Digital Privacy: GDPR and Its Lessons for Australia

Ratul Das Chaudhury ⬤ and Chongwoo Choe*

Abstract

Australia's Privacy Act 1988 is under review with a view to bringing Australia's privacy laws into the digital era, more in line with the European Union's General Data Protection Regulation (GDPR). This article discusses how the GDPR can be refined and standardised to be more effective in protecting privacy in the digital era while not adversely affecting the digital economy that relies heavily on data. We argue that an ideal data policy should be informative and transparent about potential privacy costs while giving consumers a menu of opt-in choices into which they can self-select.

* Das Chaudhury: Monash Digital Lab, Monash Business School, Monash University, Clayton, Victoria, 3800, Australia; Choe: Department of Economics, Monash Digital Lab, Monash Business School, Monash University, Clayton, Victoria, 3800, Australia. Corresponding author: Das Chaudhury, email <ratul.daschaudhury@monash.edu>.

1. Introduction

If this is the age of information, then privacy is the issue of our times. Activities that were once private or shared with the few now leave trails of data that expose our interests, traits, beliefs, and intentions. (Acquisti, Brandimarte & Loewenstein 2015).

A popular business model adopted by many of the world's largest tech platforms is the so-called broadcasting model where services are provided free in return for advertising revenue. These firms collect and process consumer data generated from the use of their 'free' services. Consumer data thus gathered can help create value for the business in various ways: it can be used for product improvement, for developing new business models, or for general management purposes; the data can be also monetised through sales of data-based services or even by direct sales of data to third parties.[1] A famous quote dating back to the 1970s in relation to advertising in commercial broadcasting resonates even louder in the digital era: *if you are not paying for the product, then you are the product*. But the key difference between the traditional broadcasting model and the business model in the digital era is the role played by consumer data.

In the age of digital transformation, buyers are not only consumers but also producers of data, which in turn becomes a valuable input to the production of goods and services. Indeed, data is the new oil in the digital era, as famously declared by *The Economist* in 2017.[2] Consumer-generated data analysed with powerful machine-learning tools can enable firms to offer

new or improved products, develop more target-oriented business models, and venture into new business opportunities (Hagiu & Wright 2020). Online recommendation systems and targeted advertising have become the cornerstone of modern-day marketing. The availability of big data and finer-grained analysis has also enabled firms in some industries to exercise personalised pricing, once considered only a theoretical possibility (Choe, King & Matsushima 2018; Chen, Choe & Matsushima 2020).[3]

Consumer data is collected not only by tech platforms with which consumers directly interact, but also by data brokers who collect and sell data to third parties. There are about 4,000 data brokers globally, including companies such as Acxiom and Oracle, who keep an enormous amount of data about individual consumers, ranging from relatively harmless data such as the city of residence to more sensitive data such as health issues or police records. A recent estimate suggests that the global data broker market is worth approximately US$250 billion in 2020 and is expected to grow to US$365 billion in 2027.[4]

Given the stratospheric rise of large tech platforms, the expansion of the data brokerage industry, and the rapid growth in online activities, consumers are increasingly concerned about the privacy risks associated with how their personal data is collected and shared. According to the Australian Community Attitudes to Privacy Survey 2020 (OAIC 2020), privacy is a major concern for 70 per cent of Australians, and almost 9 in 10 want more choice and control over their personal information. The survey also finds that 84 per cent of Australians perceive identity fraud and data breaches as the biggest risk to data privacy. Such a concern is well justified: from January to June 2021, the Office of the Australian Information Commissioner received 446 data breach notifications, with about half of these breaches resulting from cyber security incidents.[5] Similar sentiments towards online privacy are observed in the United States: a study by Pew Research Center reports that about 80 per cent of Americans think their personal data is less secure now and that data collection poses more risks than benefits (Auxier et al. 2019).

Before the advent of the digital era, privacy was not viewed as something that needed regulatory protection, an argument put forward most notably by the Chicago School. Posner (1981) regarded the 'right to privacy' of fully-informed economic agents with control over disclosing or withholding information as a mere artefact, rendering any legislation to protect privacy unnecessary. He argued that any regulatory intervention would interfere with the efficient flow of information. But Acquisti & Grossklags (2005) challenge this view by arguing that people are not informed enough to make privacy-sensitive decisions and, even when they are sufficiently informed, they trade off long-term privacy for short-term benefits. The latter is also related to the so-called privacy paradox whereby people relinquish privacy in exchange for small incentives, even though their stated preferences for privacy may be strong (Berendt, Günther and Spiekermann 2005; Athey, Catalini & Tucker 2017). In addition, the monitoring of personal information is ubiquitous in the digital era, as the opening quote suggests. A recent study finds that 80 per cent of the data collected by online service providers through mobile apps is not related to the direct performance of the app, but is primarily shared with data brokers or third parties for analytics, advertisement and so on (Bian, Ma & Tang 2022). In short, people are barely aware of the extent to which their personal information is collected and shared; nor do they have full control over their personal information.[6]

Even if people are well-informed, their decision to share personal information is influenced by various behavioural elements. Johnson, Bellman & Lohse (2002) provide experimental evidence that well-informed individuals' decision to share personal information is significantly affected by the default option and framing effect. For example, individuals are more likely to share personal information when facing an opt-out choice than an opt-in choice. In the former, data collection is the default setting while, in the

latter, no data collection is the default setting. In addition, many studies report that websites can influence consumers' data sharing decision by using dark patterns, implied consent to data collection and various forms of nudging (Utz et al. 2019; Machuletz and Böhme 2020; Matte, Bielova & Santos 2020; Nouwens et al. 2020; Obar & Oeldorf-Hirsch 2020). Such evidence, admittedly more relevant after the advent of the digital era, weakens the Chicago School's argument and lends support to regulatory protection of privacy.

The European Union's General Data Protection Regulation (GDPR) that came into effect in 2018 is a response to the growing privacy concern in the digital era. The two key pillars of the GDPR are privacy rights and data security. The former stipulates individuals' right to explicit opt-in consent, right to be forgotten and right to data portability, while the latter mandates protection against privacy breaches through unauthorised access. It was followed by similar privacy laws and regulations around the world. In Australia, the Attorney-General announced in 2019 that the Australian Government would conduct a review of the *Privacy Act 1988*, as part of the government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry.[7] The review seeks to bring Australia's privacy laws into the digital era and, therefore, the GDPR assumes critical relevance in the review.

