This PDF is a selection from a published volume from the National Bureau of Economic Research

Volume Title: The Economics of Privacy

Volume Authors/Editors: Avi Goldfarb and Catherine E. Tucker, editors

Volume Publisher: University of Chicago Press

Volume ISBNs: 9780226834078 (cloth), 9780226834085 (electronic)

Volume URL: https://www.nber.org/books-and-chapters/economics-privacy

Conference Date: October 14, 2022

Publication Date: August 2024

Chapter Title: Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond

Chapter Author(s): Garrett A. Johnson

Chapter URL: https://www.nber.org/books-and-chapters/economics-privacy/economic-research-privacy-regulation-lessons-gdpr-and-beyond

Chapter pages in book: p. 97–126

4

Economic Research on Privacy Regulation
Lessons from the GDPR and Beyond

Garrett A. Johnson

4.1 Introduction

Privacy is a conundrum. Privacy and the data economy are two sides of the same coin. Viewed from each side, progress on the respective dimension can seem obvious. Nevertheless, the two are often at cross-purposes.[1] Economic researchers can illuminate our understanding of privacy, the data economy, and the trade-offs involved. Policy makers and regulators worldwide wrestle with crafting and enforcing privacy regulation. Economic research can inform their difficult task.

The European Union's General Data Protection Regulation (GDPR) is a landmark privacy regulation that elevated the tension between privacy and the data economy. The European Union (EU) passed the GDPR in April 2016, but delayed enforcement until May 25, 2018. In many ways, the GDPR set the privacy regulation agenda globally. Dozens of countries have since passed privacy regulation, including Brazil, China, India, and New Zealand (Greenleaf 2023). At its heart, the GDPR defines personal data expansively to include all data relating to an individual. The regulation provides EU residents with multiple data rights, like the right to access and delete their

Garrett A. Johnson is an assistant professor of marketing at the Questrom School of Business at Boston University.

I thank Samuel Goldberg, Matthew Schneider, Scott Shriver, the book editors, and an anonymous referee as well as seminar participants at the NBER's 2022 Privacy Tutorial, the European Commission's Joint Research Centre Digital Economy Unit, the Federal Communications Commission, and Université Paris Dauphine for providing helpful comments. I thank the NBER for providing funding for this work. I dedicate this work to Luke. For acknowledgments, sources of research support, and disclosure of the author's material financial relationships, if any, please see https://www.nber.org/books-and-chapters/economics-privacy/economic-research-privacy-regulation-lessons-gdpr-and-beyond.

1. The World Bank devoted its 2021 World Development Report to exploring this tension.

data. The GDPR imposes responsibilities on firms like data auditing and data-breach notification. The regulation also lays out multiple legal bases—including consent—for processing personal data. The GDPR's maximum fines of 4 percent of a firm's annual revenue ensured it caught the attention of firms and the wider public. As a landmark and influential regulation, the GDPR is of great interest to economists.

However, the GDPR poses three key challenges for empirical research. First, economists often examine the GDPR as an event study but may lack a suitable control group in certain settings. In particular, the GDPR covers most of Europe and also has substantial global spillovers that contaminate candidate control group members. Second, GDPR compliance and enforcement vary by industry, compliance requirement, firm size, country, and over time. This creates gaps between the regulation as written and the regulation in practice which, in turn, complicates the conclusions we can draw from GDPR research. Third, the GDPR may directly restrict the availability—and selection into—individual-level data that economists can use to understand the impact of the regulation. As we will see, economists have proposed various solutions to and workarounds for these challenges.

Five years after the GDPR's enforcement deadline, economic research on the GDPR is maturing. To date, much economic research examines the GDPR's impact on firms. The GDPR hurt firm performance by imposing costs, decreasing revenue, and thereby hurting profitability. Venture funding for technology firms fell—particularly for more data-related ventures. The GDPR limited economic dynamism by accelerating market exit and slowing entry. At the same time, the GDPR created an opportunity to test hypotheses about the consequences of privacy regulation for firm competition and innovation (see, e.g., Goldfarb and Tucker 2012). Research shows that the GDPR hurt competition by creating greater harms for smaller firms and by increasing market concentration in the data vendor market. The evidence for innovation is more mixed, though several studies suggest that the GDPR constrained data-related innovation. Research shows that the GDPR reduces the share of individual-level data available to firms. When firms rely on consent to process data, consumer data becomes self-selected though consenting consumers tend to be favorably selected. On the web, studies show a decrease in EU traffic to web sites after the GDPR, a modest drop in ad revenue, as well as a short-lived reduction in sites' use of third-party vendors. However, the GDPR had no apparent effect at the Internet's connectivity layer or on web site content provision. Finally, the GDPR seemed to constrain firms' marketing activities for personalized channels like email and online display advertising.

