Volume **3** (1) 2021 https://doi.org/10.5204/lthj.1595

Beyond Privacy: Protecting Data Interests in the Age of Artificial Intelligence

Matt Bartlett
The University of Auckland, New Zealand

Abstract

Serious challenges are raised by the way in which technology companies like Facebook and Google harvest and process user data. Companies in the modern data economy mine troves of data with sophisticated algorithms to produce valuable behavioural predictions. These data-driven predictions provide companies with a powerful capacity to influence and manipulate users, and these risks are increasing with the explosive growth of 'Big Data' and machine learning. This article analyses the extent to which these challenges are met by existing regimes such as Australia and New Zealand's respective privacy acts and the European Union's General Data Protection Regime. While these laws protect certain privacy interests, I argue that users have a broader set of interests in their data meriting protection. I explore three of these novel interests, including the social dimension of data, control and access to predictions mined from data and the economic value of data. This article shows how existing frameworks fail to recognise or protect these novel interests. In light of this failure, new legal regimes are urgently needed to protect against the worst excesses of the data economy.

Keywords: Privacy; artificial intelligence; data; General Data Protection Regulation; Facebook; Google.

Introduction

The fact that it is now a cliché to refer to our digital era as the 'Fourth Industrial Revolution' reinforces how important the internet and artificial intelligence (AI) have become. Algorithms increasingly influence the way we perceive ourselves, interact with others and understand the world around us. These are seismic impacts on the scale of the upheaval caused by the original Industrial Revolution. However, transformational change is usually a complicated mix of good and bad. For instance, while the Industrial Revolution may have created the foundations for the wealth and quality of life we enjoy today, it is also responsible for the explosion in carbon emissions that now drive catastrophic climate change. Similarly, while today's technology industry is well known for building brilliant applications and devices, it also displays a dangerous proclivity to accumulate and manipulate personal data. To ameliorate the worst effects of this data-driven revolution, we must think more broadly about our data interests and how to best protect them. Protecting these interests requires re-thinking the law on information privacy and questioning whether the existing regimes are sufficient.

Part I of this article discusses the nature and origins of the interests we have in data. It discusses the internal logic of the modern data economy, which is driven by large technology companies ('data harvesters') that accumulate and process personal data at scale. These companies mine troves of data using sophisticated algorithms to generate behavioural insights about individuals. These insights are traded to advertisers and other buyers in a colossal auction system powered by machine-learning AI that matches buyer's objectives with the appropriate behavioural insights. To explain the data economy another way, if you 'like' the Facebook page of the football club, Barcelona, it is likely you will soon see targeted advertisements for Barcelona merchandise. No human has decided to target you with those advertisements. Instead, a grand coalition of data-mining AI and insight-trading AI have deduced from your activity that you are reasonably likely to want a playing shirt with 'Lionel Messi' emblazoned on the back.

Although a data economy revolving around these kinds of transactions might sound relatively benign, there are mounting challenges raised by the way this system is evolving. The advent of 'Big Data' has caused the scale and capacity of data harvesting to grow exponentially. Almost every activity and action users take online are now catalogued as data points and fed into algorithms that grow increasingly adept at understanding those users' feelings, wants and needs. Consequently, algorithms can produce even more detailed and accurate predictions about those users' likely behaviour, which are worth more money to advertisers. This powerful feedback loop for data has caused an arms race among technology companies to collect as much data as possible. Data-driven behavioural insights are also being put to a greater variety of uses, including uses outside the commercial sphere. Technology companies have demonstrated a capacity and willingness to instrumentalise data for other means, such as manipulating voting in democratic elections. Unfortunately, the same algorithms responsible for your new Lionel Messi shirt have a growing capacity to influence you in a practically limitless range of ways, raising serious public policy issues.

Part II discusses how information privacy law has responded to the challenges born out of the data economy. My article is specifically concerned with information privacy and the regimes designed to protect it. For instance, when my article later addresses the idea in legal jurisprudence of privacy as property, this is done in the context of information privacy and the increasing economic value of personal information. Accordingly, Part II includes a brief overview of the fundamentals of information privacy. I address how existing regimes suffer from structural limitations that limit the extent to which they can protect against the encroaches of data harvesters. An analysis of two distinct example studies reinforces this idea: a flexible approach to privacy principles, such as that adopted in New Zealand and Australia; as well as the European Union (EU)'s General Data Protection Regulation (GDPR). These systems are different but share key characteristics such as an individualistic focus. Although the GDPR is undoubtedly a step in the right direction, my argument is that the structural design of information privacy regimes limits how they can adequately address the challenges raised by the data economy.

Part III discusses how the evolution of the data economy has created novel interests in data. I propose that users of technology platforms have a social interest in how their friends and family's data are mined for insights about them. These interests include a control interest, in which parties have access to the behavioural predictions made about them, and an economic interest, in which the data are viewed as a productive asset that can be monetised. An information privacy regime is a poor vehicle for defending any of these interests. Finally, Part IV analyses two proposals regarding whether they would safeguard the broader extent of these novel interests. These proposals include the information fiduciary concept proposed by Jack Balkin and the data union model advocated by Eric Posner and Glen Weyl. If we are to protect the real interests we have in our data, there is no option but to consider new legal options that go beyond privacy.

Part I: The Data Economy

To understand how the data economy operates, take the trailblazing leader of this new world, Google, as a case study. The defining characteristic of data harvesters such as Google is the large-scale accumulation of data to feed machine-learning algorithms, which produce insights and predictions of user behaviour.[1] Of particular note is how these processes have been crafted to avoid breaching user privacy but have allowed some concerning and problematic developments. To quote the quintessential Silicon Valley venture capitalist, Marc Andreesen, 'software is eating the world'.[2] The advent of Big Data and this new capacity for orchestrating behavioural change lend an urgency to the legal challenges canvassed in the rest of this article.

The data economy began with a young company named Google in the mid-2000s. While the company at first operated a simple web search system that used search data to improve the accuracy and quality of searches, Google engineers soon developed ways to use the other kinds of data that the company collected.[3] These were helpfully laid out in a patent Google's top engineers submitted in 2003, entitled 'Generating User Information for Use in Targeted Advertising', and described by Zuboff as 'emblematic of the new mutation and the emerging logic of accumulation that would define Google's success'.[4] In the patent, the engineers wrote about the vast amount of demographic data that went unused by advertisers. The patent went on to discuss the 'need to increase the relevancy of ads served for some user request, such as a search query', and how Google could use its 'novel methods and data structures for determining user profile information and using such determined user profile information

[1] Zuboff, Age of Surveillance Capitalism, 67.

