whereby consumers could choose to allow access to service providers to their data. This was to drive a new range of innovative information services.

There were several lessons to be learned from the miL project. One was that these kinds of initiatives provided businesses and policymakers with an opportunity to accelerate innovation, but importantly, in a safe environment. It was shown that working together in these multi-disciplinary teams enabled rapid progress and accelerated the development of new concepts.[127] There were also benefits for individuals. They were able to make decisions about data sharing based upon their opinion of the company. This meant that trust became a key element when disclosing information. All this being said, it was clear that outside of this environment, individuals privacy and improper uses of their data remained the key concern. Designing effective interoperating data sharing systems would be essential in expansionary programmes so that they can be said to protect the security of individuals data.[128]

---

[125] Finextra 'Midata initiative launches to help Brits pick best bank account providers' (March 2015) <https://www.finextra.com/newsarticle/27168/midata-initiative-launches-to-help-brits-pick-best-bank-account-providers>.

[126] Department of Business Innovation & Skills and the Rt Hon Edward Harvey "The midata vision of consumer empowerment" (November 3rd 2011) <https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment>.

[127] Ctrl-Shift, above n 124, at 81.

[128] Ctrl-Shift, above n 124, at 81.

Challenges

While this new GDPR legislation may be an important step towards enshrining personal data rights, critics suggest it does not go far enough in the facilitation of data mobility and value generation in data.[129] One issue is enforcement of these portability rights and how will data be shared safely and securely.[130] While it is required that personal data must be provided in a 'structured, commonly used and machine-readable format,' there are no enforcement mechanisms within the GDPR for this. For example, those requiring organisations to develop technical standards to facilitate data transfers across networks.[131] The data portability provisions also only relate to personal information provided directly by the individual. This may only be a very small amount of data that the supplier holds, for example, the tracking of online behaviour is likely to not be covered.[132] Additionally, the GDPR does not currently provide provisions for data standards or interoperability protocols that will be required to build an effective and efficient transactional environment for personal data.

It should also be noted that competition is not an objective of the GDPR. Privacy and data protection interests are those that take precedence. As aforementioned, the objectives of competition law can I believe, be accounted for even when considering data protection issues. Arguably, these are competing interests. Thus, regulating competition in the digital economy should also result in safer environments for the protection of data.

---

[129] Furman and others, above n 4, at 68.

[130] Ctrl-Shift, above n 124, at 33.

[131] Furman and others, above n 4, at 68.

[132] Furman and others, above n 4, at 68.

C: Data Mobility

At a simple level, data portability gives individuals the right to request access to their data and potentially move it from one system to another. Data portability as a standard has already been initiated across several projects. While data portability is well established in a business context, transactions often do not involve the individuals who are the subjects of the data.[133]

The concept of personal data mobility goes beyond data portability as specified in the GDPR. Mobility is premised on the idea that uses of data to create value should not only be restricted to the party responsible for its original storage and collection. Rather, individuals should on request, also be able to move their data directly to other organisations or store and use it for their purposes.[134] Data could then be recombined to create new usage opportunities.[135] Personal data mobility could also involve any type of data used by those businesses that store large amounts of personal information.[136] Much wider circulation of personal data could be created, not just between the service provider and individual, but also between providers themselves. This regime could tackle some of the power of digital companies who have large advantages coming from the returns to scale of accumulated user data. It could also provide a stimulus for growth and productivity, lowering the barriers to entry for smaller firms.

UK Initiative

[133] Ctrl-Shift, above n 124, at 94.

[134] Furman and others, above n 4, at 65.

[135] Ctrl-Shift, above n 124, at 34.

[136] Furman and others, above n 4, at 65.

The UK is striving to take the first steps in the adoption of a more expansive data mobility framework within its legislation. Some of the preliminary research can be seen in the reports from CtrlShift for the Department for Digital, Culture, Media and Sport and the Furman Report.[137] New Zealand could also be a forerunner in this field through investment in research and development, and by also working alongside UK authorities on the matter.

Challenges

Many challenges come with creating a digital environment that embraces personal data mobility. These encompass those posed in implementing data portability and extend further. It seems that extensive research in this area is necessary before the benefits of implementation could be realised. Several main parties that would be influenced are as follows. One would be individuals, as decisions regarding the mobility of data would largely be determined by them. Another party is those incumbent providers such as the GAFA's, that would need to build entirely new trust-based relationships based upon data from empowered individuals.[138] Lastly, data mobility could lower barriers to entry and create opportunities for new entrants into the digital economy.

Infrastructure and Standards

The development of common standards, technologies and services are essential for the creation of digital markets that embrace data mobility. Solutions that enable the secure and fast exchanges of data are not yet advanced enough. The infrastructure itself will also require significant

---

[137] Ctrl-Shift, Department for Digital, Culture, Media and Sport, *DATA MOBILITY: The personal data portability growth opportunity for the UK economy* (2018) and Jason Furman and others *Unlocking Digital Competition* (Digital Competition Expert Panel, March 2019), starting at page 64.

[138] Ctrl-Shift, above n 124, at 45.

investment. As the accumulation of data and the ability to exclude others from using it helps keep incumbents profits high, they have low incentives to make these investments facilitating data mobility. Thus, they may not want to share their data as it may erode their competitive advantage.[139] This may also create higher fixed costs in starting businesses for new entrants, as investment may have to be diverted into infrastructure development.[140] Furthermore, these standards must be built for fast-moving markets. Regulators and Government need to adapt quickly to ensure individuals data is protected. Individuals lack of knowledge of the digital market and its uses of their data is also an issue. Without education, individuals are less likely to be able to manage the risks that data mobility creates.[141] It may mean that individuals will be reluctant to use data-driven services and to share data, despite the new rights it provides them.

Several issues must then be prioritised. One is facilitating an environment that promotes safe data sharing. Even data portability under the GDPR may create risks for all parties involved as a result of the threats arising from misuses of data. These issues would be increased from the wider circulations of data created by data mobility. For example, providers may gain consent to access data while promising to protect it, then change policies or break promises.[142] Additionally, interoperability or the ability of digital systems to exchange information must be made available. These interoperable standards will be able to accelerate mobility progress by lowering costs, providing the ability for investment.[143]

---

[139] Ctrl-Shift, above n 124, at 58.

[140] Ctrl-Shift, above n 124, at 51.

[141] Ctrl-Shift, above n 124, at 52.

[142] Ctrl-Shift, above n 124, at 58.

[143] Ctrl-Shift, above n 124, at 104.

Research Groups

Regulators could look towards current initiatives researching the area for guidance. For example, the BSI IoT Community is developing a framework to support safe uses of data and devices through interoperability.[144] Additionally, technological developers such as Nesta DECODE are driven to put individuals in control of their personal data, allowing them the opportunity to make decisions as to whether it is best kept private or shared in the public domain.[145] Even the large digital companies themselves are voluntarily coming together to develop the standards necessary to enable mobility of data. The Data Transfer Project, consisting of Apple, Facebook, Microsoft and Twitter has the aim of building a common framework connecting online service providers. This would enable user-initiated mobility of data.[146] Of course, this may serve as a red herring, as the project could ultimately further cement competitive advantages between these dominant digital companies. It is, therefore, necessary that appropriate regulation is also implemented.

Open Banking

Open banking is the most notable example of data mobility in practice. This area offers the most developed standards for the proposed mobility system. Essentially, it allows greater access for consumers to use the data collected from them by financial institutions.[147] At a consumer's request, organisations must share information in a specific standardised manner. This means individuals can elect to have information from accounts held across multiple

---

[144] BSI "Internet of Things Enabling a Smart and Secure World" <https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/>.

[145] Nesta 2017-2020 "What we want to achieve" <https://media.nesta.org.uk/documents/nesta_strategy_2017-2020.pdf>.

[146] Data Transfer Project "About us" (2018) <https://datatransferproject.dev/>.