The GDPR is a good starting point for protecting privacy in the digital era. But it is not without problems. One of the key requirements of the GDPR is that consumers be allowed to make an informed, specific and unambiguous opt-in consent to the processing of their data. But several studies suggest that the GDPR does not appear to be effective in allowing consumers to make an informed opt-in choice (Nouwens et al. 2020; Obar & Oeldorf-Hirsch 2020). Arguably, it is because the GDPR does not go beyond requiring opt-in consent and, therefore, is not refined enough for consumers to make an informed opt-in choice. Second, growing evidence shows that the GDPR has had an adverse effect on data-driven businesses and innovation (Aridor, Che

& Salz 2020; Jia, Jin & Wagman 2021; Janßen et al. 2022). As we argue in this article, one of the reasons for this is that the GDPR's opt-in policy can be too blunt a tool in balancing the trade-off between privacy and the benefits from data. In particular, it does not recognise the fact that consumers differ in their privacy preferences and different types of data have different values. Third, the GDPR's strict and one-size-fits-all privacy regulations have been shown to tilt the playing field in favour of larger firms and increase market concentration (Schmitt, Miller & Skiera 2020; Bian, Ma & Tang 2022; Johnson, Shriver & Goldberg 2022; Peukert et al. 2022). Consequently, the GDPR needs to be improved and refined not to stifle competition and investment in data-driven businesses while protecting privacy more effectively.

The purpose of this article is to critically assess the GDPR with a view to offering some recommendations as to how the GDPR can be modified to balance the trade-off between the benefits of data and privacy. Learning from the (un)intended consequences of the GDPR, we aim to contribute to the review of Australia's Privacy Law. To keep our discussion focused and at a manageable length, we mainly discuss data collection in this article. Our key point is that an effective privacy policy needs to start by recognising the heterogeneity in consumers' privacy preferences and data types. Based on this recognition, consumers need to be given a menu of clear, transparent opt-in choices, into which different consumers can self-select. Compared to the GDPR and other existing privacy regulations, our proposed privacy policy is more effective in protecting privacy without leading to undesirable loss of valuable data.

The rest of the article is organised as follows. In Section 2, we discuss the key elements of the GDPR, provide evidence on the effects of the GDPR and document the problems identified with the GDPR. Section 3 discusses how the data policy under the GDPR can be modified in the Australian context to better manage the trade-off between privacy and the benefits from data. This is followed by a brief conclusion in Section 4.

2. The GDPR and Its Effects

Privacy concerns arise when personal data is collected and shared without the knowledge or consent of the data subjects.[8] On the other hand, consumer data is a valuable input in the digital era, as explained previously. The ACCC's latest report on the digital platform services inquiry acknowledges that data is fundamental to the digital economy by delivering important societal benefits in the form of new products, better delivery of services, including government services, and advances in medicine, communications, and responses to threats such as natural disasters (ACCC 2022, p. 57). In addition, data sharing can be vital for innovations leading to new products and services. For example, sharing health data can be instrumental in innovations in health care (or tackling the global pandemic such as COVID-19), and sharing detailed automation data is required for developing the technology for safer self-driving cars. Finally, given the data advantages enjoyed by large digital platforms that may also work as barriers to entry, data sharing can be considered necessary in promoting competition, open banking being a prime example.[9] Strict privacy laws may help protect privacy but stifle innovation and competition, and harm data-driven businesses. Thus, the key question is how to balance the benefits of data and the costs of privacy breaches.

Before the GDPR, the Data Protection Directive (Directive 95/46/EC) adopted by the European Union in 1995 specified a number of guidelines for the collection and use of personal data. The Data Protection Directive builds on the principles such as notice, purpose, consent, security, disclosure, access and accountability. But these guidelines were non-binding and not specific enough. Consequently, online businesses often relied on opaque processes in collecting data, rendering consumers little or no control over how their data is collected and used. In this section, we first discuss how firms collected consumer data before the GDPR. Then we discuss how the GDPR tried to rectify the problem, after which we document studies that report 'unintended' consequences of the GDPR.

2.1 Data Collection

There are various ways digital businesses collect user data, the use of internet cookies being one of the most popular methods. Cookies (HTTP cookies, internet cookies, web cookies or browser cookies) are small text files that are downloaded into the user's device by a web browser when the user visits a particular website. They are browser- and site-specific.[10] Cookies were initially designed to enhance user experience, reduce network traffic and lower server storage costs by enabling web servers to store useful user information including browsing activity, and retrieve this information during subsequent page visits. Over time, however, third-party cookies have become commonly used by analytics firms and advertisers primarily to gather user data. These are cookies issued by an external domain and not by the website a user is browsing and can track a user across websites.

A website's cookie policy can be based on users' opt-in consent or opt-out consent. In the former, no data collection is set by default and the website can collect data only when the user explicitly opts in to data collection by agreeing to accept the website's cookies. In the latter, data collection is set by default and users have to act proactively to opt-out if they do not want to accept the website's cookies. Studies show that default settings matter for individual decisions in various contexts (Acquisti, Brandimarte & Loewenstein 2015) including online privacy policies. For example, Johnson, Bellman & Lohse (2002) provide evidence from online privacy experiments showing that opt-in results in much lower levels of participation (20 per cent) than opt-out (75 per cent). In a similar vein, Johnson, Shriver & Du (2020) examine the AdChoices program in the United States and its opt-out mechanism for data consent and report that only a small fraction of consumers opt out of online behavioural advertising: only 0.23 per cent of ad impressions are from

opt-out consumers. Consequently, websites can collect more data when they rely on opt-out consent than opt-in consent.

Prior to the GDPR or in jurisdictions without GDPR-style data protection laws such as the California Consumer Privacy Act, digital businesses tried to keep users in the dark regarding how their data is collected. Their websites typically detailed their privacy policies in a long and complex legal language, but without much information on their cookie policies. Even when the website provides information on its cookie policies, opt-out consent was a dominant form of data collection. It is conceivable that some tech-savvy, privacy-conscious consumers may proactively choose to opt out of the website's data collection or delete cookies after each session.[11] Nonetheless, the absence of a clear opt-in choice resulted in the unregulated collection of personal data with the potential for privacy breaches, prompting the necessity of various privacy regulations and laws around the world.