[2] Zuboff, Age of Surveillance Capitalism, 68.

[3] Zuboff, Age of Surveillance Capitalism, 68.

[4] Generating User Information for Use in Targeted Advertising, US20050131762A1, filed December 31, 2003; Zuboff, Age of Surveillance Capitalism, 77.

for ad serving'.[5] As Zuboff stated, Google would no longer mine behavioural data to improve their core service for users but rather to try and read users' minds for the purpose of matching advertisements to their interests.[6]

Google is unrecognisable now compared to its size and stature in the mid-2000s, but its core business model has held true to the economic logic espoused in that 2003 patent. Google is thought of as an internet search company, but it might be more appropriate to think about it as an AI or data analytics company. Google harvests as much data as possible to enable its AI to make accurate predictions about what someone wants at any given time. These predictions are of considerable value to advertisers. The main change in the intervening 17 years is scale. Google's system for advertisement targeting—the process by which advertisers ensure their advertisements are seen by the right people at the right time—has evolved into a vast, fully automated auction system.[7] This system can accommodate millions of simultaneous advertisement buys, with algorithms representing advertising budgets bidding automatically on the predicted behaviour they deem the best fit.[8] The system is an automated futures market for human behaviour: advertisers are buying predictions of what a Google user will do at a particular time.[9] It is important to note that advertisers are not buying the personal data of that Google user (which would breach, for instance, the GDPR). They do not need that data—instead, they are much more interested in predicting what that user wants to buy, as derived from the behavioural insights produced by Google's analytics.

This economic logic about buying predictions in user behaviour holds true for technology companies other than Google. For instance, Facebook has a similar wealth of user data, mined by machine-learning AI to produce valuable behavioural predictions.[10] Although the advertisements may appear on a Facebook feed rather than a Google search result, the algorithmic logic is the same. Likewise, Amazon accumulates data so it can place products on users' homepages that they are likely to buy.[11] Similar examples of data mining and usage can be found in many other technology companies. Most people are familiar with the media companies Netflix and Spotify and their ability to suggest content that users are likely to enjoy. These models, too, derive from sophisticated analytics built from troves of user data.[12] These examples illustrate why data have become one of the most important economic goods on the planet and explain the arms race between technology companies to accumulate the most data possible in the shortest amount of time. This dynamic explains why it is illustrative to term these companies 'data harvesters'.

Importantly, even if users do not choose to give a particular data harvester any information about themselves whatsoever, it might still be the case that that platform's algorithms produce data-driven insights about them. This apparent oddity is a consequence of the networked nature of data. The data of your friends and family include information about you. For instance, if many of your close friends attend a particular concert or sporting event (and indicate this, for instance, on Facebook), Facebook can sell a futures contract on the likelihood that you, too, may attend that event.[13] While this might make you feel uncomfortable, it is unlikely to represent a breach of your privacy. Your friends have willingly provided data about themselves, and the algorithm can create a prediction for your behaviour based on their data. At no point is your actual behaviour known to the algorithm (and so your private information is not disclosed), but it can generate insights about you, nonetheless.

This networked feature of data has another, even more, discomforting dimension. Using data provided consensually by people close to any particular user, algorithms can generate insights about that user that they might not even be aware of themselves. The example given by Weyl is of someone who provides access to their health data for commercial or research reasons.[14] That data contains health information about the person's entire family, such as the likelihood that family members have certain hereditary diseases. Providing these data could then result, for instance, in different health insurance premiums for the rest of the family, whether or not the other family members are aware of the health risk in question. A comprehensive data network based on a user's friends and family can provide a more comprehensive picture about the than anything a user could provide themselves. The seriousness of this challenge to privacy is amplified by the new-found ability of AI to influence actual behaviour, far beyond the realm of advertising.

Data harvesters have long shown both the capacity and willingness to use their data stores to shape human behaviour, including without consent from the user or a warning to the user. For instance, in 2012, Facebook researchers published an article titled

[5] Generating User Information for Use in Targeted Advertising, US20050131762A1, filed December 31, 2003.
[6] Zuboff, Age of Surveillance Capitalism, 78.
[7] Nicas, "Google's Ad Auctions."
[8] Nicas, "Google's Ad Auctions."
[9] Zuboff, Age of Surveillance Capitalism, 96.
[10] Biddle, "Facebook Uses Artificial Intelligence."
[11] Hearn, "Amazon's New Ad Strategy."
[12] Pressman, "Spotify Nabs Top AI Expert."
[13] Biddle, "Facebook Uses Artificial Intelligence."
[14] Bacchi, "Personal? Private?"

'A 61-Million-Person Experiment in Social Influence and Political Mobilization' in the scientific journal *Nature*.[15] This article revealed that Facebook had conducted a controlled, randomised study during the 2010 Congressional elections in the United States. Essentially, they manipulated the content and positioning of voting-related information to see if it would change the behaviour of 61 million American Facebook users.[16] The study showed that displaying images of a user's Facebook friends made a statistically significant difference in the number of users who chose to vote. Facebook engineers calculated that their study led to approximately 340,000 additional votes in the congressional elections.[17] They wrote that 'showing familiar faces to users can dramatically improve the effectiveness of a mobilization message … the results suggest that online messages might influence a variety of offline behaviours'.[18] The careful phrasing of these comments should not distract from the chilling implications. As one newspaper asked, when the results came out, 'if Facebook can tweak emotions and make us vote, what else can it do?'[19]

Although the 2012 Facebook study focused on increasing net voting rates, an ostensibly (although not totally) politically neutral aim, there have been plenty of examples of more partisan attempts at the same kind of data-driven social engineering. Take the infamous example of Cambridge Analytica, a consultancy firm that pioneered the use of data-based social engineering. One of Cambridge Analytica's leaders was secretly recorded discussing the firm's activities in Trinidad's general election.[20] Hired by one of Trinidad's two major political parties, Cambridge Analytica accessed a vast amount of Facebook data about the other major party's supporters, mostly comprising Black Trinidadians.[21] The company composed an elaborate campaign through Facebook's platform to target those voters and influence them to feel apathetic about the election. This deeply troubling strategy worked, as gleefully recounted on the secret recording: 'the difference on the 18–35-year-old turnout was like 40%, and that swung the election by about 6%—which is all we needed!'[22] This goes far beyond the advertising focus that makes up most of the data economy and offers a warning of the kind of manipulative power offered by modern technology platforms. Cambridge Analytica was caught and ultimately defenestrated, but not before they had field-tested the hypotheses about data-driven manipulation that Facebook forwarded in 2012. It should be no surprise that there are reports of other companies offering similar services.[23]

Part II: The Limitations of Information Privacy

Considering the context around the modern data economy, the second section of this article discusses the limitations of existing approaches to information privacy. The first of these is the flexible approach to information privacy adopted in New Zealand and Australia. I also discuss the EU's GDPR, a comprehensive framework for data protection with many more moving parts. Despite their differences, these privacy regimes largely embody the historical design of information privacy frameworks, particularly those recommended by the Organisation for Economic Cooperation and Development (OECD) in 1980.