[147] PwC 2018 "Open Banking 101" <https://www.pwc.com.au/banking-capital- markets/banking-matters-hot-topic-open-banking-101.pdf>.

providers, shared with a single app.[148] The reforms to deliver Open Banking were initiated by the UK Competition Markets Authority (CMA). Using its powers, the authority was able to make the largest banks comply and implement the initiative. A regulation entity was funded by the CMA to design standards to make the system function effectively.[149] An interesting characteristic of the scheme is that the Revised Payment Services Directive (PSD2) ensured that third parties who access consumer's account information have to be authorised by the Financial Conduct Authority.[150] This was one way to give individuals the confidence to trust third parties with their personal data.

The Productivity Commission suggested co-operation between Australia and New Zealand in developing open banking standards, that could enable greater mobility of data.[151] This could be a way to incrementally implement data mobility, by only compelling the largest digital companies to comply with standards.[152] As noted above, the implementation of data mobility will likely have substantive costs and complexities. The systems used in the UK Opening Banking schemes could be studied for guidance. Wider balancing tests between benefits and costs should be undertaken so that the tool is only used in digital markets where it is likely to be an effective intervention.[153]

Opportunities

Recombinant Innovation

---

[148] Furman and others, above n 4, at 69.

[149] Furman and others, above n 4, at 70.

[150] Furman and others, above n 4, at 70.

[151] Australian Productivity Commission and New Zealand Productivity Commission, above n 1, at 111.

[152] Furman and others, above n 4, at 70.

[153] Furman and others, above n 4, at 71.

If data that is held by different parties can be combined there are a multitude of different ways it can be used to create growth across the digital economy. For example, data from multiple financial providers could create a stronger understanding of an individual's financial position, as the basis for the provision of financial advice.[154]

Productivity benefits

Personal data mobility would reduce data access costs. This could enable businesses to acquire data more cost-effectively, stimulating economies of scale. Additionally, easier access to larger varieties of data could lead to reductions in production costs and better-tailored products.[155] When individuals share data in exchange for new products or services, that data could help organisations improve or develop their products. This could benefit not just the individual who originally shared the data, but potentially large amounts of individuals through aggregation effects.[156] For example, if data based on individuals' health was more readily available, a better understanding of health issues could be achieved. Furthermore, predictive health services could be improved.[157]

Competition

Mobility may also be able to stimulate more innovation in the digital economy. Larger amounts of access to personal data mean that new entrants can more readily understand consumer needs. This would contrast current markets whereby several dominant firms large silos of data make it difficult

---

[154] Ctrl-Shift, above n 124, at 34.

[155] Ctrl-Shift, above n 124, at 41.

[156] Ctrl-Shift, above n 124, at 41.

[157] Ctrl-Shift, above n 124, at 41.

for new companies to find footholds. This could reduce barriers to entry, particularly in markets like the digital economy where there are high concentrations of dominant suppliers without a great deal of competition.[158]

Individuals

Furthermore, decisions regarding the mobility of personal data will be placed into the hands of individuals. Mobility is also likely to increase the probability that individuals will be able to access a larger range of services and products from existing providers. They may also be able to benefit from innovative services from new entrants operating in competitive markets.[159] For example, consumers can react more quickly to price signals, switching to a supplier that may offer a better deal. It may also enable them to access more accurate price information, to better compare goods and access more tailored advice. They can also request for their data to be transferred. Lower switching costs could make it easier for market entrants to find new consumers who can more easily move away from large incumbent companies.[160]

Chapter 4: Data Protection

A: Data Protection frameworks relating to personal data disclosures

The Elliot report identified that redress of the consent-based approach to data protection is necessary.[161] In the following chapters, the discussion of privacy law will refer to exclusively to those aspects concerning the use of individuals personal data in the digital economy.

---

[158] Ctrl-Shift, above n 124, at 42.

[159] Ctrl-Shift, above n 124, at 44.

[160] Ctrl-Shift, above n 124, at 43.

[161] Elliott and others, above n 5, at 25.

Traditional Approaches

Notice, consent and collection based frameworks consist of some of the fundamental elements of traditional data protection legislation that can often be exploited by digital companies. These were initially designed after discussions in North America and Europe, where a number of information privacy principles were formed.[162] They became the foundation for the Organisation for Economic Cooperation and Development (OECD) guidelines on the Protection of Privacy and Transborder Flows of Personal Data in the 1970s.[163] The principles of these guidelines form the basis of most privacy legislation around the globe. Fundamentally, they are concerned with the processing of individuals' data being undertaken lawfully. In the context of the internet, this system of "notice and consent," has become a dominant mechanism of privacy frameworks.[164] The aim of such an approach is intended to provide people with control over their personal data. Individuals can then theoretically decide to weigh up the costs and benefits of disclosing their personal information themselves. Daniel Solove refers to this approach as 'privacy self management.'[165] Frameworks based upon these approaches align with traditional views that individual privacy decision making aligns with rational choice theory. This is the theory that individuals maximise utility over

[162] Fred Cate, Viktor Mayer-Schönberger "Notice and Consent in a World of Big Data" (2013) Articles by Maurer Faculty, 2662 at 1.

[163] Cate, Mayer-Schönberger, above n 162, at 1.

[164] Cate, Mayer-Schönberger, above n 162, at 1.

[165] Daniel J Solove 'Why Privacy Matters Even if You Have Nothing To Hide' *The Chronicle of Higher Education* (2011) at 1.

time while using all the possible information available to them.[166] The appeal of such an approach lies in the value of facilitating individual autonomy.[167]

GDPR requirements on Consent and Collection

GDPR legislation strongly relies upon consent and collection. The basic requirements for legal consent are defined in Article 7 and outlined in Article 32. A clear affirmative action must be given. The request for consent must be given in an intelligible and accessible form by digital companies, with the procedure for data processing attached. The act must then establish a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data.[168] Freely given consent means consent given voluntarily. To be informed and specific, the individual must be notified of the digital companies identity, the kind of data that is being used, how it will be used and the purpose of the processing operations. The consent must also be bound to one or more purposes that must then be sufficiently explained. It must also be unambiguous, requiring either a statement or an affirmative act.[169] Individuals also have the right to withdraw their consent at any time.[170]

Article 13 of the GDPR sets out the information that is to be provided to individuals where personal data is collected by digital companies. The individual is to be provided with specific information from the company, including the contact details and identity of that controller, along with the

---

[166] Alessandro Acquisti and Jens Grossklags "What can behavioural economics teach us about privacy" in Acquisti and others *Digital Privacy: theory, technology, and practices* (Taylor and Francis Group, 2007) at 1.

[167] Rishab Bailey and others "Disclosures in privacy policies: Does notice and consent work?*"* (NIPFP Working Paper 246, December 2018).

[168] General Data Protection Regulation 2018, Article 32.

[169] General Data Protection Regulation 2018, Article 7.

[170] General Data Protection Regulation 2018, Article 7(3).

purposes and legal basis for processing.[171] Additionally, the controller must provide the individual with information as to how long the personal data will be stored.[172] Even when that information is not directly collected from the individual, they are still required to provide them with similar information.[173] These requirements are stringent relative to the NZ framework.

Notice, Consent and Collection in the New Zealand Privacy Bill

As mentioned in Chapter 1, the New Zealand Government is currently in the process of amending the Privacy Act 1993. Within the Privacy Bill, IPP 10 provides that personal information acquired for one purpose cannot be used for another unless an exception applies.[174] Under IPP 2, personal information must be collected directly from the individual concerned, albeit subject to several exceptions.[175] Several submissions suggested explicit consent should be required for disclosures of personal information by digital companies. According to the Departmental Report on submissions, the Bill seeks to retain the Act's focus. That being on companies retaining a lawful purpose for which information is collected.[176] Agencies can only disclose information to other companies if it is for that purpose. One exception to this is where the individual has authorised the disclosure of their personal data.[177] Thus, under New Zealand law, it is the concept of purpose that plays a central role in authorising the collection, use and disclosure of personal information. In both the Act and the new Bill, there is no use of the term "consent." Rather, "authorised by" is used. The Chief Justice's interpretation of the section was

[171] General Data Protection Regulation 2018, Article 13 s(1)(a) and (b).