2.2 The GDPR

The stated purpose of the GDPR is to protect natural persons with regard to the processing of personal data, to promote the free movement of such data and to repeal Directive 95/46/EC. The GDPR is the most stringent law governing personal data protection. It was adopted on 14 April 2016, and became enforceable on 25 May 2018. The GDPR builds on the same principles as its predecessor, the Data Protection Directive 95/46/EC, but it superseded the Directive with more specific data protection requirements, stiffer enforcement and penalties for non-compliance. Importantly, the GDPR enhances individuals' control over data by stipulating the right to explicit consent, the right to data erasure, and the right to data portability. The GDPR's consent requirement stipulates that consumers be allowed to make informed, specific and unambiguous consent to allow businesses to process their data. Thus, it requires in principle opt-in consent to data collection, which essentially bans data controllers from

using opt-out options, a predominant way to obtain consent prior to the GDPR.[12]

The GDPR became a blueprint for various privacy regulations in countries such as Chile, Brazil, Japan, New Zealand, Singapore, South Korea, and so forth. The United States does not have a federal-level law on consumer privacy like the GDPR. Instead, a few US states have laws to protect consumer privacy, with California taking the lead. The California Consumer Privacy Act (CCPA) was signed into law in 2018 and took effect in 2020. The CCPA secures new privacy rights for consumers in California by providing them with the rights to know, to delete, to opt-out and not to be discriminated against based on their personal information. In this sense, the CCPA is similar to the GDPR, although there are differences in their legal framework, the scope of personal information covered, transparency obligations and so on[13] It is also worth noting that the CCPA requires opt-out rather than opt-in as in the GDPR, but it limits the selling of personal information, requiring a 'Do Not Sell My Personal Information' link to be included by businesses on their homepage.[14] Other states such as Maryland (Maryland Online Consumer Protection Act) and New York (New York Privacy Act) also require firms to inform consumers about the broad categories of information shared with third parties, but without allowing the consumers an opportunity to opt-out.

2.3 The Effect of the GDPR on Cookie Policies

Following the enactment of the GDPR and its commencement in 2018, there has been a significant increase in the use of cookie consent notices, transparent display of privacy policy and opt-in consent, and some decrease in the use of cookies. At the same time, there have been numerous reported cases of GDPR data breaches and fines for non-compliance.

First, Degeling et al. (2019) examined the 500 most popular websites for each EU country—6,579 websites in total—between December 2017 and October 2018. They found a significant increase in the display of cookie

consent notices, or cookie banners, which inform users about a site's cookie use and user tracking practices. There was a 16 per cent rise in the implementation of cookie consent notices among these websites, from 46.1 per cent in January 2018 to 62.1 per cent in May 2018. The websites displaying cookie banners increased by 43 per cent in Ireland and 45.4 per cent in Italy.

Second, according to Degeling et al. (2019), the majority of websites they examined had some form of privacy policies in January 2018, which rose to 84.5 per cent after May 2018. Countries with a lower rate of privacy policies (e.g., Latvia) added more privacy policies than those where privacy policies were already common (e.g., Germany, Spain). As for industries, the availability of privacy policies in the EU increased by 9.7 per cent in education, 7.1 per cent in health and 6.8 per cent in government websites, to name but a few.

Third, during the past decades, the use of third-party cookies had been increasing, largely due to the increased use of web analytics, targeted advertising and marketing campaigns. For example, as of 2014, many websites set over 100 third-party cookies, with a maximum number of cookies (both first and third-party) reaching over 800.[15] A month after the GDPR took effect, Degeling et al. (2019) found no significant change in the use of third-party cookies although the number of first-party cookies decreased from 22 to 18 on average. On the other hand, Libert, Graves & Nielsen (2018) found from popular news websites in seven EU countries that the average count of third-party cookies per page has gone down by 22 per cent following the GDPR, 45 per cent in the UK, 33 per cent in Spain and 32 per cent in Italy and France. They also found that the GDPR led to a reduction in advertising and marketing cookies by 14 per cent, and social media cookies by 9 per cent.

Finally, there have been numerous cases of GDPR non-compliance and attendant fines. The GDPR Art. 83 and 84 stipulate that relevant national authorities must assess and impose fines for data protection violations. The fines could be up to 20 million euros or 4 per cent of the total global turnover of the preceding fiscal year, whichever is higher. Nonetheless, many businesses were slow in getting their websites GDPR-compliant. By May 2018, over 800 fines were issued for GDPR non-compliance. The biggest fine to date is 746 million euros that the Luxembourg National Commission for Data Protection imposed on Amazon on 16 July 2021 for violating data processing guidelines and forcing users to comply with cookie policies. Other examples of large fines include 225 million euros for WhatsApp, 90 million euros for Google Ireland, 60 million euros for Facebook, 20 million pounds for British Airways and 20.4 million euros for Marriott.[16] More recent cases are the fines France's privacy watchdog (CNIL) levied on Google (150 million euros) and Facebook (60 million euros) in January 2022 for making it difficult for users to reject cookies,[17] and the fine Ireland's Data Protection Commission issued in September 2022 to Instagram (405 million euros) over children's data privacy.[18]

2.4 The 'Unintended' Consequences of the GDPR

In the assessment of the GDPR two years after it took effect, the European Commission hailed it as an overall success, in particular by empowering citizens through enhanced transparency and privacy rights, and by providing businesses with a harmonised framework for the protection of personal data.[19] Although the information provided in the previous section lends some support to this assessment, our view is that such an assessment might be misleading.

First, the GDPR's cookie rules do not go beyond requiring opt-in consent and, therefore, are not refined enough for consumers to make an informed opt-in choice. Indeed, GDPR-compliant cookie policies can take different forms as long as they are largely consistent with the GDPR's principle of opt-in consent for data collection. For example, a website may have a simple binary opt-in policy as in the *Financial Times*, where a user can allow or block all non-essential cookies, as shown in

Figure 1 Cookie Policy at the *Financial Times*

Figure 1.[20] In this case, consumers may not understand the full implications of opt-in.

In the case of the English Premier League Football website, non-essential and third-party cookies are further divided into nine different groups with a brief description of their purposes, and users can opt-in to each of them separately, as shown in Figure 2.[21]

Although the English Premier League Football website's cookie policy is more informative than a binary choice, consumers who are not tech-savvy may find it difficult to make an informed choice. Given that consumers' main concern in data collection is privacy, it would be better if information is given on what type of data is collected and how privacy-invasive it is. Consequently, a more careful study is needed to examine whether the GDPR has empowered European citizens through enhanced transparency and data privacy. But the available evidence does not appear to support the European Commission's assessment. For example, Nouwens et al. (2020) scraped the designs of the five most

popular consent management platforms introduced after the GDPR on the top 10,000 websites in the UK, and find that dark patterns and implied consent are ubiquitous.[22] In addition, Obar & Oeldorf-Hirsch (2020) provide experimental evidence showing that participants demonstrate general apathy toward privacy and select the 'quick join' clickwrap to simply access the website while ignoring the website's privacy policy and terms of service.[23] If a user agrees to the consent notices to save time and get past the large banners to get access to the website's content, then it defeats the purpose of 'informed consent' stipulated in the GDPR guidelines.