For a brief context, this section begins with an overview of information privacy and the important distinctions from other types of privacy. A longstanding theoretical concept, the Universal Declaration of Human Rights in 1948 recognised privacy in Article 12, which provided that 'no one shall be subjected to arbitrary interference with his privacy … everyone has the right to the protection of the law against such interference'. Privacy can encompass different categories. These include physical privacy or bodily privacy, which concerns protecting someone's body from invasive procedures. Another example is territorial privacy, limiting intrusion into domestic and other environments such as the workplace. This article is concerned with the specific category of information privacy, defined by the Electronic Privacy Information Center as 'the establishment of rules governing the collection and handling of personal data'.

It is also vital to note the differences between the information privacy approach adopted in New Zealand and Australia, and the GDPR adopted by the EU. New Zealand's and Australia's privacy regimes require organisations that hold personal information about individuals to behave according to a range of principles concerning how that information is collected, stored, accessed and disclosed. It is high level, without detailed or prescriptive rules, and it does not provide any legal recourse to affected individuals. Instead, it encourages individuals to lay complaints with the relevant privacy commissioner to investigate. By contrast, while the GDPR also contains a set of principles and rights, the substance of the regulation is much more comprehensive and comprises a prescriptive set of rules about how entities holding personal information can collect, use and

[15] Bond, "61-Million-Person Experiment."
[16] Bond, "61-Million-Person Experiment."
[17] Bond, "61-Million-Person Experiment," 296.
[18] Bond, "61-Million-Person Experiment," 296.
[19] Arthur, "If Facebook Can Tweak Emotions and Make Us Vote, What Else Can It Do?".
[20] Hilder, "Stealing the Election."
[21] Hilder, "Stealing the Election."
[22] Hilder, "Stealing the Election."
[23] Waterson, "Tories Hire Facebook Propaganda Pair."

process personal information. Despite the advances of the GDPR, both approaches share a limited capacity to regulate data harvesting by technology companies.

New Zealand's and Australia's Privacy Acts and the EU's GDPR

Basic principles of information privacy developed in an age where technology and data simply did not exist in the way they do now. New Zealand's and Australia's privacy regimes are good examples of privacy frameworks that have undergone plentiful changes and revisions but are still fundamentally built around these dated principles of information privacy. New Zealand recently passed the Privacy Act 2020 to replace the Privacy Act 1993, but it did not substantially change the framework of privacy protection. The main changes in the new law related mostly to the scaling up of enforcement processes. Australia's Privacy Act 1988 has a similar basic framework to New Zealand's, again despite some revisions over time. Penk and Tobin noted that both privacy acts were created in response to concerns around limited access to personal information such as employment records and medical information. This approach was not unusual or unorthodox in those days and was based on the OECD's recommendations in 1980.

This approach to privacy is problematic, as the challenges raised by the data economy did not exist when these legacy privacy regimes were designed. As stated, New Zealand's and Australia's privacy regimes revolve around a set of flexible principles that set out rules for how personal information should be collected and stored. There are few prescriptive rules or requirements. There are distinct operational and theoretical distinctions between these regimes and the EU's GDPR. For instance, Article 22 of the GDPR restricts the use of automated decision-making tools where the decisions may have a legal effect, and it allows for the affected person to seek human intervention or contest the decision. New Zealand's and Australia's frameworks are silent on this point.

New Zealand's and Australia's regimes have clear principles on giving individuals the right to access personal information that a third party is storing, check its accuracy and correct it. These principles make sense in the context that each privacy act was designed for, such as the medical file a hospital keeps about you. It is important that you can access that file and check the information is correct and correct it if not. However, these principles are challenging to apply to the modern day's complicated mechanics of data harvesting and algorithmic analysis. The foundation of information privacy that New Zealand's and Australia's privacy regimes was built on was not created with that context in mind.

There are also structural weaknesses built into these legacy privacy regimes. For instance, both New Zealand's and Australia's privacy acts explicitly state that none of the privacy principles is enforceable in a court unless against a public sector agency. Breaches of the privacy act are instead governed by regulatory bodies: The Office of the Australian Information Commissioner in Australia and the Office of the Privacy Commissioner in New Zealand. These are relatively small and poorly resourced agencies. The real weakness of these systems as a means of enforcing data rights was cemented in 2018 when New Zealand's privacy commissioner issued a statutory demand to Facebook to give up certain documents so that the office could commence an investigation into an alleged privacy breach. Facebook categorically refused, and that essentially ended the matter—to quote the privacy commissioner, 'under current law there is little more I am able to do to practically protect my, or New Zealanders' data on Facebook'.

It is not just New Zealand's and Australia's privacy laws that are founded on dated foundations. Take the EU's GDPR—while the GDPR is often considered the quintessentially 'modern' privacy regime, it retains many of the fundamental dynamics of the 1995 Data Protection Directive, designed for a very different technological landscape. Shimanek noted that the 1995 Data Protection Directive itself was designed with reference to the OECD's 1980 recommendations—the same recommendations used by New Zealand and Australia in their privacy models. The roots of this 1980's design are apparent in the GDPR, despite its evolution.

An example of legacy design is the way in which the GDPR has few restrictions on the second and third-order products of personal data, in favour of a comprehensive framework for the personal data itself. For instance, the GDPR has strong punishments for data breaches where that information is sold or leaked, and it provides a framework for safely porting such information between platforms. However, as discussed in Part I, the data economy revolves not just around personal information but also the use of algorithms to mine that information for behavioural insights. As Rubinstein noted, the GDPR is mostly silent on these algorithmic products, meaning that data mining may 'largely escape regulatory oversight, even though it permits inferences of previously private information … that may cause as much or more harm as the regulated collection and use of personal data'.