[172] General Data Protection Regulation 2018, Article 13 s(3)(2)(a).

[173] See the requirements set out in General Data Protection Regulation 2018, Article 14.

[174] Privacy Bill 2018, s 19, Information Privacy Principle 10.

[175] Privacy Bill 2018, s 19, Information Privacy Principle 2.

[176] Ministry of Justice, above n 10, at 43.

[177] Privacy Bill 2018, s 19, Information Privacy Principle 11(1)(c).

that informed consent is implicit to the concept of collection.[178] The interpretation given by the Ministry's report suggested similarly that "authorised by," was included to indicate that a high level of consent is required, as it can often be implied.[179]

Aside from these principles based upon notice, collection and consent, it seems that the majority of changes that will apply to the digital economy are mostly reactive and ex-post in nature. By ex-post, they apply after data has been improperly used. These changes are inclusive of some of the following provisions. It is now mandatory for digital companies to report privacy breaches.[180] Those breaches that pose a serious risk of harm to individuals must be notified to both the Privacy Commissioner and those affected. The Privacy Commissioner also has heightened powers. One of these includes the ability to issue compliance notices to agencies.[181] These can be enforced by the Human Rights Tribunal.[182] The Commissioner can also issue a determination to agencies where an individual has requested access to personal information and has been refused. While these changes have been welcomed, there is a new body of literature that suggests frameworks that are still primarily focused upon notice, consent and collection are susceptible to manipulation by digital companies. It seems that even with these new changes, the purpose of collection is still a primarily ex-ante focus concerning the protection of information in the Privacy Bill. In the GDPR, the approach is more tilted towards strengthening traditional consent-based frameworks.

Criticism of traditional collection and consent-based frameworks

---

[178] *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR at [138].

[179] Ministry of Justice, above n 113, at 52.

[180] Privacy Bill 2018, Part 6, Subpart 1, Notifiable privacy breaches.

[181] Privacy Bill 2018, Part 6, Subpart 2, Compliance Notices.

[182] Privacy Bill 2018, s 130.

Data protection has historically been defined by consent. Once it is obtained, a digital company is generally free to collect, process and use data for a specified purpose and will not be liable for any consequences that may result. Thus, the onus is essentially on the individual to be aware of the terms of data access they consent too. Concerns have been growing that frameworks relying heavily upon consent and collection may not be sufficient to protect individuals personal data. These concerns of misuse are particularly pertinent in the age of emerging technologies.[183] Traditional frameworks that were initially aimed to help individuals seem skewed towards benefits for digital companies. One reason for this is the broad discretion companies have in designing notice and consent mechanisms for information technologies. Companies can also use formalistic or technical legal compliance with privacy principles that may overwhelm individuals with information. So that in theory, user autonomy is prioritised, but due to some of the following reasons, it is clear that such an approach is weakened by design features, as guidelines often do not focus on how technology affects individuals.[184] So what are some of the criticisms of these frameworks? There are a series of arguments suggesting several difficulties distance actual privacy decision making from that of traditional rational choice theory.

Asymmetric Information

Evidence shows that most individuals do not read privacy notices.[185] An empirical study of 543 participants that were familiar with privacy law issues found that 74% of participants opted for the "quick join" procedure, bypassing

---

[183] Rahul Matthan *Beyond consent: A new paradigm for data protection* (Takshashila Discussion document 2017-03) at 1.

[184] Woodrow Hartzog *Privacy's Blueprint* (Harvard University Press, Massachusetts, 2018). at 61.

[185] Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880 at 6.

the privacy policy.[186] Researchers calculated that the documents required at least forty-five minutes of adequate comprehension, but the median time spent by each individual was fourteen seconds.[187] One explanation for this phenomenon may be that privacy choices are often affected by asymmetric or incomplete information.[188] The surveillance capitalism model incentivises digital companies to obtain as much personal information as possible so that they can put it to use. This way they are best able to maximise profits. Thus, disclosing risks or providing complete information is counterintuitive. Additionally, there are multitudes of different companies that collect and use data. The amount of these entities collecting personal data make it infeasible for the rational person to manage their privacy.

From the individuals perspective, information asymmetries also prevent an individual from knowing when another entity has gained access to their data. Further to this point, that individual may not be aware of the potential future consequences that come with continued use of their personal information.[189] These difficulties are becoming increasingly amplified in highly digitised information networks. Incomplete information does complicate privacy decision making. Primarily this is due to the multiplicity of outcomes and the lack of pure knowledge of those outcomes, relative to those that are deterministic.[190]

Cognitive Biases

These complexities characterising privacy choices exacerbate the cognitive and behavioural biases that influence individuals in day to day decision

[186] Zuboff, above n 16, at 237.

[187] Zuboff, above n 16, at 237.

[188] Acquisti and Grossklags, above n 166, at 2.

[189] Acquisti and Grossklags, above n 166, at 3.

[190] Acquisti and Grossklags, above n 166, at 5.

making. Some studies argue that even if individuals had complete information, they would still be unable to process large amounts of data.[191] This is due to our innate bounded rationality, limiting our ability to memorise and process all relevant information, instead forcing individuals to rely on simplified mental models and heuristics.[192] Individuals are also prone to rely heavily on information that is easiest to recall in our minds, as opposed to its relevance. This process is known as the availability heuristic.[193] In alignment with hyperbolic discounting, we often choose smaller sooner rewards, relative to larger ones later.[194]

Aggregation Effects

Possibly the most important objection to traditional privacy self management theory is that it addresses privacy in a series of isolated transactions by particular individuals.[195] It seems that the costs and benefits may be better assessed cumulatively as opposed to at an individual level. This would align with the findings of the Workshop Report, that suggested recalibration towards issues that have collective impacts.[196] Privacy protection has distributive effects. It benefits some while harming others. As one person's decision to consent may not collectively give the most social utility, frameworks based upon privacy self management may continue to fail in addressing these wider social values. This reasoning leads to the discussion of aggregation effects. Lots of small data aggregated together may be able to tell a lot about a group of individuals, or a specific individual.[197] New predictive analytics that can be

[191] Acquisti and Grossklags, above n 166, at 7.

[192] Acquisti and Grossklags, above n 166, at 7.

[193] Hartzog, above n 184, at 36.

[194] Hartzog, above n 184, at 37.

[195] Solove, above n 185, at 3.

[196] Elliott and others, above n 5, at 25.

[197] Solove, above n 185, at 12.

gathered through aggregation accentuate the pace that is too fast for individuals to assess the risks and benefits that are entailed with data use.[198]

Three Themes

Three themes emerge to explain our vulnerabilities to external forces when disclosing personal data.[199] Individuals' privacy preferences are malleable, in that they are subject to influence from those who have better insight in terms of what incentivises disclosures. Digital companies have developed expertise in exploiting behavioural and psychological processes promoting exchanges of data.[200] Context is also paramount. Depending on the situation, individuals exhibit anything from extreme concern to indifference on privacy issues. All the while, individuals are uncertain about the privacy tradeoffs they prefer. Information asymmetries prevent individuals from properly assessing risk and even when consequences are clear, people are uncertain as to their preferences.[201] So it may be true that our privacy preferences and behaviours are malleable and able to be influenced by those who would manipulate context to their advantage. It is also necessary to discuss what improper uses of data could undermine these frameworks that rely on notice and consent.

B: Improper Uses of Personal Data

Cambridge Analytica

The mass data breach of Facebook in 2014 facilitated by Cambridge Analytica is one example of data misuse on a large scale. The settings of Facebook

---

[198] Solove, above n 185, at 12.

[199] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein "Privacy and Human Behaviour in the Age of Information" (January 30th 2015) VOL 347 ISSUE 622, at 1.

[200] Ryan Calo "Digital Market Manipulation" (August 2014) Geo. Wash. L. Rev. 82, 995–1304, at 36.