Second, research shows that the GDPR has had an adverse effect on data-driven businesses and innovation. The GDPR's opt-in policy can be too blunt a tool in balancing the trade-off between privacy and the benefits of data. As mentioned previously, opt-in consent results in less participation than opt-out consent, implying a decrease in data collection, which in turn can harm businesses and

Figure 2 Cookie Banner at the English Premier League

innovations that rely heavily on data. Indeed, the GDPR has been shown to significantly reduce the number of visits to a website (Aridor, Che & Salz 2020; Schmitt, Miller & Skiera 2020). For example, Aridor, Che & Salz (2020) report about a 12.5 per cent reduction in total cookies after the GDPR. In addition, Jia, Jin & Wagman (2021) report that the GDPR has dampened incentives to invest in data-related B2C ventures while Janßen et al. (2022) show that the GDPR has induced the exit of about 1/3 of available apps at the Google Play Store. Finally, strict privacy laws can tilt the playing field in favour of large firms (Campbell, Goldfarb & Tucker 2015). This is supported by several studies that report evidence that the GDPR increased market concentration on websites

(Schmitt, Miller & Skiera 2020) and web technology services (Johnson, Shriver & Goldberg 2022; Peukert et al. 2022). Somewhat related, Apple's release of privacy label requirements in 2020 is shown to have resulted in a decrease in iOS app downloads and app developers' revenue, but smaller firms are more adversely affected than larger firms (Bian, Ma & Tang 2022).

Put together, one may question if the GDPR is effective in managing the trade-off between privacy and the benefits of data. It could well be that the GDPR's focus was too much on privacy without fully taking into account the benefits of data and the implications for competition. Even on the privacy side, however, it is questionable if the GDPR enabled consumers to make an informed choice in agreeing to the processing of their data. In addition, the case is rather clear, and the evidence is accumulating, that the GDPR has adversely affected data-driven businesses.[24]

3. Lessons From the GDPR for Australia

In Australia, the *Privacy Act 1988* (*Privacy Act*) was introduced to protect the privacy of Australian citizens and to regulate the process of how personal information is handled by 'reasonably large' organisations.[25] The 13 Australian Privacy Principles (APPs) place a general obligation on organisations about protecting consumer data against loss, interference, or misuse by unauthorised parties. The APPs are principles-based laws and provide guidelines for data collection, data anonymisation, data security, direct marketing, and so forth. Since the introduction of the *Privacy Act*, however, there has been a significant change in the digital landscape in Australia, which calls for the adaptation of the APPs in the digital era.[26] This is also echoed in the ACCC's latest report on the digital platform services inquiry. Specifically, the ACCC states that the *Privacy Act 1988* does not contain sufficient mechanisms to allow consumers to understand and control how their data is collected and for what purposes (ACCC 2022, p. 174) and recommended changes to Australia's privacy regime to better

account for the ways in which consumer privacy can be degraded in the online economy (ACCC 2022, p. 68).[27]

Compared to the GDPR, the APPs give businesses more autonomy and flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. Given that Australian businesses operating outside the European Union are not subject to the GDPR, we observe that Australian websites vary widely in the way they display cookie banners or provide information on their privacy policies. Many websites do not display cookie banners that allow users to opt-in or opt-out of their cookie policies. For example, *The Age* provides a long and detailed privacy policy statement without giving clear opt-out or opt-in choices on its website; in order to opt out, users are asked to send an email.[28] As another example, the Commonwealth Bank of Australia describes the types of cookies they use along with an instruction on how users can delete cookies from their browsers, but not the GDPR-style opt-in boxes that users can tick.[29] In contrast, the Australian Broadcasting Corporation displays a cookie banner that gives users an option to accept only required cookies or all cookies including performance and marketing cookies, hence is GDPR-compliant, albeit in the simplest way.[30]

In this section, we discuss how data collection under the GDPR can be modified to better manage the trade-off between privacy and the benefits of data. Specifically, we focus on how the various cookie policies described above can be refined and standardised in a way that is more informative to consumers while not leading to unnecessary loss of valuable data. The key starting point is to recognise the fact that there are different types of data with different benefits and privacy costs, and consumers' attitudes towards privacy are also different across individuals. We discuss this below, followed by suggestions as to how the cookie policy under the GDPR can be modified. We then provide an illustrative example to clarify our main point.

3.1 Data Types and Consumer Heterogeneity

The GDPR Art. 4(1) defines personal data as 'any information relating to an identified or identifiable natural person ("data subject"); … such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'.

Clearly, personal data includes a host of information, some of which may be more valuable to the firm than others. For example, a consumer's income level would be more valuable information than gender information where a firm uses the information for targeted promotion. Likewise, some personal data may cause more privacy concerns than others when shared with the firm. In an experimental study, Lin (2022) estimates consumers' intrinsic preferences for privacy based on their willingness to accept (WTA) monetary compensation in exchange for their personal data. She reports the estimated WTA of $0.14 for gender information and $3.82 for income information. These observations suggest that one needs to classify personal data based on at least two attributes, (benefits to the data collector, and privacy costs to the data subject). A logical conclusion is that a desirable cookie policy is the one that leads to the collection of more data types with larger benefits and lower privacy costs.

Consumers also differ in their attitudes towards privacy because what constitutes sensitive personal information differs across individuals. Acquisti, Brandimarte & Loewenstein (2015) discuss studies that cluster individuals to three privacy segments: privacy fundamentalists, pragmatists, and unconcerned. Goldfarb & Tucker (2012) report differing preferences for privacy across different age groups. Lin (2022) provides experimental evidence that shows people are highly heterogeneous in their preferences for privacy. For example, more educated and wealthier consumers tend to have stronger preferences for privacy. Recognising such heterogeneity is important since one-size-fits-all cookie policies can result in either too much or too little data collected. A desirable cookie policy that recognises consumer heterogeneity is the one that offers a menu of opt-in choices, into which different consumers can self-select.

3.2 Towards a More Effective Cookie Policy

There are two main factors to consider in designing an effective cookie policy. First, it needs to be informative and easy to understand. Research shows that users respond more effectively when privacy notices are concise and displayed in a salient way (Ebert, Ackermann & Scheppler 2021). Apple's Privacy Nutrition Labels introduced in 2020 serve as a good example. Their purpose is to provide users with standardised and transparent information regarding the way iOS app developers collect and use consumer data, as shown in Figure 3.[31] The privacy labels fall into three categories: Data Not Linked to You, Data Linked to You, and Data Used to Track You. The first category relates to data that does not count as personal information. The second