Fewer studies examine the GDPR's consequences for consumers, though this gap largely reflects the inherent measurement challenge. Survey evidence quantifies consumer valuations for their data rights as well as consumer's awareness of privacy and perceived control over their personal data. Empiri-

cal research shows post-GDPR reductions in data collection and use that suggest objective improvements in consumer privacy. Structural modeling suggests consumer harm from the GDPR's adverse impact on innovative product development. Theory evidence suggests varying consequences of certain elements of the GDPR for both firms and consumers.

The economics literature also illuminates the consequences of the GDPR's design decisions. The literature documents important spillovers of the GDPR outside of the EU. In particular, research shows that foreign firms that serve EU consumers sometimes exhibit greater compliance than EU firms. This may reflect the GDPR's penalty design: foreign firms that fall under the GDPR's extraterritoriality component may be especially leery of GDPR fines that are based on global revenue rather than EU revenue alone. Research also shows indirect spillovers like global firms implementing their compliance efforts worldwide, so that non-EU consumers benefit. Though the GDPR intended to harmonize regulation within the EU, several scholars document differences in regulatory impact by the perceived strictness of EU country-level regulators.

This review is far from the last word on the GDPR, as the literature and the practical application of the regulation are both still evolving. I focus on the economic literature and the empirical economic literature in particular. However, the study of the GDPR is inherently interdisciplinary, so I occasionally draw on research from law and computer science. This review was commissioned for the NBER Privacy Tutorial in October 2022. As such, my emphasis on research challenges and future research opportunities in part stems from that tutorial's doctoral student audience. Nonetheless, I think that this emphasis is helpful for understanding the literature and the shape it has taken so far. For future research, I indicate more privacy-related changes—whether through regulation or platform policies—that provide possible event studies for empiricists. I also suggest that economists should study privacy-enhancing technologies that are beginning to be commercialized, as these technologies improve the trade-off between privacy and economic uses of data.

This review builds on previous review articles on the economics of privacy and complements other work by great scholars in this volume. For instance, Acquisti, Taylor, and Wagman (2016) provide a general introduction to the economics of privacy. In this volume, the chapter by Miller (2024) on health information privacy describes important antecedents to GDPR research that often exploit changes in health privacy regulation. Carrière-Swallow and Haksar (2019) and the World Bank (2021) examine data policy from an economic perspective. Goldfarb and Tucker (2012) discuss the economics of privacy and innovation. Notably, Prasad and Perez (2020) provide an early review of the economic literature on the GDPR.

The rest of this guide is organized as follows. Section 4.2 provides a background on the GDPR. Section 4.3 discusses key challenges that the GDPR

poses for empirical research. Section 4.4 reviews the economic literature to date on the GDPR. Section 4.5 highlights some avenues for future research on the economics of privacy regulation. Section 4.6 concludes.

4.2 GDPR Background

The GDPR is a lengthy and multifaceted regulation, which opens many avenues for economic research. In this section, I share background on the regulation *as written* for economists. The GDPR contains 99 articles and is supported by an additional 173 recitals. Jones and Kaminski (2020) provide a helpful background for those who are more familiar with the American legal context. Jones and Kaminski point out that the GDPR is situated within a broader legal context that includes the EU Charter, complementary EU and national privacy regulations, EU privacy regulator guidance, EU judicial rulings, and the EU's 1995 Data Protection Directive that preceded the GDPR.

I begin by laying out the regulation's essential features. The GDPR takes a broad approach to data protection regulation by defining personal data as all data relating to a person (Article 4(1)). This extends beyond personally identifiable information like a name or address to include pseudonymous identifiers and online identifiers. For brevity, I refer to personal data as simply *data* below. The GDPR refers to the "processing" of data which includes data collection, storage, use, analysis, sharing, and more (Article 4(2)). The GDPR further distinguishes what it refers to as "special category data" as being particularly privacy-sensitive. This includes data on health, genetics, sexual orientation, political opinions, religious beliefs, and more (Article 9(1)). Though this review focuses on firms, the GDPR covers all individuals and institutions (e.g., governments and non-profit organizations) that process personal data.[2]

The GDPR establishes six data rights for EU residents (Articles 12–23). Under this regulation, residents gain the rights to access and correct data that a firm has about them. Residents gain the right to delete their data, which is often referred to as the "right to be forgotten." Residents even receive the right to port their data to another firm. Residents gain the right to object to data processing and even the right to object to decisions made on the basis of automated processing.