The GDPR does provide for some regulations around how data can be processed. Article nine of the GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, genetic or biometric data and information about someone's sex life or sexual orientation. The GDPR demarcates these fundamental aspects of someone's life as 'special categories' of data, meriting a greater degree of protection. However, this protection is far from ironclad: in Article 9(2), a number of exceptions are spelled out, including 'where processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim'.

In any case, as Zarsky pointed out, the real value of the GDPR's protection of sensitive data such as through Article nine may be more symbolic than practical. The algorithmic and all-encompassing nature of information processing in the data economy blurs the lines between special categories of data and any other data. Zarsky gave the example of how health data can be deduced from an endless array of data sets, such as shopping databases, which expands the scope of Article nine so far as to render it meaningless. This is a further example of how the GDPR was not designed in a way that adequately deals with the challenges of the algorithmic data economy.

A key structural limitation of the GDPR is how it locates data interests as exclusively individualistic. This approach flows from an historical emphasis of privacy law on an individual's right to privacy and personal information. As an extensive legal literature has covered, this individualistic approach to privacy is suboptimal: as Cohen stated, 'privacy rights protect individuals, but to understand privacy simply as an individual right is a mistake'. An individualistic framework, inherited from the 1995 Data Protection Directive, is a particularly poor fit for the networked reality of the data economy. Even if you refuse to give consent to any particular technology platform to access your data, it is extremely likely that the platform will still be able to generate accurate predictions about your behaviour. There is an enormous amount of data that pertain to you directly or indirectly, and only a small subset of that data is classified as 'personal information' under the GDPR. Although an advantage of a rights-based framework is to construe this subset more broadly than any prescriptive detail, this approach only goes so far. The GDPR protects some of your interests in your personal information but not your interests in anybody else's. This approach reflects an overly narrow view of what your interests in data are. The balance of this article will consider these interests in more detail and how they might be best protected.

Part III: Novel Interests in Data

In this section, I sketch out what three of these new interests are, how the data economy has given rise to them and why privacy laws fail to protect them. First, I explore the social interest we have in our data and the data of those close to us. The way data are aggregated and networked means that an individualistic approach to protecting data is no longer adequate, and that a communal social interest in data must be recognised. Second, I discuss the idea of a control interest. This term refers to the fundamental interest we all share in having some degree of control over who or what groups can access behavioural insights about us mined from our data. The data economy revolves around the sale of data-driven predictions, not the sale of data itself, and this gives way to a broader control interest in how data are processed and commodified. Lastly, I will discuss an economic interest flowing out of the new reality of personal data as a valuable commodity.

These three interests certainly do not present an exhaustive list of people's interests in their data. This is particularly true given the rapid pace at which technology is developing and the evolving relationship that people have with their data and the technology companies who seek it. However, for the purposes of this analysis, these interests are some of the most important interests that flow from the way in which the data economy has evolved. The global focus on regulating technology companies through information privacy has left these novel interests unprotected, ill-suited as they are to a privacy framework.

Social Interest

The first novel interest this article considers is social. Privacy regimes, and the way privacy is typically considered, is individualistic in nature.[24] However, thinking about data rights solely from the individual's perspective, as through the lens of privacy, fundamentally misunderstands how data is now used in the data economy. As discussed briefly in Part I, data that 'belongs' to a particular user usually contains a huge amount of information about others. Examples include social media updates, photos, messaging and email conversations, calendar bookings, meeting records and every single like and comment the user makes online.[25] The analytics that power the data economy are extremely good at combing through this mountain of content and distilling it into an analysis about any of the people involved. Zuboff terms this content heap as 'behavioural surplus', which data harvesters have been able to use to 'ignite new markets in future behaviour'.[26] Importantly, any one

[24] Cohen, "What Privacy Is For," 19.
[25] Zuboff, Age of Surveillance Capitalism, 186.
[26] Zuboff, Age of Surveillance Capitalism, 337.

person's behavioural surplus contains data relating to a multitude of other people. This critical fact gives rise to a powerful social interest in data.

As Martin Tisné has written, even in situations where you have explicitly denied consent to 'your' data being used, an organisation can use data provided by other people to draw extrapolated predictions about you.[27] In this way, your consent is rid of any power, becoming increasingly irrelevant to the processes of the data economy. You are bound by other people's consent. Tisné writes about how this era of 'machine learning driven group profiling' strips us of any ability to opt out of these processes.[28] Thinking of your data as exclusively personal property—something you can control access to—misunderstands the structural and networked way the data economy works. Given the network effects and data analytics of gigantic platforms like Facebook or Google, it is practically inevitable that these platforms can make accurate predictions about most individuals, whether or not they have provided the platform with their data.

This issue is compounded by the well-known issues with consent when it comes to engaging with large technology platforms like Facebook, Google or Twitter. While those companies' lawyers might say users give consent when they agree to a platform's terms and conditions, the reality is that those documents are constructed to be complex, extensive and the language inaccessible to the average reader.[29] In one empirical study, 543 participants who were told to join a new online service spent, on average, 14 seconds looking at the terms and conditions.[30] The researchers calculated that the document required at least 45 minutes of reading for adequate comprehension.[31] Another study indicated that the 'vast majority of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data'.[32] The process of 'consenting' to data access has been distorted in two ways that are fundamentally social: first, consenting to the access of your data almost always provides data about your friends, families and colleagues (whether or not you are aware of this), and second, the very process by which you consent is unlikely to be reasonable or considered.[33]

This is a critical point because it exposes why a focus on information privacy is a poor defence to the challenges and excesses of the modern data economy. Part II demonstrated how privacy law is conducted within the sphere of the individual, protecting their particular rights to their 'own' data. Fundamentally, this is incongruent with the networked way in which the data economy accumulates and processes data. Because the ability of any data harvester to make accurate predictions about a particular user relies as heavily on information provided by the people around them as much as the information they provide themselves, this social interest in how data are conceived and protected is vital. As the data economy revolves around the way data is networked and aggregated, an effective legal framework must recognise and cater to data networking.