Figure 3 Apple's Privacy Nutrition Labels
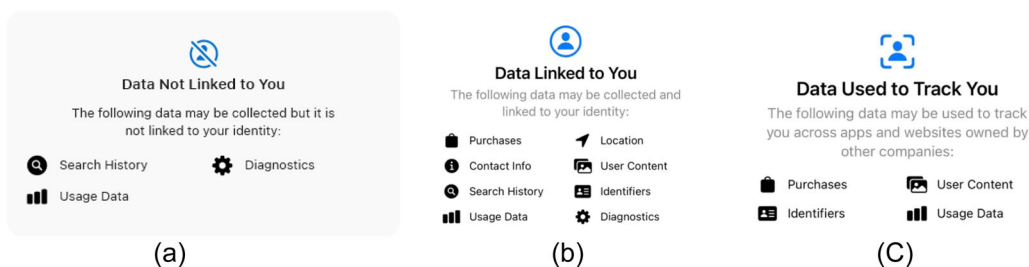
category is about data that is linked to a user's identity such as account details, device ID and so on An important difference between the first two categories is that, in the first category, any data that can be used to identify a user needs to be stripped of any identifiable information before collection. For example, search history appears in both categories as shown in (a) and (b) in Figure 3, but in (a), such data is collected after any information that can be used to identify a user has been removed. The third category relates to data that is collected from third-party websites and can be used for ads or shared with a data broker. Thus one can say the first category represents the least invasive data collection, and the third is the most invasive.[32] Bian, Ma & Tang (2022) report that the introduction of privacy labels was conducive to raising privacy awareness, consistent with the experimental evidence in Ebert, Ackermann & Scheppler (2021).

Second, users need to be given clear choices presented in a transparent way. For example, cookies can be divided into several groups, depending on the types of information collected, how invasive the tracking can be and for what purposes the data is used. Once again, Apple's Privacy Labels can be a good example in this regard. However, Apple does not allow consumers to opt in to only a subset of cookies: the user faces a binary choice of agreeing to all data collection or none.[33] After Apple introduced the binary choice for opt-in consent, just about 4 per cent of US users are reported to have opted in, with adverse effects on app developers and advertisers.[34] Giving users more choice may have resulted in more users opting in to a subset of cookies, thereby preventing unnecessary loss of valuable data.

Based on the above discussions, we argue that a desirable cookie policy needs to combine transparency and informativeness as in Apple's Privacy Labels with several options to opt in to different sets of cookies. Clear and transparent gradations will reduce the cognitive load on consumers when making their privacy choices. A simple example would be to classify all cookies into three categories depending on how privacy-invasive the data collection can be, as in Apple's Privacy Nutrition Labels. Each category needs to have a clear explanation of possible privacy costs and the expected benefits if consumers opt-in. Given this, consumers have the choice to opt in to each category of cookies separately. Consumers choosing to opt in to highly privacy-invasive cookies would do so because they are less privacy-sensitive and/or because they expect extra benefits by opting into that category of cookies, which more than offset their privacy concerns. Consumers with significant privacy concerns may opt-in to only the least invasive category of cookies. This way, consumers can self-select into different sets of cookies, thereby optimally balancing their privacy costs and the utility from using the website. As a result, different amounts of data are collected from different types of consumers, which improves upon the case where opt-in choice is binary. This will also reduce socially inefficient loss of data that could result when consumers face a binary opt-in choice. In the next section, we illustrate this idea with an example.

3.3 An Illustrative Example

In this section, we provide a simple example that clarifies the point we discussed above. Our main aim is to show that, given the heterogeneity in consumers' privacy preferences and data types, allowing consumers to make choices on a finer menu of options is weakly more efficient than allowing them a coarser menu of options. Here, efficiency relates to both the amount of data collected and privacy costs incurred by consumers. That is, efficiency dictates that data is collected if and only if the social value of data less the privacy costs borne by consumers is positive. Note also that consumers' self-selection matters because their privacy preferences are private information, which generally prevents the first-best optimum from being implemented. Thus, the purpose of the example is not to show that a finer menu of options can implement the first-best optimum;[35] rather, it is to show that a finer menu of self-selecting options can alleviate the inefficiency associated with existing privacy regulations based on opt-out or binary opt-in choice.

Specifically, we compare below three privacy regimes: (i) no privacy regulations, (ii) binary opt-in regulations, and (iii) self-selecting opt-in regulations.

Consider an economy with two consumers, indexed $i = \{1, 2\}$, two types of data for each consumer, denoted by $\theta = \{a, b\}$, and one digital business, which we simply call the firm. Each type of data from each consumer has value to the firm denoted by $\pi_\theta > 0$. Data also has additional value to the economy as a whole because data can create external benefits beyond the firm that collects it.[36] Thus, the social value of data exceeds the private value of data to the firm, which we denote by v_θ where $v_\theta > \pi_\theta$. A consumer agreeing to share their data with the firm incurs expected privacy cost that is consumer- and data-dependent, denoted by $c_{i\theta} > 0$ for $i = \{1, 2\}$ and $\theta = \{a, b\}$. For example, the privacy cost incurred by consumer 1 in sharing type-*a* data with the firm is c_{1a}.[37]

Consumer 1 is more privacy-sensitive than consumer 2 in the sense that $c_{1\theta} > c_{2\theta}$ for $\theta = \{a, b\}$. A consumer's privacy sensitivity is their private information. We assume that type-*a* data is less privacy-invasive, hence leading to lower privacy costs to consumers, than type-*b* data. But it also has a lower value to the firm and the economy as a whole.[38] For example, type-*a* data may include the consumer's name, email address, city of residence and so on, while type-*b* data may include credit card details, purchase behaviour, browsing history, health details and so on We summarise our assumptions below.

Assumption 1 $c_{2a} < c_{1a}$ and $c_{2b} < c_{1b}$.

Assumption 2 $c_{1a} < \pi_a < v_a$ and $\pi_b < v_b < c_{1b}$.

Assumption 3 $c_{2a} < \pi_a < v_a$ and $c_{2b} < \pi_b < v_b$.

Assumption 2 implies that it is socially optimal to collect only type-*a* data from consumer 1, while Assumption 3 implies that it is socially optimal to collect both types of data from consumer 2.

3.3.1 No Privacy Regulations

Consider first the case where the firm can costlessly collect data and consumers do not make opt-in decisions.[39] This may describe the situation before the GDPR where the traditional broadcasting model applies. Consumers may simply log in to the firm's website to enjoy its 'free' service without knowing that their data is being collected. This may also apply to jurisdictions where opt-out is a default setting for data collection. As discussed previously, default settings matter for individual decisions, and online privacy experiments show that opt-out results in much higher levels of participation than opt-in. Since the firm does not need to induce consumers' opt-in, it only cares about π_θ and ignores the consumer's privacy cost. Consequently, the firm will collect both types of data from both consumers, resulting in too much data being collected relative to the social optimum.

3.3.2 Binary Opt-in Regulations

Suppose now consumers proactively make opt-in decisions but the opt-in choice is given in a binary form in which the consumer opts in to both types of data or none. Given the prevalence of binary opt-in consent in GDPR-compliant websites, one can say this is a reasonable description of the situation after the GDPR. Unlike the first case, cookie banners and opt-in consent boxes inform consumers of possible privacy costs that may follow their opt-in decisions. This means that, in order to induce consumers to opt-in, the firm needs to provide additional benefits to consumers to compensate for their privacy cost, by providing improved service or even offering monetary incentives such as discounts or promotions through loyalty programs.[40] We call these opt-in benefits, denoted by γ, which are assumed to be equal to the cost to the firm in providing the benefits. The firm chooses γ to maximise its profit. Then, there are two possible cases to consider.