[201] Acquisti, Brandimarte, and Loewenstein, above n 199, at 1.

allowed developers to access data related to the user's friends without their knowledge or consent.[202] The data itself was specific to each person and could contain names, email addresses and personal messages.[203] One of these developers was Aleksander Kogan, a lecturer at the University of Cambridge in the Department of Psychology. In the spring of 2014, he developed the GSR App that collected data from participants at an individual level. Mr Wylie described the data obtained from Dr Kogan's GSR App as the foundation dataset of the Cambridge Analytica company, which collected data on up to 87 million users Facebook profiles.[204] When Facebook questioned him about his application, Kogan claimed his research was for solely academic purposes.[205] Psychographic profiling was then used to micro-target adverts at voters in the lead up to the 2014 US election, across five distinct personality groups.[206] After the campaign, according to a presentation document seen by the Committee, the company claimed that there was a 39% increase in awareness of the issues featured in the campaign's advertising amongst those who had received targeted messages.[207] Cambridge Analytica would later claim that the 1.5 million advertising impressions they generated through their campaign led to a 30% uplift in voter turnout, against the predicted turnout, for the targeted groups.[208]

Assessing the clear impact of this misuse of data against the five key features of democracy identified in the Workshop Report shows some fundamental

---

[202] Sandy Parikilas Oral Evidence "Submission to the Digital, Culture, Media & Sport Committee Fake news inquiry 2017" at Q1189.

[203] Digital, Culture, Media and Sport Committee *Disinformation and 'fake news': Interim Report* (Fifth Report, Session 2017–19, HC 363, 29th July 2018).

[204] Digital, Culture, Media and Sport Committee, above n 203, at 113.

[205] Zuboff, above n 16, at 281.

[206] Digital, Culture, Media and Sport Committee, above n 203, at 110.

[207] Digital, Culture, Media and Sport Committee, above n 203, at 110.

[208] Digital, Culture, Media and Sport Committee, above n 203, at 110.

flaws in policing notice and collection based frameworks.[209] By targeting individuals with personalised advertising based on information that they did not freely consent to give, it cannot be said that individuals could be capable of making active or informed decisions, or make important moral judgements. Furthermore, if voting patterns are impacted, it is clear that the electoral process itself may have been disrupted.

Unknown Threats

At a greater level of abstraction, another consequence of disclosing data is the further uses it could be put towards. We know from Cambridge Analytica that disclosures of data without restrictions as to their future use can have detrimental societal impacts. What is equally challenging is that much of the value of data is not apparent at the time when it is collected, when individuals consent for its use.[210] As Solove argues, the ways data or personal information could be used are extremely vast.[211] Without set limits and accountability for usage, it is almost impossible for people to assess the dangers that come with digital companies holding their data.[212]

C: Modern Enforcement Mechanisms

NZ Privacy Commissioner response to Cambridge Analytica

The last time the Privacy Commissioner tried to enforce notice on a major technology company the results were relatively futile. On the third of April

---

[209] These are as follows; Electoral process and pluralism, active informed citizens, shared democratic culture, civil liberties and competitive economy and trust in authority in Marianne Elliott and others, *Digital Threats To Democracy*, (The Workshop, May 2019) at 12.

[210] Cate, Mayer-Schönberger, above n 162, at 1.

[211] Solove, above n 165, at 1.

[212] Cate, Mayer-Schönberger, above n 162, at 2.

2018, John Edwards named Facebook as non-compliant with New Zealand privacy law. This was because 64,000 New Zealander's saw their data shared without permission in the Cambridge Analytica scandal.[213] In light of complaints made by individuals to the Commissioner, he requested that Facebook release the information on those complainants. Stephen Deadman (the Global Deputy Chief Privacy Officer of Facebook) stated that Facebook was not required to comply with the New Zealand Privacy Act (the requests would violate Irish Data protection law and that is the company that provides the Facebook service in New Zealand). Then, even if the Act applied, Facebook would not be legally required to disclose the information requested. This was because it would violate the data protection rights of the New Zealander's concerned.[214]

CNIL Fines on Google

The GDPR, on the other hand, does have greater power in holding large tech companies to account. On the 21st January 2019, France's data-privacy regulator (CNIL), imposed a fine of €50 million on Google for breaches of the General Data Protection Regulation (GDPR).[215] The two complaints principally concerned "consent," with CNIL accusing Google of lacking a transparent legal basis for processing individuals data. This was due to the fact people were forced to consent to processing they did not understand.[216] Particularly, customers were not asked for their consent for personalised advertising. Instead, they were required to agree to Google's Terms and

---

[213] John Edwards "Facebook: What this is really about" (3rd of April 2018) <https://www.privacy.org.nz/blog/facebook-what-this-is-really-about/>.

[214] Edwards, above n 213.

[215] Shannon Closey, Rachel O'Brien and Joe Edwards "Google faces record NZ$85 million fine for GDPR violations" (January 23rd 2019) <https://www.russellmcveagh.com/insights/january-2019/google-faces-record-nz-85-million-fine-for-gdpr-vi>.

[216] Closey, O'Brien and Edwards, above n 215.

Privacy Policy to access services. On this basis, CNIL concluded that Google had failed to meet the GDPR's consent requirements.[217]

So will these penalties create the necessary deterrent for further misuses of data? In the case of events such as Cambridge Analytica, where consent and knowledge were not necessary, these increased protections surrounding consent, and large fines, may not prevent the events that are of the most concern to regulators. Perhaps regulators' focus could move toward frameworks that focus upon provisions that identify problems before or as they arise. I have referred to these as "ex-ante" provisions. One of those adopted by the GDPR is the Privacy By Design provision.

GDPR "Readiness"

While these concerns may exist, research also shows that digital companies are striving to reach GDPR obligations. Among the respondents in the Data Privacy Benchmark Study, 59% of companies claimed they were meeting all requirements.[218] Another 29% stated they would be compliant within a year.[219] I would suggest that what GDPR 'readiness' actually means is a question that is yet to be answered, as there are many new provisions within the GDPR that are yet to be applied and interpreted. One such provision is Privacy By Design requirements, identified by 34% of organisations as being one of the biggest challenges associated with compliance.[220] The provision was suggested in seven submissions to the Select Committee concerning the Privacy Bill. Catalyst IT submitted that such a requirement could help to address privacy

---

[217] Closey, O'Brien and Edwards, above n 215.

[218] Data Privacy Benchmark Study *Maximizing the value of your data privacy investments* (Cisco, January 2019) at 4.

[219] Data Privacy Benchmark Study, above n 218, at 4.

[220] Data Privacy Benchmark Study, above n 218, at 5.

issues in early stages where it may be less costly to do so.[221] Notwithstanding these endorsements, the Law Commission's initial report recommended no change.[222] It was stated that it would run against the flexible nature of the privacy principles for the Act to specify any measures must be taken.[223] The Ministry of Justice's departmental report also agreed, citing that there were other ways to encourage agencies to adopt privacy-enhancing technologies.[224]

Chapter 5: Privacy By Design

GDPR Interpretation of Privacy By Design

This provision is given effect in Article 25 of the GDPR.[225] It is a broadly based provision, stating that digital companies must implement appropriate technical and organisational measures to integrate the necessary safeguards into data processing. This must be done while addressing the competing interest of the data protection rights of individuals.[226] Given the expansive requirements, there is some ambiguity as to what the term should mean, along with how it should be implemented.[227]

A: Design Importance and Manipulation

Importance of Design

[221] Ministry of Justice, above n 10, at 44.

[222] Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011) at 259.

[223] Ministry of Justice, above n 10, at 44.

[224] Ministry of Justice, above n 10, at 49.

[225] General Data Protection Regulation 2018, Article 25(1) and (2) Data protection by design and by default.

[226] General Data Protection Regulation 2018, Article 25(1) and (2) Data protection by design and by default.

[227] Intersoft Consulting "Key Issues, Privacy By Design" <https://gdpr-info.eu/issues/privacy-by-design/>.