Control Interest

People have a control interest in their data, which is the second novel interest this article analyses. It is legitimate and reasonable for people to want to withhold their data from particular actors, even if the data are anonymised, aggregated and not necessarily in breach of any privacy laws. While users might consent to a particular data harvester (say, Facebook or Google) having access to their data, there is seldom any consent or awareness of what happens to their data after that point of consent. When machine-learning algorithms produce predictions based in part on your data, and those predictions are sold to a huge number of different parties with different ends, it would be strange to conclude that your interest in your data only extends to the technology platform you interacted with in the first instance. The notion of a control interest captures the extent of this interest.

One way of demonstrating the necessity of this control interest is to consider the thin veneer of consent that occurs when a new user signs up to a service like Facebook or Google. Even assuming that every user properly and diligently consents to their data being accessed by the data harvester (unlikely given that the average user spends 14 seconds reading terms and conditions), nobody would conclude that the user ceases to have an interest in their data from that point onwards.[34] Although frameworks such as the GDPR are intended to have a principled application to ensure users have some element of control over their personal data, this control does not extend to the algorithmic products of that data. For an analogy, when I sign an employment contract that discusses the terms of a new job, neither common sense nor employment law dictates that I cease to have any interest in what happens to the work I produce in that job. Similarly, our control interest in data should be understood as multi-layered,

[27] Tisné, "Data isn't the new oil."
[28] Tisné, "Data isn't the new oil."
[29] Turow, Tradeoff Fallacy.
[30] Obar, "Biggest Lie on the Internet."
[31] Obar, "Biggest Lie on the Internet."
[32] Turow, Tradeoff Fallacy, 4.
[33] Solove, "Privacy Self-Management," 1880.
[34] Obar, "Biggest Lie on the Internet."

going beyond the primary or precursory agreement. This is particularly true when there is mounting evidence that the products of data are used in a manner that is demonstrably against our interests.

Recall the example discussed in Part I about how Cambridge Analytica manipulated an election in Trinidad by analysing Black Trinidadians' profiles. Of course, few of those citizens would have had any awareness that their Facebook data was being used to feed a political campaign to keep them from the polling booths. Research suggests that most Facebook users have a sense that Facebook uses their data only for 'advertising', a helplessly generic understanding that Facebook cultivates as far as it possibly can.[35] When pushed on the adverse effects of their model of selling data-driven predictions, Facebook Chief Operating Officer Sheryl Sandberg's favourite example to draw upon is of a 'dog-walking business looking for customers'.[36] Sandberg argues that there are no disadvantaged parties if the dog-walking business can use Facebook to find clients needing those services. Of course, many more groups are interested in what is gleaned from your data than a humble dog-walking business, and you might not want some of those groups to have access to those insights. A control interest in your data flows from these dynamics about how the data economy operates.

Economic Interest

The last of these novel interests is economic. Before setting out my analysis regarding this economic point, it is important to triangulate my argument regarding the divisive legal literature around whether privacy rights can be considered a form of property and whether doing so would better strengthen privacy norms in society.[37] In this article, my aim has been to demonstrate how data are currently being monetised by data harvesters and how regimes such as the GDPR and flexible privacy principles do little to prevent these processes. I believe that this monetisation has given users an economic interest in their data, whether or not that interest could correctly be described as akin to 'property'.

It is correct to think of the data held by technology companies as a productive asset in reference to its ability to generate returns indefinitely into the future. Put simply, data have become a gold mine in today's data economy, and data harvesters have consequently become the most valuable companies in the world.[38] And yet, those productive assets are accumulated essentially for free. For example, Facebook pays approximately one per cent of its value each year to workers, compared with other large businesses like Walmart, which pays 40 per cent.[39] The difference is that Facebook obtains an enormous amount of value from users and their data, without any commensurate compensation for those users. The Australian Competition & Consumer Commission's Digital Platforms Inquiry in 2019 considered this point in depth.[40] The dynamics of the relationship between platforms and users are distorted by the way in which technology companies can take advantage of the fact that people do not understand the value of their data.

That existing legal frameworks do little to recognise this economic interest in data is problematic, not least because technology platforms have cultivated the norm that users should give their data away as freely as possible. While data harvesters use these informational asymmetries to monetise personal data, it is well established that users have little concept of what their data are actually worth. Solove notes that privacy "self-management", i.e., users making their own decisions about how to weigh the costs and benefits of consenting to the collection of their data, is subject to severe cognitive problems that impair individuals' ability to make informed, rational choiceschoices.[41] In this way, users' economic interest in their data is under attack, and information privacy provides no shield at all. It is unarguable that many in society have voted with their feet, willing to trade access to their personal information in exchange for a free online network such as Facebook or a free service such as Google Search. However, the literature suggests that the vast majority of users are unaware of the economic worth of their data, let alone that those access rights represent an income source in perpetuity for the technology company.[42] Facebook and Google are at pains to avoid the idea that a user signing up to their terms is taking part in an economic interaction, and this language is very much absent from those terms. However, personal data must be acknowledged as having economic value. This article is not so concerned with the debate around property or how that value is calculated, so much as highlighting that this economic interest exists and that current frameworks do not recognise or protect this interest.

[35] Turow, Tradeoff Fallacy.
[36] Byers, "Transcript: Facebook's Sheryl Sandberg."
[37] Lessig, "Privacy as Property," 247.
[38] Zuboff, Age of Surveillance Capitalism, 19.
[39] Arrieta Ibarra, "Should We Treat Data as Labor?"
[40] Australian Competition & Consumer Commission, "Digital Platforms Inquiry," 380.
[41] Solove, "Privacy Self-Management," 1880.
[42] Turow, Tradeoff Fallacy.

Part IV: Supplementary Frameworks for Data Protection

So far, this article has set out the context and challenge of the data economy and how data harvesting exposes the limitations of information privacy and the existence of novel interests in data. In this final section, I apply this frame of analysis to two proposals in the legal literature that have offered alternative regimes. The first of these is Balkin's proposal for a system of information fiduciaries. Second is the proposal of data unions championed by Posner and Weyl. Both proposals offer ways to protect users and their novel interests in data and compare favourably to existing regimes.

Information Fiduciaries

In 2016, Balkin set out a proposal for 'information fiduciaries'. In this framework, technology companies with a large amount of data would be designated as 'information fiduciaries', binding them to a strict legal standard and code of conduct modelled after existing law and finance models. Broadly speaking, technology companies bound by a fiduciary responsibility would not be able to act against their users' interests. Much like the principle that governs lawyers and financial advisers, the principle underpinning information fiduciaries would recognise that data harvesters benefit from a significant imbalance of power and that this privilege has an associated level of responsibility. Although the specifics of fiduciary responsibility differ in various jurisdictions around the world, this fundamental principle of identifying and rectifying power asymmetries is consistent globally.