First, suppose $\sum_\theta c_{1\theta} < \sum_\theta \pi_\theta$. By Assumption 3, we also have $\sum_\theta c_{2\theta} < \sum_\theta \pi_\theta$.

Thus, the firm can induce opt-in by both consumers by choosing $\gamma \in \left(\sum_\theta c_{1\theta}, \sum_\theta \pi_\theta\right)$, or opt-in by consumer 2 only by choosing $\gamma \in \left(\sum_\theta c_{2\theta}, \sum_\theta c_{1\theta}\right)$. In the former case, the firm maximises its profit by choosing $\gamma = \sum_\theta c_{1\theta}$, with the resulting profit $2\left(\sum_\theta \pi_\theta - \sum_\theta c_{1\theta}\right)$.[41] In the latter case, the firm maximises its profit by choosing $\gamma = \sum_\theta c_{2\theta}$, with the resulting profit $\sum_\theta \pi_\theta - \sum_\theta c_{2\theta}$. Then, it follows that the firm induces opt-in by both consumers if $\sum_\theta \pi_\theta - \sum_\theta c_{1\theta} > \sum_\theta c_{1\theta} - \sum_\theta c_{2\theta}$, and opt-in by consumer 2 only otherwise. Recall that it is socially optimal to collect only type-*a* data from consumer 1 and both types of data from consumer 2. Thus, binary opt-in regulations fail to achieve the socially optimal amount of data collection.

Second, suppose $\sum_\theta \pi_\theta \leq \sum_\theta c_{1\theta}$. In this case, the firm cannot choose $\gamma > 0$ that can induce consumer 1's opt-in. But, since $\sum_\theta c_{2\theta} < \sum_\theta \pi_\theta$ by Assumption 3, it can choose $\gamma = \sum_\theta c_{2\theta}$ to maximise profit by inducing consumer 2's opt-in. Thus, binary opt-in regulations result in loss of socially valuable data, type-*a* data from consumer 1 in this case.

In sum, binary opt-in regulations lead to a weakly smaller amount of data collected than when consumers do not make opt-in decisions, but socially optimal data collection is not possible under the binary opt-in choice, given the consumer heterogeneity. The primary reason for the latter is that, under binary opt-in regulations, the firm chooses only the aggregate size of opt-in benefits to induce consumers to share both types of data. In contrast, self-selecting opt-in regulations can allow the firm to choose opt-in benefits that can vary depending on the types of data, which we discuss below.

3.3.3 Self-Selecting Opt-in Regulations

Consider now the case where consumers can choose to opt in to each data type separately and the firm can offer opt-in benefits for each data type. Denote by γ_θ the opt-in benefits for type-θ data, $\theta = \{a, b\}$.

Consider first type-*a* data. Because $c_{2a} < c_{1a} < \pi_a$, the firm can choose $\gamma_a = c_{1a}$ to induce opt-in by both consumers, or $\gamma_a = c_{2a}$ to induce opt-in by consumer 2 only. The profit from the former is $2(\pi_a - c_{1a})$ and the profit from the latter is $\pi_a - c_{2a}$. Thus, the firm optimally collects type-*a* data from both consumers if $\pi_a - c_{1a} > c_{1a} - c_{2a}$, and from consumer 2 only otherwise.

Next, consider type-*b* data. Again, the firm can choose $\gamma_b = c_{1b}$ to induce opt-in by both consumers, or $\gamma_b = c_{2b}$ to induce opt-in by consumer 2 only. The profit from the former is $2(\pi_b - c_{1b})$ and that from the latter is $\pi_b - c_{2b}$. But we have $\pi_b - c_{2b} - 2(\pi_b - c_{1b}) = (c_{1b} - \pi_b) + (c_{1b} - c_{2b}) > 0$ because $c_{1b} > \pi_b > c_{2b}$ by Assumptions 2 and 3. Thus, the firm optimally chooses $\gamma_b = c_{2b}$ to induce opt-in by consumer 2 only.

Put together, we have the following outcome. If $\pi_a - c_{1a} \leq c_{1a} - c_{2a}$, then self-selecting opt-in regulations leads the firm to choose opt-in benefits $(\gamma_a, \gamma_b) = (c_{2a}, c_{2b})$. This results in both types of data collected from consumer 2 but no data collected from consumer 1. In this case, there is inefficiency since type-*a* data from consumer 1 is not collected. If $\pi_a - c_{1a} > c_{1a} - c_{2a}$, then self-selecting opt-in regulations lead the firm to choose opt-in benefits $(\gamma_a, \gamma_b) = (c_{1a}, c_{2b})$. This results in both types of data collected from consumer 2 but only type-*a* data collected from consumer 1, which is the socially optimal outcome. In this case, consumer 1 self-selects into opting in to only type-*a* data, which was not possible under binary opt-in regulations.

We summarise the main points from the example. Recognising that consumers differ in their privacy preferences and different data types have different social values, a key question is to identify privacy regulations that optimally balance the trade-off between the benefits from data and privacy cost. When consumers' privacy preferences remain private information that the firm cannot use in designing its cookie policy, the firm needs to be allowed to design a cookie policy that depends on data types. This can lead to a

separation of consumers with different privacy preferences into different opt-in choices. In the context of our example, efficient separation requires clear information about possible privacy costs, that is, $c_{i\theta}$, and the opt-in benefits that can vary depending on data types, that is, γ_θ. Although this is a simple example, a general point is that more refined opt-in regulations can alleviate the inefficiency in data collection associated with opt-out regulations or simple, binary opt-in regulations.

4. Conclusion

Australia's *Privacy Act* dates back to 1988, when the digital economy was still in its infancy. As the digital economy grows at breakneck speed and affects every aspect of our daily lives, consumers' digital privacy has become a pressing issue. The GDPR is a good starting point for protecting consumers' privacy in the digital era. But it appears that not enough consideration was given to the adverse effects of the GDPR on data-driven businesses. Nor is it clear if the intended privacy protection achieves the desired outcome. In this article, we have discussed how the GDPR can be refined and standardised to be more effective in protecting privacy while not stifling the data-based economy. Our main point is that an ideal data policy should inform consumers about possible privacy costs in a transparent way while giving consumers a menu of opt-in choices into which consumers can self-select. Compared to the GDPR's opt-in requirement, such a policy will be more effective in protecting privacy without leading to undesirable loss of valuable data.