Woodrow Hartzog argues that we place too much emphasis on our current frameworks on the collection, use and disclosure of information.[228] He suggests legal frameworks should begin to prioritise the role of design. A common theme of traditional frameworks is that users, not technologies are to blame for privacy violations. These technological neutrality arguments have political appeal and are used to shift lawmakers' focus away from technologies and toward bad actors using those technologies.[229] As our principle-based frameworks do not give any specific technology mandates or guidance, privacy law seems to gloss over design.[230]

Indeed, the phrase is often used as a marketing slogan rather than as a plan for privacy control.[231] At some level, this seems to be understandable, given the complex nature of the concept itself. Privacy in this sense can be referred to as the rules or norms that govern action or inaction relating to our personal information.[232] Design refers very broadly to how a system is architected, its function, along with how that function affects people.[233] The term can itself can be seen to refer to the self-regulatory measures taken by digital companies.[234] As previously discussed in chapter 4, many privacy laws focus to protect the harmful collection, use and disclosure of personal information. While these are essential, it seems further protections must be provided to prevent harmful events like Cambridge Analytica, that do not require consent or notice, but rather take advantage of the systems used by digital companies.

---

[228] Hartzog, above n 184, at 50.

[229] Hartzog, above n 184, at 50.

[230] Hartzog, above n 184, at 61.

[231] Hartzog, above n 184, at 62.

[232] Neil M Richards "Four Privacy Myths," in a *World Without Privacy: What Law Can and Should Do?* (New York, Cambridge University Press, 2015), at 33-82.

[233] Hartzog, above n 184, at 12.

[234] Hartzog, above n 184, at 5.

Hartzog argues that privacy law is deficient because it ignores design.[235] In this chapter I will explore this concept and whether it should be introduced into the New Zealand Privacy Bill.

In a world where digital companies have dominance, most threats of privacy harm are not obvious. This is because they are incremental. Slowly our data is gathered. As information privacy harms are small and dispersed between many individuals, courts and lawmakers fail to realise them. There are also other barriers to implementing a privacy by design provision. Regulation could impede innovation and progress. It could also undermine the flexibility of the legal frameworks that are currently employed. It seems that the design of popular technologies, including these online platforms and digital markets, could be critical to the protection of privacy.[236] The design could and should be a way to protect privacy-related values like trustworthiness and autonomy for individuals. It seems that design may be more capable of protecting personal information than laws targeting the actions of the controllers of data. If these companies were to commit themselves to provide privacy by design, they could ultimately earn the trust of individuals and governments.[237]

Design methods used by digital companies

Design is a form of power.[238] It is such because people react to design in predictable ways. There is much literature dedicated to harnessing the power of design in policy and industry. For some examples, rooms are built that allow natural light to flow into them. Exposure to this can increase workplace

---

[235] Hartzog, above n 184, at 6.

[236] Hartzog, above n 184, at 7.

[237] Hartzog, above n 184, at 9.

[238] Hartzog, above n 184, at 34.

performance.[239] Additionally, walks from airplanes to baggage claim areas are deliberately long, so that the wait time at the baggage claim feels shorter in duration.[240] I would suggest that some of the most important decisions concerning privacy are made before signing up to an app, rather, in the design itself. Hartzog uses the example of app developer Goldenshores Technologies. That company designed a flashlight app, that collects the user's geolocation data. A flashlight app does not require this data and thus, it seems the collection itself was unnecessary. It was likely designed to collect location data because it is financially advantageous to do so.[241] Hartzog compares this choice with the design decision to Gizmodo, a tech media outlet, who had designed their services to not store IP addresses of those who visit its website. Annalee Newitz explained the decision by stating that "we don't log that data, period. And we chose to set up our commenting system that way because we want to protect your right to speak freely and anonymously."[242] Perhaps the issue in the past is letting these digital companies self regulate themselves. Most will be incentivised to continue to maximise profits at the expense of protecting individuals data.

On another note, protective designs over personal information have other indirect benefits for society. Granted, they may also frustrate law enforcement and reduce cybersecurity in the process. Importantly though, they may still address abuses of processes by governments and attacks from hackers.[243] One example of this is Apple's encryption system for mobile devices. Essentially,

---

[239] Christopher Bergland, "Exposure to Natural Light Improves Workplace Performance," *Psychology Today*, (online ed, June 5 2013).

[240] Alex Stone, "Why Waiting Is Torture," *New York Times* (online ed, New York, August 18th 2012).

[241] Hartzog, above n 184, at 24.

[242] Annalee Newitz "And This Is Why Gizmodo Doesn't Collect IP Address Data," Gizmodo (June 10 2015) <https://gizmodo.com/and-this-is-why-gizmodo-doesn't-collect-ip-address-data-1710446008>.

[243] Hartzog, above n 184, at 25.

the company could not disclose information about those using these devices. An example of enforcement was Apple's refusal to co-operate with the FBI in accessing the phone of a terrorism suspect in the California shootings.[244] It seems these restrictions may be necessary to ensure the freedom and autonomy necessary for human development and commerce, whilst also strengthening national security.[245]

Hartzog also suggests that the frequency of errors online point towards design flaws. He suggests that even though we can be more careful online, companies must be failing to design software to help obvious human error.[246] This coincides with some of the earlier analysis of the failures of traditional collection methods in data protection frameworks. A further example of this was when computer scientists from Columbia University carried out a usability study of privacy settings using Facebook as an example. Conclusively, they found that privacy settings do not match users sharing intentions. The majority of participants also suggested they would not fix the problems they created. To these scientists, one central conclusion was that a completely different approach is needed.[247] This research shows that technological design can make us feel in control or frustrate us. It is also difficult to get right. It seems important that design should seek to anticipate human errors and look to protect personal information. Although researchers study design, along with companies investing heavily in it, one cannot help but conclude that privacy law itself has failed to take design seriously.[248]

---

[244] Alex Hern "Apple's Encryption Means It Can't Comply with US Court Order" *The Guardian* (September 2015), <http://www.theguardian.com/technology/2015/sep/08/apple-encryption-comply-us-court-order-iphone-imessage-justice>.

[245] Hartzog, above n 184, at 25.

[246] Hartzog, above n 184, at 33.

[247] Michelle Madejski, Maritza Johnson, Steven M Bellovin *A study of privacy settings errors in an online social network* (Budapest: IEEE, 2012).

[248] Hartzog, above n 184, at 34.

B: Setting standards for privacy by design

The central challenge for privacy design policy is to find the balance between over and under regulation. Too few boundaries would fail to prevent technologies that exploit individuals. Too many could stifle commerce and impede technological progress. Those who forward innovation suggest that adopting a "precautionary principle" in regulating technology would be unfairly incursive. Adopting such a principle would suggest that innovations should be disallowed until developers can prove the technology will not harm people.[249] One important part of design will be finding the balance of how much regulation is necessary.

Fundamental aspects of design

On the one hand, well-designed objects are easily understood. On the other, poorly designed objects are difficult to use. They do not provide visible hints or provide those that are deceptive or misleading. Don Norman describes the fundamental principles of designing for people are to "(1) Provide a good conceptual model and (2) Make things visible."[250] The keys to these two principles are in the visible structure of objects, namely, in their affordances, constraints and mappings. Norman's definition of affordances is that they are the properties of something that determine how it could be used. In reference to technological design, this could refer to web pages, for example, where boxes are to be checked, or where a hyperlink changes the cursor's shape. Mapping refers to the relationships between controls and their movements that result. Cursors mimic the movements of a touchpad, while icons all rely upon mapping to point us towards the use of an interface. Constraints are the physical properties of objects that constrain possible operations. For one

---

[249] Hartzog, above n 184 at 85.

[250] Don Norman *The Design of Everyday Things* (New York, Basic Books, 1988), at 2.

example, social norms can act as a constraint. Password prompts along with two-factor authentication schemes are examples of technological designs preventing third parties from accessing information.