Although Balkin situates his argument in the American context, the principles of his approach can be transposed to other jurisdictions on a principled basis. It is well established that data harvesters, on account of their scale, technological complexity and network effects, benefit from a position of privilege when engaging with users. Previous examples given in this article have shown that anyone who is not a lawyer would struggle to read or understand even the basic terms of service offered by platforms such as Facebook or Amazon. In addition, much like a patient could not be expected to have the knowledge or skill to analyse a doctor's medical advice and challenge it, users of technology services cannot be expected to understand the complicated algorithms that are consuming their data, nor what the consequences might entail. There is a huge information asymmetry incumbent in the data economy that makes genuine consent extremely difficult to determine. In these circumstances, a fiduciary approach seems an appropriate fit.

There is also cause for optimism that a system of information fiduciaries and associated responsibilities would help defend the novel interests in data outlined in this article. Holding a technology platform to a fiduciary standard would drastically change the economic relationship between the user and their platform. Much like doctors cannot auction information derived from their patient's data, data harvesters would lose their free rein to profit from mining user data without a clear consensus reached with users. The fiduciary standard would go far beyond the requirements of the GDPR and place the onus squarely on the technology platforms rather than their users. This standard would appropriately reflect the imbalance of power and informational asymmetry between the technology platforms and their users. Although limitations on how data are processed might temper the business model of data harvesters, positive-sum actions would not be affected in the slightest. Google could continue to improve the accuracy of Google Search, the companies' most important product, as doing so is clearly aligned with the best interests of its users.

The information fiduciary approach could have an even greater effect on protecting users' control interests. Because data harvesters would be bound to act in their users' best interests, theoretically, they would be unable to provide unsavoury actors with the tools they need to manipulate those users. Just as a person's financial adviser legally cannot provide insider information to a third party who wants to manipulate that person, selling data to a third party that wants to manipulate voters would breach a fiduciary standard of behaviour. The data harvesters would need to be more discerning about whom they sell data-driven insights to, and the users would have definitive legal recourse if the data harvesters failed to meet the standard. Admittedly, because of the latent information asymmetry, the vast majority of users would not know whether a technology platform was acting in their best interests or not. This is a weakness in Balkin's regime, but the hope is that regulatory agencies would be suitably resourced to enforce this fiduciary standard on behalf of users (as is the case with financial advisers and lawyers). Khan and Pozen raise other issues with the regime, such as the potentially irreconcilable tensions between shareholders and users following the imposition of a fiduciary duty.

The final aspect of the information fiduciary approach that appeals is how it aligns with the technology platforms' values and their public messaging, particularly the idea that they should be trusted with your data. An information fiduciary approach might be supported by the technology companies, even though it would restrict their activities and rebalance power towards users in some important ways. For instance, some technology companies have already displayed some tentative interest in this kind of reform. When asked in a congressional hearing specifically about the idea of information fiduciaries, Facebook Chief Executive Officer Mark Zuckerberg said it was 'certainly an interesting idea … Jack is very thoughtful in this space so I do think it deserves consideration'. Indeed, as a path forward for reforming how the data economy operates and how our data interests are best protected, Balkin's proposal for information fiduciaries certainly deserves consideration.

Data Unions

The second proposal for a framework to better protect our interests in data uses the concept of 'data unions' and is advocated by Posner and Weyl. The proposed data unions would function similarly to trade unions. Specific organisations—data unions—would be formed to manage and represent many people's personal data. Technology platforms would then agree on terms with the data unions rather than enter into an agreement with the individuals those unions represent. Data unions would be legally required to act in the best interests of the people they represent, perhaps to a fiduciary standard, as described in Balkin's proposal. Posner and Weyl's proposal would empower a 'middle layer' of unions able to organise creatively and commit strongly to defending the interests we have in data and then negotiate more forcefully with the data harvesters.

The advantage of Posner and Weyl's system is the considerably greater bargaining power held by a collective of users, as opposed to individuals, ameliorating the weaknesses of the information fiduciary proposal described above. In the status quo, any user has vanishingly little capacity to 'negotiate' terms with technology platforms, let alone economically sensitive terms such as those around data usage. Data harvesters like Facebook and Google can safely adopt a 'take it or leave it' approach to users raising concerns, secure in the knowledge that the majority of users will simply click through terms without a second thought. The considerable power imbalance would be somewhat levelled if users banded together in large groups or unions. Although a technology platform can afford to 'lose' any user who dissents to their terms, no business can be blasé about losing a collective of a million users. Enabling unions to negotiate terms with the powerful technology companies would allow for greater defence of users' broad interests, such as those outlined in Part III. Data unions could negotiate on economic terms, ask for greater protections in line with users' control interest and help protect the users' social interest.

Data unions also have the capacity to offer a coherent alternative vision for users around data. Research has suggested that users are broadly dissatisfied in their relationship with social media platforms and other technology companies, but most users (understandably) do not have a clear idea about an alternative. Data unions could frame reasonable terms of use for data that are separate to, and contrast with what is forwarded by technology platforms. It is not in the best interest of a technology company to spell out the nature of data as an economic resource and set terms of use on that basis; however, a data union could do just that. The advent of data unions could see the democratisation of data rights, with different unions offering different visions to attract members. One data union might promise to treat political nudging or manipulation as a red line in negotiations, whereas another might be equivocal on that point but demand that users are paid. The most popular visions would attract the most users and become the most powerful and influential data unions.

Of course, the idea of data unions comes with its own challenges and a number of open-ended questions. Most of all, it is not clear whether technology users would want to delegate any control or bargaining power to a data union. For a data union to bargain effectively with technology platforms, it would need to have the delegated authority to take serious measures, such as withdraw its members from a particular platform. An analogy is the importance of the strike to trade unions in employment negotiations. The ability to credibly guarantee adverse action by its members is what gives trade unions their power. Data unions would need similar authority to have power, but it might prove difficult to convince social media users that the inconvenience (of union action) would be worthwhile. However, even if 10 to 15 per cent of a platform's users unionised, it would substantially increase the pressure on data harvesters to change their terms. Data unions would create space for general discussion around data and its protection, which would be a helpful step forward from the present day's blanket acceptance of terms proposed by technology companies. Data unions could potentially collaborate and advocate for new kinds of comprehensive data protection laws.