Endnotes

1. See, for example, 'Data monetization: New value streams you need right now', *Forbes*, 9 June 2020.

2. 'The world's most valuable resource is no longer oil, but data', *The Economist*, 16 May 2017. For a comprehensive review of the literature on the digital economy, see Goldfarb & Tucker (2019).

3. Personalized pricing can hurt firms if firms with comparable data endowments compete in personalized

pricing, because it intensifies competition compared to when they do not use personalized pricing (Choe, King & Matsushima 2018). But it can benefit competing firms if consumers can bypass price discrimination by exercising identity management (Chen, Choe & Matsushima 2020).

4. https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/

5. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021

6. For a comprehensive review of the economics literature on privacy, see Acquisti, Taylor & Wagman (2016).

7. https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

8. One may ask if the problem can be solved by anonymising personal data before processing it, which is indeed a requirement in various data protection laws. However, Rocher, Hendrickx & de Montjoye (2019) demonstrate that anonymising personal data through deidentification is not a fail-safe way to protect privacy, showing that almost all Americans can be correctly re-identified in any dataset using 15 demographic attributes.

9. For discussions on the costs and benefits of customer data sharing in the digital era, see, for example, Liu & Serfes (2006) or Choe, Matsushima & Tremblay (2022).

10. As an example, Google Analytics uses a cookie named '_ga cookie' to assign a client ID to a user, which can be used to track the user in subsequent visits to the website. The _ga cookie comprises four distinct values (version, domain, random unique ID, and the first visit time stamp), and is used to uniquely identify the user. Each time the user takes action on a website or an app (called a 'hit'), the data and the user's client ID are sent back to Google Analytics.

11. Some privacy-sensitive consumers may also use browsers that are more privacy-oriented, for example, Mozilla Firefox, DuckDuckGo or Tor web browsers. These browsers help block a range of trackers and third-party cookies.

12. The GDPR applies uniformly to all businesses that handle personal data of EU residents, or operate in the EU. The European Data Protection Board (EPDB) has set the guidelines for GDPR compliance clarifying what is acceptable as valid consent (see https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf). For example, cookie banners cannot have pre-checked boxes, scrolling a website without accepting the cookie policy cannot be assumed as implied consent and so on.

13. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

14. Under both the GDPR and the CCPA, residual rights are vested in the firm. For example, if a consumer ticks the box requiring not to sell their personal information

under the CCPA, the firm is legally obligated to abide by the request. But it can still share personal information with third parties. For example, Paypal shares consumer information, such as name, e-mail address, IP address and so on with listed third parties (https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list). Additionally, businesses can use the collected information for product improvements, targeted advertising, or other activities.

15. https://en.wikipedia.org/wiki/HTTP_cookie

16. https://termly.io/resources/articles/biggest-gdpr-fines/

17. https://www.reuters.com/world/europe/france-imposes-fines-facebook-ireland-google-2022-01-06/

18. https://www.bbc.com/news/technology-62800884

19. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166

20. https://www.ft.com/preferences/manage-cookies

21. https://www.premierleague.com/cookie-policy

22. A dark pattern is a deceptive user interface that is designed to trick users into doing things that they did not intend to.

23. Related evidence on websites' nudging consumers into making specific choices is reported in Machuletz and Böhme (2020), and Matte, Bielova & Santos (2020). Utz et al. (2019) provide experimental evidence in support of this.

24. Needless to say, the GDPR's adverse effect on data-driven businesses needs to be assessed against possible gains from privacy protection. As we argued above, however, the GDPR does not appear to be effective in protecting privacy. The main aim of this article is to propose a privacy policy that better manages the trade-off between privacy and the benefits from data than the GDPR.

25. These organisations include all Australian government agencies, businesses with an annual turnover of at least A$3 million, and businesses that trade personal information, health services or businesses that have agreed to comply with the *Privacy Act*.

26. The APPs are technology neutral, which allows them to be adapted to changing technologies.

27. At the time of writing this article, the Attorney General's review of the *Privacy Act* is still under way. Thus, it is not clear what the final recommendations will entail, except that there will be a binding Online Privacy code for social media and some online platforms, and increased penalties and enhanced enforcement measures (https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988).

28. https://login.nine.com.au/privacy?client_id=theage

29. https://www.commbank.com.au/important-info/cookies.html?ei=CB-footer_cookies

30. https://help.abc.net.au/hc/en-us/articles/4447588409871

31. https://www.apple.com/au/privacy/labels/

32. For more details on the privacy labels, see Bian, Ma & Tang (2022).

33. Apple used to allow its app developers to track users' online activities by using Apple's IDFA (identifier for advertisers), a unique ID assigned to an Apple device. Consent to IDFA-tracking was set by default, although users could opt out. After its iOS 14.5 update in 2021, Apple introduced GDPR-style opt-in consent whereby users are given a binary option to click 'Allow' button in a pop-up message (https://developer.apple.com/app-store/userprivacy-and-data-use/).

34. https://mashable.com/article/ios-14-5-users-opt-out-of-ad-tracking

35. An optimal privacy policy given consumers' private information about their privacy preferences is an application of mechanism design under adverse selection, of which classic references are Mussa & Rosen (1978) or Baron & Myerson (1982). The resulting second-best optimal policy generally fails to achieve the first-best optimum due to incentive compatibility constraints.

36. For discussions on the positive externalities from data, see, for example, Fainmesser, Galeotti & Momot (2022) or Bergemann, Bonatti & Gan (2022).

37. Sharing data by one consumer can impose privacy costs on other consumers (Acemoglu et al. 2022; Choi, Jeon & Kim 2019; Ichihashi 2021). For simplicity, we do not consider such negative data externalities. But the analysis can be extended without difficulty.

38. Such a correlation between privacy cost and the value to the firm may be reasonable for some data and some industries, while the correlation can be in the other direction in other cases. Although we do not consider other cases, the analysis can be done in an analogous way.

39. Our main point stays robust when we allow consumers to make opt-in decisions with a small probability, as long as that probability is smaller than that under the GDPR.

40. Under the GDPR, businesses do not have the right to deny service or reduce quality of service to customers who choose not to provide personal information. But they can offer discounts or promotions to customers who choose to provide their personal information. An example is a loyalty program, which provides additional benefits in exchange for customer data.

41. We assume consumers choose opt-in when indifferent.

ORCID

Ratul Das Chaudhury ⬤ http://orcid.org/0000-0002-8836-9296

REFERENCES

ACCC 2022, 'Digital platform services inquiry', Interim report No. 5—Regulatory reform.

Acemoglu, D., Makhdoumi, A., Malekian, A. and Ozdaglar, A. 2022, 'Too much data: Prices and inefficiencies in data markets', *American Economic Journal: Microeconomics*, vol. 14, no. 4, pp. 218–56.