Norman formulates several principles for using design:

1. Simplify the structure of tasks (i.e. require users to take fewer steps).
2. Make an object's use obvious from its visual elements, and make important design elements obvious.
3. Get mappings right, (i.e. make tasks performed on or with the object correspond intuitively with their results in the world).
4. Exploit the power of constraints, both natural and artificial.
5. Design for (human) error.[251]

Of course, not all issues can be addressed by design. Determining those values directly impacted by design should be focused upon, whilst the rest can be left to the other protections granted under privacy law.[252] Hartzog suggests that there are several issues in design worth focussing upon. Three of those are trust, obscurity and autonomy.

Trustworthiness

A privacy self management approach within the law is flawed as it asks users to shoulder all the risks of disclosure.[253] I would suggest that trustworthiness is the most important privacy value in the digital economy. For example, if you consider sites like Amazon. A site like this knows any given individuals browsing, listening and viewing habits. They give recommendations on what products people may wish to purchase. In a hypothetical situation, after

[251] Norman, above n 250, at 188.

[252] Hartzog, above n 184, at 94.

[253] Hartzog, above n 184, at 97.

realising the company has recklessly sold that information away for an improper purpose, this would most likely make those individuals feel betrayed. Despite this, through the use of 'notice,' the responsibility of Amazon is abrogated. Neil Richards suggests this is one of the failures of privacy self management.[254] It punishes people for trusting these digital companies. Trust and the value it can create can and should be nurtured through the design of information technologies. The Computer Science and Telecommunications Board referred to the terms trust and trustworthy to describe systems that were predictably correct, reliable and capable of survival.[255] Individuals entrust information to companies all the time. Once this personal information switches hands, those individuals have effectively lost control.

So how can the law further the value of trustworthiness through design? Trustworthiness can add nuance to concepts like discretion, honesty, protection and loyalty. These are not new qualities, rather they are some of the most established legal concepts. Take for example the goal of fiduciary law. Generally, fiduciaries owe a duty of care to those who place their trust in them. Perhaps digital companies should have a duty to look out for the interests of people, particularly as it is their personal data they can make a profit from.[256] One way to build trust is for companies to create designs that facilitate signals and transaction costs to create expectations of discretion. Hartzog refers to these as discretion indicators. One example of this is the ability of individuals to adjust privacy settings so that posts are available to "friends only," for just one example.[257] Technologies could also be designed to accommodate requests

---

[254] Neil Richards and Woodrow Hartzog "Taking Trust Seriously In Privacy Law" Stanford Technology Law Review 19 (2016) 431-472.

[255] Computer Science and Telecommunications Board, National Research Council *Trust in Cyberspace*, ed. Fred Schneider (Washington, DC, National Academies Press, 1999) at 11.

[256] Hartzog, above n 184, at 101.

[257] Hartzog, above n 184, at 101.

for inspection. One application of this is Facebook designing its software in a way that allows users to download their data.[258] Companies could also design themselves according to updated threat models with the objectives of minimising data collection and storage, along with preparing data breach responses.[259]

Autonomy

In terms of autonomy, we should resist the traditional approaches of emphasising individuals' ability to control how all of their personal information is collected, used and shared.[260] Design should not be burdened with so many practical controls that it overwhelms individuals.[261] Rather, it should give individuals control where it is most important and useful to do so, without these complications. Control must be distinguished from autonomy. The terms are not synonymous. Well-formed design should facilitate individuals without providing unnecessary confusion. If designs are transparent and easily able to be followed, individuals can be seen to exercise these levels of autonomy. Technological design could be seen to serve autonomy when it allows individuals to freely enter trust relationships that create and maintain obscurity.[262] By collectively overwhelming people with control that relies upon consent to the collection, use and disclosure of personal information, designers can abrogate responsibility for harmful design while claiming to give others the control they want.[263]

---

[258] Facebook, "Downloading Your Info," <https://www.facebook.com/help/131112897028467>.

[259] Hartzog, above n 184, at 105.

[260] Hartzog, above n 184, at 95.

[261] Hartzog, above n 184, at 95.

[262] Hartzog, above n 184, at 117.

[263] Hartzog, above n 184, at 118.

Obscurity

Furthermore, to maintain relative privacy, or obscurity, individuals should be able to rely on the designs of our online environments to make certain personal information more difficult to access.[264] Digital companies or individuals could routinely hide information by making it invisible to search engines through the use of pseudonyms, or multiple profiles that take advantage of privacy settings.[265] One example is search visibility. This is the degree to which individuals and the content they produce are locatable and accessible through an online search.[266] Designers could also offer users control over the inclusion of their information in both internal and external search services. A modest application could be Facebook search ability becoming limited to friends of friends.

C: Summing Up

It is important to note that traditional disclosure regimes should be treated as necessary but not absolute. They should be treated alongside design interventions so that individuals can be confident that their data is protected while minimising the costs to digital companies.[267] Design interventions must also be proportionate to the threat that any given design poses. While many tools are already established, further research is necessary to achieve the right balances and fits.

Design policy could include more than legal prohibitions. Hartzog refers to these regimes as “soft” whereby they do not impose penalties on companies

---

[264] Hartzog, above n 184, at 96.

[265] Hartzog, above n 184, at 112.

[266] Hartzog, above n 184 at 112.

[267] Hartzog, above n 184, at 151.

for going outside the set boundaries of design.[268] These would be the least intrusive into design processes while being aimed to educate digital companies and individuals about design. This makes these responses better suited for designs that affect people in more subtle or ambiguous ways.[269] Where these approaches are insufficient, regulators could look to moderate approaches that impose certain obligations on designers. The next step would be outright bans along with formidable controls on design decisions that have more robust responses.[270] These could impose tort liability or outright categorical prohibitions.

While traditional frameworks may be sufficient for most improper uses of data, those posed by the largest digital companies may continue to evade responsibility. As technologies are involved in nearly every act of collection, use and disclosure, their architecture should also be an essential part of information privacy. It seems that the design of information technologies currently faces little scrutiny.[271] Of course, even well-formed privacy by design will not provide all the answers. While this may be true, it could be one method to begin remedying the larger issues that are posed by the mass collection of data in the digital economy. If these digital companies can use data to make a profit, it only seems reasonable that they design information technology systems in ways that can protect individuals' data. The outcomes suggested by Hartzog could be expanded upon. These focus on trustworthiness, obscurity and autonomy as enabling values. Autonomy should also be prioritised over consent and control. In creating an environment for this informed choice, it seems areas such as the design of technologies should be considered for regulatory intervention. These interventions could help mitigate asymmetric information, cognitive biases and aggregation effects. A

[268] Hartzog, above n 184, at 161.

[269] Hartzog, above n 184, at 161.

[270] Hartzog, above n 184, at 159.

[271] Hartzog, above n 184, at 277.

diverse approach is also necessary to create policy that does not stifle innovation but also appropriately safeguards personal data. The points touched upon are merely a starting point. This area requires more research and development before it is implemented.

Chapter 6: A digital markets unit and adequacy

Digital Markets Unit

Regulation across these different sectors needs to be strengthened to address the impacts of the digital economy. Several reports have indicated that the creation of a specialist body to co-ordinate regulators may be the next appropriate step.[272] New Zealand could also establish such a body to continue to research and apply standards. A body like this could have several functions. One could be to continually assess regulation in the digital world, making recommendations on where additional powers are necessary. It could inform Parliament of technological developments, engage with the tech sector, along with raising awareness of the issues connected to the digital world.[273] The unit could also be in regular communication with other international bodies, such as those enforcing the GDPR. If New Zealand were to seek to implement standards like privacy by design and data mobility, they could look to these other bodies for further guidance.

Code of Conduct

Digital companies that achieve dominance hold large amounts of power as to how users access the market. This can result in direct harm to individuals,

---

[272] See the House of Lords Select Committee on Communications *Regulating in a digital world* (9th March 2019) at 62, and Jason Furman and others *Unlocking Digital Competition* (Digital Competition Expert Panel, March 2019), at 5.