The GDPR imposes a number of responsibilities on firms (Articles 24–43). Firms have to fulfill the above rights-related responsibilities in a timely manner. Firms need to audit their data processing activities—also known as a "Data Protection Impact Assessment." Firms need to minimize their data

2. The GDPR distinguishes between data controllers and data processors (Article 4(7–8)). This distinction refers to cases where, e.g., firm X delegates data processing to firm Y, but firm X retains decision rights regarding the data processing. In this example, firm X is the data controller and firm Y is the data processor.

processing activities—i.e., data protection by default—which is also a key principle of the GDPR (Article 5(1c)). Firms must encrypt and pseudonymize the data they process—i.e., data protection by design. In the event of a data breach, firms must notify the regulator and affected consumers within 72 hours. Finally, firms should designate a data protection officer—either an employee or an external consultant—to oversee their data protection-related activities.

Though consent sometimes plays an outsized role in discussions about the GDPR (Jones and Kaminski 2020), consent is only one of the GDPR's six legal bases for processing data (Article 6(1)). These legal bases are consent, contractual obligation, legitimate interest, legal obligation, vital interest of an individual, and public interest. For most firms, the first three bases are most relevant. As an example, an ecommerce web site could use contractual obligation as a legal basis for processing a consumer's name and address information for the purpose of shipping products to the consumer. Legitimate interest is the most flexible of the legal bases, but it is not a *carte blanche* as it should not override an individual's right to privacy (ICO 2021). Legitimate interest carries additional duties like carrying out and documenting a "legitimate interest assessment" that weighs the firm's specific interest against consumers' privacy interest (ICO 2021). Regardless of the legal basis, the firm should provide information to the consumer including the purpose(s) of data processing, the relevant legal basis(es), the contact information of the data protection officer (where applicable), and the identities of all third-party data recipients (Article 13). Note that special category data has additional restrictions (Article 11) as does child's consent (Article 7).

The GDPR sets a high standard for consent (Article 7). Consent should be an unambiguous, affirmative act like ticking a box on a web site: preticked boxes or inactivity do not indicate valid consent (Recital 32). Consumers must be able to withdraw consent at any time, and just as easily as they provided consent. In obtaining consent, firms must inform consumers using plain language. Consent should be granular to the purpose(s) of processing (Recital 32). As mentioned above, this includes listing all third-party data recipients. Consent should be freely given in that the firm should not condition its consumer offerings on consent when these do not require data processing. Finally, firms must be able to show a record of the consumer's consent.

The GDPR also covers data transfer outside of the European Economic Area (i.e., EU plus Iceland, Liechtenstein, and Norway). Article 45 permits the transfer to countries that have adequate data protection, which encourages foreign countries to adopt GDPR-like regulation. As of now, the European Commission deems 14 countries as adequate, including: Argentina, Canada, Israel, Japan, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay. Articles 45 to 50 lay out alternative data transfer arrangements including foreign firms' adherence to standard contractual

clauses adopted by the European Commission. Data transfers to the US remain a thorny issue, however.[3] The 2016 "EU-US Privacy Shield" permitted data transfers to certified firms but was invalidated by the Court of Justice of the European Union in 2020. In 2022, the European Commission and the US agreed in principle to a new data-transfer arrangement, but this is still being finalized. Despite this, Meta received the largest ever GDPR fine of €1.2 billion in May 2023 for processing EU user data in the US. For the same reason, four EU regulators have ruled that Google's popular web site analytics product (Google Analytics) is illegal.