Acquisti, A., Brandimarte, L. and Loewenstein, G. 2015, 'Privacy and human behavior in the age of information', *Science*, vol. 347, no. 6221, pp. 509–14.

Acquisti, A. and Grossklags, J. 2005, 'Privacy and rationality in individual decision making', *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33.

Acquisti, A., Taylor, C. and Wagman, L. 2016, 'The economics of privacy', *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–92.

Aridor, G., Che, Y. K. and Salz, T. 2020, The economic consequences of data privacy regulation: Empirical evidence from GDPR, NBER Working Paper 26900, Cambridge, MA, USA.

Athey, S., Catalini, C. and Tucker, C. 2017, 'The digital privacy paradox: Small money, small costs, small talk', NBER Working Paper 23488, Cambridge, MA, USA.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. and Turner, E. 2019, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Research Center, Washington DC, USA.

Baron, D. and Myerson, R. 1982, 'Regulating a monopolist with unknown cost', *Econometrica*, vol. 50, pp. 911–30.

Berendt, B., Günther, O. and Spiekermann, S. 2005, 'Privacy in e-commerce: Stated preferences vs. actual behavior', *Communications of the ACM*, vol. 48, no. 4, pp. 101–6.

Bergemann, D., Bonatti, A. and Gan, T. 2022, 'The economics of social data', *RAND Journal of Economics*, vol. 53, no. 2, pp. 263–96.

Bian, B., Ma, X. and Tang, H. 2022, The supply and demand for data privacy: evidence from mobile apps, <https://ssrn.com/abstract=3987541>

Campbell, J, Goldfarb, A. and Tucker, C. 2015, 'Privacy regulation and market structure', *Journal of Economics & Management Strategy*, vol. 24, no. 1, pp. 47–73.

Chen, Z., Choe, C. and Matsushima, N. 2020, 'Competitive personalized pricing', *Management Science*, vol. 66, no. 9, pp. 4003–23.

Choe, C., King, S. and Matsushima, N. 2018, 'Pricing with cookies: Behavior-based price discrimination and spatial competition', *Management Science*, vol. 64, no. 12, pp. 5669–87.

Choe, C., Matsushima, N. and Tremblay, M. J. 2022, 'Behavior-based personalized pricing: When firms can share customer information', *International Journal of Industrial Organization*, vol. 82, p. 102846.

Choi, J. P., Jeon, D. S. and Kim, B. C. 2019, 'Privacy and personal data collection with information externalities', *Journal of Public Economics*, vol. 173, pp. 113–24.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. 2019, 'We value your privacy… now take some cookies: Measuring the GDPR's impact on web privacy', Network and Distributed Systems Security Symposium 2019, San Diego, CA, USA.

Ebert, N., Ackermann, K. A. and Scheppler, B. 2021, 'Bolder is better: Raising user awareness through salient and concise privacy notices', Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, article no: 67, pp. 1–12.

Fainmesser, I. P., Galeotti, A. and Momot, R. 2022, 'Digital privacy', *Management Science*, Forthcoming, https://doi.org/10.1287/mnsc.2022.4513

Goldfarb, A. and Tucker, C. E. 2012, 'Shifts in privacy concerns', *American Economic Review*, vol. 102, no. 3, pp. 349–53.

Goldfarb, A. and Tucker, C. E. 2019, 'Digital economics', *Journal of Economic Literature*, vol. 57, no. 1, pp. 3–43.

Hagiu, A. and Wright, J. 2020, 'When data creates competitive advantage', Harvard Business Review, January-February issue.

Ichihashi, S. 2021, 'The economics of data externalities', *Journal of Economic Theory*, vol. 196, p. 105316.

Janßen, R., Kesler, R., Kummer, M. E. and Waldfogel, J. 2022, 'GDPR and the lost generation of innovation apps', NBER Working Paper 30028, Cambridge, MA, USA.

Jia, J., Jin, G. Z. and Wagman, L. 2021, 'The short-run effects of the general data protection regulation on technology venture investment', *Marketing Science*, vol. 40, no. 4, pp. 661–84.

Johnson, E. J., Bellman, S. and Lohse, G. L. 2002, 'Defaults, framing and privacy: Why opting in-opting out', *Marketing Letters*, vol. 13, no. 1, pp. 5–15.

Johnson, G. A., Shriver, S. K. and Du, S. 2020, 'Consumer privacy choice in online advertising: Who opts out and at what cost to industry?' *Marketing Science*, vol. 39, no. 1, pp. 33–51.

Johnson, G. A., Shriver, S. K. and Goldberg, S. G. 2022, 'Privacy & market concentration: Intended & unintended consequences of the GDPR', Working paper, SSRN: https://ssrn.com/abstract=3477686

Libert, T., Graves, L. and Nielsen, R. K. 2018, 'Changes in third-party content on European news websites after GDPR', Reuters Institute for the Study of Journalism, Oxford, UK.

Lin, T. 2022, 'Valuing intrinsic and instrumental preferences for privacy', *Marketing Science*, vol. 41, no. 4, pp. 235–53.

Liu, Q. and Serfes, K. 2006, 'Consumer information sharing among rival firms', *European Economic Review*, vol. 50, no. 6, pp. 1571–1600.

Machuletz, D. and Böhme, R. 2020, 'Multiple purposes, multiple problems: A user study of consent dialogs after GDPR', *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 481–98.

Matte, C., Bielova, N. and Santos, C. 2020, 'Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework', IEEE Symposium on Security and Privacy, pp. 791–809.

Mussa, M. and Rosen, S. 1978, 'Monopoly and product quality', *Journal of Economic Theory*, vol. 18, pp. 301–17.

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. 2020, 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence', Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.

OAIC 2020, Australian community attitudes to privacy survey 2020. Prepared for the Office of the Australian Information Commissioner by Lonergan Research.

Obar, J. A. and Oeldorf-Hirsch, A. 2020, 'The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services', *Information, Communication & Society*, vol. 23, no. 1, pp. 128–47.

Peukert, C., Bechtold, S., Batikas, M. and Kretschmer, T. 2022, 'Regulatory spillovers and data governance: Evidence from the GDPR', *Marketing Science*, vol. 41, no. 4, pp. 318–40.

Posner, R. A. 1981, 'The economics of privacy', *American Economic Review*, vol. 71, no. 2, pp. 405–9.

Rocher, L., Hendrickx, J. M. and de Montjoye, Y.-A. 2019, 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications*, vol. 10, no. 1, pp. 1–9. https://doi.org/10.1038/s41467-019-10933-3

Schmitt, J., Miller, K. M. and Skiera, B. 2020, 'The impact of privacy laws on online user behavior', Working paper, arXiv:2101.11366v2.

Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T. 2019, '(Un)informed consent: Studying GDPR consent notices in the field', Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 973–90.