[273] House of Lords Select Committee on Communications, above n 55, at 68.

particularly concerning data privacy. The unit could research the creation of a voluntary code of conduct for digital platforms. This could be set around core principles for companies that have this strategic market status to abide by. The unit could also look to other jurisdictions, such as the European Commission's plans to introduce a similar platform to business regulations. These proposals are based upon a range of requirements for these companies to be more transparent about their practices. They also will include voluntary codes of conduct for providers of online services.[274]

Creating this code of conduct could help facilitate more competitive outcomes. It can extend beyond the reach of existing competition and data protection frameworks, to clarify situations that are currently unclear or legal.[275] The aim of such a unit should be to achieve fast resolutions, through working alongside and participating with affected parties. Moving towards a system that incorporates an increasing amount of ex-ante monitoring and enforcement of clear standards may be a more efficient way of regulating the digital economy. This could prevent negative outcomes before they occur.[276]

The unit could also be charged with enabling greater data mobility where the tool will increase competition and individuals choice. It could host what is known as a 'sandbox,' where innovators build and test propositions making use of consumer data in a safe environment. In doing so, it could look to the experiences of the Financial Conduct Authority in the implementation of Open Banking.[277] Additionally, the body could enforce ethical design standards to be complied with by companies. There are strong arguments that ethical

---

[274] Regulation (EU) 2019/1150 of the European Parliament and of the Council *Promoting fairness and transparency for business users of online intermediation services* (20 June 2019) PE/56/2019/REV/1, OJ L 186, 11.7.2019, at 57–79.

[275] Furman and others, above n 4, at 62.

[276] Furman and others, above n 4, at 63.

[277] Financial Conduct Authority "Regulatory sandbox" <https://www.fca.org.uk/firms/regulatory-sandbox>.

standards, such as safety and privacy, should be incorporated into the design of technology and delivered by default.[278] A warning from the unit could trigger further cause for concern from other international bodies, with consensus providing compliance from digital companies.

GDPR Adequacy

Currently, New Zealand is one of only twelve countries that has EU 'adequacy status.' This means that businesses and organisations can send personal information to New Zealand without applying further safeguards.[279] Our status will be reviewed in light of the GDPR's new standards that will be put in place on the 25th of May 2020.[280] Agencies in New Zealand may be forced to comply with international practices. Business requirements and contractual obligations could likely be based around the GDPR in the future. Therefore, maintaining GDPR adequacy is another important element. This may work in regulators' favour, as provisions like data portability and privacy by design will already be enforced by the GDPR. Working together to research these standards with European authorities may make enforcement less complex, given their power. Additionally, this gives further impetus for authorities within New Zealand to research and adopt provisions of the GDPR that promote some of these competing standards. In doing so, however, some of the novel complex provisions of the GDPR that do not fit the New Zealand context may be left alone for future research. Any reform must be tailored to work in the New Zealand context rather than directly imported.[281] The rates of change posed by the digital economy also mean there is a need for ongoing

---

[278] House of Lords Select Committee on Communications, above n 55, at 19.

[279] Ministry of Justice, above n 10, at 37.

[280] Ministry of Justice, above n 10, at 37.

[281] Ministry of Justice, above n 10, at 38.

reviews of legislation. This is another aspect that the Digital Markets Unit may be able to oversee, in tandem with the Privacy Commissioner.

Conclusion

The digital economy is growing at incredible rates. It provides many opportunities, but alongside these come great challenges. In seeking to achieve the impossible task of finding the best way to promote societies interests through the use of their data, I have endeavoured to maintain certain propositions. One is that data gives digital companies market power. It is also a key feature of their business models. Thus, digital companies with the largest data silos pose the greatest threats. I suggest that when large digital companies use data for improper purposes, it can have detrimental effects not only for any given individuals' privacy but also for democracy itself. This should be where regulation is the most stringent. It also means that certain areas of law, like competition and data protection policy, can often be intertwined when addressing the challenges of the digital economy. Business models where individuals gain free services in exchange for their personal data shows these often competing objectives.

In regulating the digital economy, I have also suggested that frameworks should move towards a greater reliance on ex-ante approaches, as opposed to those that are ex-post. Researching an ethical design provision could help in facilitating informed choice for individuals when they disclose information. Carefully designed systems could also prevent data breaches before they arise. Digital companies would also have to follow standards of compliance in their design of information technologies. Additionally, a data mobility provision may facilitate competition by lowering barriers to entry in digital markets. It could also give individuals more power over their data while taking some away from large incumbent firms. Perhaps this would facilitate dynamic efficiency, in realising the many opportunities and benefits of the digital

economy. Similar provisions to these are included within the GDPR. This could play a part in mitigating the issues of transnational enforcement as EU authorities may have more success in holding digital companies to account. The creation of a new digital markets unit could be tasked with providing some of these new changes. Its aim could be to ensure effective and timely policy-making. This is essential as the speed at which the digital economy is growing and changing poses serious challenges to regulators around the globe.

BIBLIOGRAPHY

A. Cases

Harder v Proceedings Commissioner [2000] 3 NZLR 80.

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

B. Legislation

1. New Zealand

Commerce Act 1986.

Privacy Act 1993.

2. Europe

General Data Protection Regulation 2018.

3. Bills

New Zealand

Privacy Bill 2018 (34-2).

C. Official Documents

Australian Competition and Consumer Commission *Digital Platforms Inquiry – Preliminary Report* (December 2018).

Australian Productivity Commission and New Zealand Productivity Commission *Growing the digital economy in Australia and New Zealand.* Maximising opportunities for SMEs, Joint Research Report, (January 2019).

Commerce Commission New Zealand *Mergers and Acquisitions Guidelines* (July 2013).

Directorate General For Internal Policies Policy Department A: Economic and Scientific Policy, *Challenges for Competition Policy in a Digitalised Economy* (IP/A/ECON/2014-12 July 2015 PE 542.235).

House of Lords Select Committee on Communications *Regulating in a digital world* (9th March 2019).

House of Commons Digital, Culture, Media and Sport Select Committee *Disinformation and 'fake news'*: *Final Report* (February 2019).

Law Commission *Review of the Privacy Act 1993* (NZLC R123, 2011).

Ministry of Business, Innovation and Employment *Business Information and Communication Technology (ICT) use and productivity growth in New Zealand* (October 2017).

Ministry of Justice *Departmental Report - Part One, Privacy Bill* (13th March 2019).

Ministry of Justice *Departmental Report - Part Two, Privacy Bill* (13th March 2019).

Organisation for Economic Co-operation and Development *Big data: bringing competition policy to the digital era* (November 2016).

Regulation (EU) 2019/1150 of the European Parliament and of the Council *Promoting fairness and transparency for business users of online intermediation services* (20 June 2019) PE/56/2019/REV/1, OJ L 186, 11.7.2019.

D. Secondary Material

1. Books and Chapters in Books

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

Computer Science and Telecommunications Board, National Research Council *Trust in Cyberspace*, ed. Fred Schneider (Washington, DC, National Academies Press, 1999).

Don Norman *The Design of Everyday Things* (New York, Basic Books, 1988).

Matt Sumpter *New Zealand Competition Law and Policy* (CCH, Auckland, 2010).

Maureen Brunt *Economic Essays on Australian and New Zealand Competition Law* (The Hague, Kluwer Law International, 2003).

Neil M Richards "Four Privacy Myths," in a *World Without Privacy: What Law Can and Should Do?* (New York, Cambridge University Press, 2015).

Shoshana Zuboff *The Age of Surveillance Capitalism* (Hachette Book Group, New York, 2019).

Thomas Friedman *The world is flat: a brief history of the twenty-first century* 1st ed (Farrar, Straus and Giroux, New York, 2005).

Whish, *Competition Law* 6th ed (Oxford University Press, Oxford, 2009).

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

2. Journal Articles

Alessandro Acquisti, Laura Brandimarte, and George Loewenstein "Privacy and Human Behaviour in the Age of Information" (January 30th 2015) VOL 347 ISSUE 622.