Conclusion

This article is intentionally titled '*beyond privacy*', not '*replacing privacy*'. Information privacy and existing data protection regimes have played an important role in protecting data and holding data harvesters to account. Indeed, both Google and Facebook have been sued for breaching the GDPR and, to some extent, have changed their systems.[43] However, this article elaborated the case for thinking beyond privacy when it comes to protecting data and regulating data harvesters' activities. As argued in Part I, the data economy has evolved such that existing frameworks for protecting users' data interests are poorly suited to meet the varied challenges offered by the data economy and its data-driven insights. Part III explored some of the novel interests that we have in our data, which flow from how the data economy operates. Part IV analysed two alternative

[43] Brandom, "Facebook and Google Hit."

frameworks for protecting users, set against the backdrop of those interests, and my hope is that this article can stir further discussion about how best to tackle these challenges.

Criticism of this article's analysis is likely to concentrate on the risks posed by a new framework and argue that the current legal paradigm strikes a good balance between users and technology platforms. Some theorists have already argued that privacy regulations unreasonably impede technological development and have a chilling effect on further innovation.[44] To some, what happens to a user's data after the user signs a set of terms and conditions does not matter—consent is key, and if technology companies have found a novel way of processing the data in a way that provides value, the outcome can only be positive. For a pre-emptive rebuttal, I will suffice to simply note that our legal system derives no small part of its legitimacy from providing a framework that protects fundamental interests. Part III set out three interests in data that are unprotected by existing frameworks. As data harvesting accelerates and the sophistication of data analytics develops, these interests will increasingly be observed in the breach.

The law has never been particularly responsive to areas of fast-changing technological development, and it is unlikely that this new era of data and AI will provide an exception to the rule. However, keeping an open mind is critical. Silicon Valley is not the only place that can display creativity and innovation, and my hope is that lawmakers will do so when they consider their response to this new age. Rather than shoehorn policy responses to the technology sector using regimes that are not fit for purpose, we ought to think instead about a new system with appropriate principles. New frameworks are required to ensure that the nascent data economy grows in tandem with our values instead of consuming them.

Bibliography

Andreessen, Marc. "Why Software Is Eating the World." *A16z* (blog). August 20, 2011. https://a16z.com/2011/08/20/why-software-is-eating-the-world/

Arrieta Ibarra, Imanol, Leonard Goff, Diego Jiménez Hernández, Jaron Lanier and E. Glen Weyl. "Should We Treat Data as Labor? Let's Open Up the Discussion." *Brookings* (blog). February 21, 2018. https://www.brookings.edu/blog/techtank/2018/02/21/should-we-treat-data-as-labor-lets-open-up-the-discussion/

Arrieta Ibarra, Imanol, Leonard Goff, Diego Jiménez Hernández, Jaron Lanier and E. Glen Weyl. "Should We Treat Data as Labor? Moving Beyond 'Free'." *American Economic Association Papers and Proceedings* 108 (2018): 38–42.

Arthur, Charles. "If Facebook Can Tweak Our Emotions and Make Us Vote, What Else Can It Do?" *Guardian,* June 30, 2014. https://www.theguardian.com/technology/2014/jun/30/if-facebook-can-tweak-our-emotions-and-make-us-vote-what-else-can-it-do

Australian Competition & Consumer Commission. *Digital Platforms Inquiry – Final Report*. (Australian Competition & Consumer Commission, July 26, 2019). https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

Bacchi, Umberto and Zoe Tabary. "Personal? Private? No Such Thing in Data-Hungry World." *Reuters,* November 15, 2019. https://www.reuters.com/article/us-tech-conference-data-trfn/personal-private-no-such-thing-in-data-hungry-world-idUSKBN1XO2HQ

Balkin, Jack. "Information Fiduciaries and the First Amendment." *UC Davis Law Review* 49, no 4 (2016): 1183–1234.

Biddle, Sam. "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document." *Intercept,* April 13, 2018. https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/

Bond, Robert, Christopher Fariss, Jason Jones, Adam Kramer, Cameron Marlow, Jaime Settle and James Fowler. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489 no 9 (2012): 295–298. https://doi.org/10.1038/nature11421

Bostrom, Nick. *Superintelligence.* Oxford: Oxford University Press, 2014.

Brandom, Russell. "Facebook and Google Hit with $8.8 Billion in Lawsuits on Day One of GDPR." *Verge,* May 25, 2018. https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe

Brandom, Russell. "This Plan Would Regulate Facebook without Going through Congress." *Verge,* April 12, 2018. https://www.theverge.com/2018/4/12/17229258/facebook-regulation-fiduciary-rule-data-proposal-balkin

Byers, Dylan. "Transcript: Facebook's Sheryl Sandberg." *NBC News,* February 29, 2020. https://www.nbcnews.com/podcast/byers-market/transcript-facebook-s-sheryl-sandberg-n1145051

Cohen, Julie E. "What Privacy Is For." *Harvard Law Review* 126, no 7 (2013): 1904–1933.

[44] Li, "The Impact of the GDPR."

Clarke, Roger. “Beyond the OECD Guidelines: Privacy Protection for the 21st Century.” Xamax Consultancy. Last modified January 4, 2000. http://www.rogerclarke.com/DV/PP21C.html

Dahlqvist, Fredrik, Mark Patel, Alexander Rajko and Jonathan Shulman. “Growing Opportunities in the Internet of Things.” *McKinsey & Company* (blog). July 22, 2019. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

Edwards, John. “NZ Privacy Commissioner: Why I Deleted Facebook.” *Spinoff*, March 28, 2018. https://thespinoff.co.nz/media/28-03-2018/nz-privacy-commissioner-why-i-deleted-facebook/

Electronic Privacy Information Center. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. Washington, DC, 2001.

Esteve, Asuncíon. “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA.” *International Data Privacy Law* 7, no 1 (2017): 36–47. https://doi.org/10.1093/idpl/ipw026

Greenleaf, Graham. “Elements of Zuboff’s Surveillance Capitalism.” *Privacy Laws and Business International Report* 160 (2019): 29–32.

Hearn, Iris. “Amazon’s New Ad Strategy Uses AI to Send Product Samples Based on Consumer Data.” *Impact* (blog). January 12, 2019. https://www.impactbnd.com/blog/amazons-new-ad-strategy-uses-ai-to-send-product-samples-based-on-consumer-data

Hilder, Paul. “ ‘They Were Planning on Stealing the Election’: Explosive New Tapes Reveal Cambridge Analytica CEO’s Boasts of Voter Suppression, Manipulation and Bribery.” openDemocracy. January 28, 2019. https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/

Khan, Lina and David Pozen, “A Skeptical View of Information Fiduciaries.” *Harvard Law Review* 133, no 2 (2019): 497–541.