Bundeskartellamt Case Summary *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for data processing* (B6-22/16, 15th February 2019).

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

Daniel J Solove 'Why Privacy Matters Even if You Have Nothing To Hide' *The Chronicle of Higher Education* (2011).

Daniel Rubinfeld, Michal Gal "ACCESS BARRIERS TO BIG DATA" Arizona Law Review, (2017) VOL. 59:339.

Fred Cate, Viktor Mayer-Schönberger "Notice and Consent in a World of Big Data" (2013) Articles by Maurer Faculty, 2662.

Herve Boulhol, Alain de Serres and Margit Molnar "The contribution of economic geography to GDP per capita," (2008) OECD Journal, Economic Studies, vol. 2008, issue 1, 1-37.

Neil Richards and Woodrow Hartzog "Taking Trust Seriously In Privacy Law" Stanford Technology Law Review 19 (2016) 431-472.

Ryan Calo "Digital Market Manipulation" (August 2014) Geo. Wash. L. Rev. 82, 995–1304.

3. Papers and reports

Article 29 Data Protection Working Party *Guidelines on the right to data portability* (16/EN WP 242 rev.01, 5th April 2017).

Ctrl-Shift, Department for Digital, Culture, Media and Sport *DATA MOBILITY: The personal data portability growth opportunity for the UK economy* (2018).

Data Privacy Benchmark Study *Maximizing the value of your data privacy investments* (Cisco, January 2019).

Diane Coyle *Practical competition policy implications of digital platforms* (University of Cambridge, March 2018).

Digital, Culture, Media and Sport Committee *Disinformation and 'fake news': Interim Report* (Fifth Report, Session 2017–19, HC 363, 29th July 2018).

Elena Argentesi and others *Ex-post Assessment of Merger Control Decisions in Digital Markets* (Lear, June 2019).

Erik Brynjolfsson, Felix Eggers and Avinash Gannamaneni *Using massive online choice experiments to measure changes in well-being* (National Bureau of Economic Research, C82, I30, O40, April 2018).

Hayden Glass and others *Data Driven Innovation in New Zealand* (Sapere Research Group & Covec, 2015).

Jason Furman and others *Unlocking Digital Competition* (Digital Competition Expert Panel, March 2019).

Marc Bourreau, Alexandre de Streel and Inge Graef *Big Data and Competition Policy: Market power, personalised pricing and advertising* (Cerre, 16 February 2017).

Marianne Elliott and others *Digital Threats To Democracy* (The Workshop, May 2019).

Markus Eurich, Michael Burtscher *The Business-to-Consumer Lock-in Effect* (University of Cambridge, August 2014).

Michelle Madejski, Maritza Johnson, Steven M Bellovin *A study of privacy settings errors in an online social network* (Budapest: IEEE, 2012).

Rahul Matthan *Beyond consent: A new paradigm for data protection* (Takshashila Discussion document 2017-03).

Renato Nazzini *Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision* (Competition Policy International, March 2019).

Rishab Bailey and others "Disclosures in privacy policies: Does notice and consent work?*"* (NIPFP Working Paper 246, December 2018).

4. Submissions

British and Irish Legal Education and Technology Association (BILETA) (IRN0029) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

Competition and Markets Authority (IRN0100) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

Doteveryone (IRN0028) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

Dr. Shehar Bano (IRN0114) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

Jennifer Cobbe and Professor John Naughton, Trustworthy Technologies Strategic Research Initiative, University of Cambridge (IRN0031) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

Sandy Parikilas Oral Evidence "Submission to the Digital, Culture, Media & Sport Committee Fake news inquiry 2017."

The Entrepreneurs and Adam Smith Institute (IRN0070) "Submission to the House of Lords Select Committee on Communications, Regulating in a digital world, March 2019."

5. Newspaper and Magazine Articles

Alex Stone, "Why Waiting Is Torture," *New York Times* (online ed, New York, August 18th 2012).

Christopher Bergland, "Exposure to Natural Light Improves Workplace Performance," *Psychology Today*, (online ed, June 5 2013).

Jennifer Cobbe "Reigning in Big Data's Robber Barons" *NYR Daily* (online ed, New York, 12 April, 2018).

"Mark Zuckerberg calls for stronger regulation of internet" *The Guardian* (online ed, London, 30 March 2019).

6. Ebooks

Paul Roth, *Privacy Law in Practice*, John Lulich (ed) *Privacy Commissioner makes recommendations for Privacy Act reform,* Judith Collins (looseleaf ed, Lexis Nexis) at [CD.1], 2017.

7. Internet Resources

Alex Hern “Apple’s Encryption Means It Can’t Comply with US Court Order” *The Guardian* (September 2015), <http://www.theguardian.com/technology/2015/sep/08/apple-encryption-comply-us-court-order-iphone-imessage-justice>.

Annalee Newitz "And This Is Why Gizmodo Doesn’t Collect IP Address Data” Gizmodo (June 10 2015) <https://gizmodo.com/and-this-is-why-gizmodo-doesn't-collect-ip-address-data-1710446008>.

BSI “Internet of Things Enabling a Smart and Secure World” <https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/>.

Data Transfer Project “About us” (2018) <https://datatransferproject.dev/>.

Department of Business Innovation & Skills and the Rt Hon Edward Harvey “The midata vision of consumer empowerment” (November 3rd 2011) <https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment>.

eMarketer “Digital Duopoly to Remain Dominant in UK Ad Race” (September 2017) <https://www.emarketer.com/Article/Digital-Duopoly-Remain-Dominant-UK-Ad-Race/1016481>.

Facebook, “Downloading Your Info” <https://www.facebook.com/help/131112897028467>.

Financial Conduct Authority "Regulatory sandbox" <https://www.fca.org.uk/firms/regulatory-sandbox>.

Finextra ‘Midata initiative launches to help Brits pick best bank account providers’ (March 2015) <https://www.finextra.com/newsarticle/27168/midata-initiative-launches-to-help-brits-pick-best-bank-account-providers>.

Information Commissioners Office, ‘Right to data portability’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>.

Intersoft Consulting “Key Issues, Privacy By Design” <https://gdpr-info.eu/issues/privacy-by-design/>.

John Edwards “Facebook: What this is really about" (3rd of April 2018) <https://www.privacy.org.nz/blog/facebook-what-this-is-really-about/>.

Nesta 2017-2020 “What we want to achieve” <https://media.nesta.org.uk/documents/nesta_strategy_2017-2020.pdf>.

Markets Insider ‘“2.7 billion people can’t be wrong: Here’s what Wall Street is saying about Facebook earnings” (31 January 2019), <https://

markets.businessinsider.com/news/stocks/facebook-stock- price-earnings-revenuewall-street-2019-1-1027913555>.

Nick Ismail, “Tech Nation 2018 report: UK tech expanding faster than the rest of the economy,” <https://www.information-age.com/tech-nation-2018-report-uk-tech-faster-economy-123471982/> (17 May 2018).

Nick Statt *Google appeals record €2.4 billion antitrust fine over manipulated search results*, The Verge <https://www.theverge.com/2017/9/11/16291482/ google-alphabet-eu-fine- antitrust-appeal>.

PwC 2018 “Open Banking 101” <https://www.pwc.com.au/banking-capital-markets/banking-matters-hot-topic-open-banking-101.pdf>.

Shannon Closey, Rachel O'Brien and Joe Edwards “Google faces record NZ$85 million fine for GDPR violations” (January 23rd 2019) <https://www.russellmcveagh.com/insights/january-2019/google-faces-record-nz-85-million-fine-for-gdpr-vi>.

Sir Tim Berners-Lee “One Small Step for the Web…” <https://medium. com/@timberners_lee/one-small-step-for-the-web-87f92217d085>.

statcounter GlobalStats “Search Engine Market Share Worldwide,” August 2019, <https://gs.statcounter.com/search-engine-market-share#monthly-201808-201908>.