Lessig, Lawrence. “Privacy as Property.” *Privacy in Post-Communist Europe* 69, no 1 (2002): 247–269. https://doi.org/10.1016/S0967-067X(96)00025-6

Li, He, Lu Yu and Wu He. “The Impact of GDPR on Global Technology Development.” *Journal of Global Information Technology Management* 22, no 1 (2019): 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Löffler, Max. “Who Will Benefit Most From the Data Economy?” *Economist*, February 20, 2020. https://www.economist.com/special-report/2020/02/20/who-will-benefit-most-from-the-data-economy.

Lombana-Bermudez, Andres, Sandra Cortesi, Christian Fieseler, Urs Gasser, Alexa Hasse, Gemma Newlands and Sarah Wu. “Youth and the Digital Economy: Exploring Youth Practices, Motivations, Skills, Pathways, and Value Creation.” Youth and Media, Berkman Klein Center for Internet & Society (2020). https://cyber.harvard.edu/publication/2020/youth-and-digital-economy

Longworth, E and T. McBride. *The Privacy Act: A Guide.* Wellington: GP Publications, 1994.

Martinez, Leah H. “Post Industrial Revolution Human Activity and Climate Change: Why the United States Must Implement Mandatory Limits on Industrial Greenhouse Gas Emissions.” *Journal of Land Use & Environmental Law* 20, no 2 (2005): 403–421.

Nicas, Jack. “How Google’s Ad Auctions Work.” *Wall Street Journal*, January 19, 2017. https://www.wsj.com/articles/how-googles-ad-auctions-work-1484827203

Obar, Jonathan A. and Anne Oeldorf-Hirsch. “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services.” *Facebook/Social Media* 2, (2018): 1–20. https://doi.org/10.1080/1369118X.2018.1486870

O’Neil, Cathy. *Weapons of Math Destruction.* United States: Penguin Books, 2016.

Office of the Privacy Commissioner. “Privacy Commissioner: Facebook Must Comply with New Zealand Privacy Act.” Office of the Privacy Commissioner. Media release, March 28, 2018. https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/

Penk, Steven and Rosemary Tobin. *Privacy Law in New Zealand.* Wellington: Thomson Reuters, 2016.

Posner, Eric A. and E. Glen Weyl. *Radical Markets.* Princeton: Princeton University Press, 2018.

Pressman, Aaron. “Spotify Nabs Top AI Expert From Netflix.” *Fortune*, September 7, 2019. https://fortune.com/2019/09/06/spotify-netflix-tony-jebara/

Purtova, Nadezhda. “Do Property Rights in Personal Data Make Sense after the Big Data Turn?” *Journal of Law and Economic Regulation* 10, no 2 (2017): 64–78.

RadicalxChange. “*The Data Freedom Act.* (RadicalxChange Foundation, Draft Proposal, 2019). https://www.radicalxchange.org/files/DFA.pdf

Regan, Priscilla M. “Privacy as a Common Good in the Digital World.” *Information, Communication & Society* 5, no 3 (2002): 382–405. https://doi.org/10.1080/13691180210159328

Rossi, Anna. “Respected or Challenged by Technology? The General Data Protection Regulation and Commercial Profiling on the Internet.” July 13, 2016. https://ssrn.com/abstract=2852739

Rubinstein, Ira S. “Big Data: The End of Privacy or a New Beginning?” *International Data Privacy Law* 3, no 2 (2013): 74–87.

Schulze, Elizabeth. “Everything You Need to Know about the Fourth Industrial Revolution.” *CNBC*, January 17, 2019. https://www.cnbc.com/2019/01/16/fourth-industrial-revolution-explained-davos-2019.html

Shimanek, Anna E. “Do You Want Milk with Those Cookies?: Complying with Safe Harbor Privacy Principles.” *Journal of Corporation Law* 26, no 2 (2001): 455–463.

Solove, Daniel J. “Privacy Self-Management and the Consent Dilemma.” *Harvard Law Rev*iew 126, no 7 (2013): 1880–1903.

Tisné, Martin. “Data Isn’t the New Oil, It’s the New CO2.” *Luminate* (blog). July 24, 2019. https://luminategroup.com/posts/blog/data-isnt-the-new-oil-its-the-new-co2

Turow, Joseph, Michael Hennessey, Nora Draper. *The Tradeoff Fallacy.* (Annenberg School for Communication, University of Pennsylvania. 2015). https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Waterson, Jim. “Tories Hire Facebook Propaganda Pair to Run Online Election Campaign.” *Guardian*, October 23, 2019. https://www.theguardian.com/politics/2019/oct/23/tories-hire-facebook-propaganda-pair-to-run-online-election-campaign.

Webb, Amy. *The Big Nine.* New York: Public Affairs, 2019.

Zarsky, Tal. “Incompatible: The GDPR in the Age of Big Data.” *Seton Hall Law Review* 47, no 4 (2017): 995–1020.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. London: Profile Books, 2019.

Primary Materials

Australia

Privacy Act 1988 (Cth).

European Union

Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Data Protection Directive 95/46/EC of the European Parliament and of the Council. October 24, 1995.

Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council. April 27, 2016.

New Zealand

Privacy Act 2020.

United Nations

Universal Declaration of Human Rights. UN General Assembly, 217 A (III). December 10, 1948.

United States

Generating User Information for Use in Targeted Advertising. US Patent No US20050131762A1, filed on December 31, 2003 (Issued June 16, 2005).

Agamben, Giorgio. *Homo Sacer: Sovereign Power and Bare Life*. Stanford: Stanford University Press, 1998.

Agamben, Giorgio. *Means without End: Notes on Politics*. Minneapolis: University of Minnesota Press, 2000.

Ahdar, Rex and Ian Leigh. *Religious Freedom in the Liberal State.* 2nd ed. Oxford: Oxford University Press, 2013.

Ahdar, Rex. “Navigating Law and Religion: Familiar Waterways, Rivers Less Travelled and Uncharted Seas.” In *Research Handbook on Law and Religion*, edited by Rex Ahdar, 2–16. Cheltenham: Edward Elgar, 2018.