The GDPR charges Data Protection Authorities (DPAs) in all EU countries with enforcing the regulation (Articles 51–59). DPAs are charged with regulating data processing by firms that are located in their country; that substantially affects their country's residents; or for which they have received a complaint by a resident or organization in their country (Articles 4(22), 57). Though the GDPR was intended to harmonize EU-wide regulation, regulators vary in resources by country (EDPB 2020). For multinational firms, the GDPR's "one-stop shop mechanism" allows firms to select a country as their lead regulator by locating their headquarters in that country (Article 56). The lead regulator mechanism simplifies the firm's dealings with EU regulators, though firms may therefore prefer to locate their headquarters in countries which they believe have weaker DPAs. Nevertheless, other EU DPAs retain considerable rights in multi-national cases (Article 60).[4] The GDPR also establishes an EU-wide European Data Protection Board consisting of the European Data Protection Supervisor and the head of each country's DPA (Article 68). The board issues guidelines, promotes cooperation between DPAs, issues opinions on draft DPA decisions, and resolves disputes between DPAs (Articles 65, 70).

The GDPR stipulates that firms can be fined up to the greater of €20 million or 4 percent of their global annual revenue (Article 83(5)). For lesser infractions, the maximum fines are halved (Article 83(4)). Enforcementtracker.com maintains a list of GDPR fines that are made public.[5] As of September 2022, this site lists 1,279 fines totaling €2 billion and averaging €1.6 million per fine. The majority of these fines are €10,000 or less. The largest seven fines have all been issued to big technology firms: Amazon (the single largest fine until 2022), Meta (3 fines), and Alphabet/Google (3 fines). The countries that have issued the most fines are Spain (496), Italy (181), and Germany

3. Using OECD data from 1995 to 2018, Ferracane et al. (2023) show that the EU adequacy is associated with a 6–14 percent increase in digital trade. This finding is driven by the EU granting adequacy to the US in 2000 and 2016.

4. In practice, impatient regulators have sidestepped the one-stop mechanism by enforcing their national privacy laws. For instance, the French DPA fined both Google and Meta despite those firms having their headquarters in Ireland.

5. Presthus and Sønslien (2021) provide an analysis of the first two years of GDPR fines.

(115). The total value of fines are highest for Luxembourg (€746 million), Ireland (€649 million), then France (€272 million). DPAs can instead handle cases by warning firms or requiring compliance plans, but these instances are usually not documented publicly. Despite this, Koutroumpis, Ravasan, and Tarannum (2022) obtain data on thousands of the British DPA's regulatory actions and show that it used fines sparingly. Beyond administrative fines, the GDPR also includes a private right of action, whereby consumers can seek compensation for privacy-related damage suffered through their country's courts (Article 82).

In sum, the GDPR is a multi-faceted regulation that increases the legal risk and cost associated with data processing. In later sections, we will discuss still more features of the GDPR for researchers to consider. As we will see in Section 4.3.2, the GDPR is further complicated by the sometimes substantial gap between the regulation as written and the reality on the ground.

4.3 Research Challenges

The GDPR represents a tremendous opportunity for economists to study privacy regulation and its impact. Nevertheless, the GDPR poses several challenges for research. Below, I focus on three key challenges and describe solutions devised from the literature.

Most economists study the GDPR as an event study. I begin by recalling a leading approach for analyzing event studies: difference-in-differences (see, e.g., Cameron and Trivedi 2005). Difference-in-differences combines two comparisons. First, we compare a treatment group that is subject to the policy with a control group that is not. These groups should satisfy the stable unit treatment value assumption (SUTVA), meaning that the GDPR does not affect the control group. Second, we compare outcomes before and after the policy. As the name suggests, the difference-in-differences approach estimates the policy's impact by subtracting the before-after means comparison in the control group from that of the treatment group. The identifying assumption is that the treatment and control groups' outcome variable would follow parallel trends after the policy, but for the policy's impact.

The GDPR poses several problems for this analysis framework. Section 4.3.1 discusses the potential challenge of finding a suitable control group that satisfies both SUTVA and the parallel trends assumption. Section 4.3.2 notes that both firm compliance and regulatory enforcement were variable under the GDPR. This poses a problem for generalizing from the real-world estimated impact of the GDPR—or lack thereof—to the regulation as written. Finally, Section 4.3.3 notes the GDPR's confounding impact on data observability. By construction, the GDPR creates a missing-data problem whereby observed individual-level data are selected and the corresponding aggregate statistics are incomplete.

4.3.1 Lack of a Suitable Control Group

Most economists study the GDPR as an event study. Event studies should include (1) a suitable control group, and (2) a clear start date. These criteria are often challenging to address satisfactorily. In the case of the GDPR, both criteria pose problems for research, though the first is unusually challenging.

The GDPR's scale and global scope can make a suitable control group difficult to find in many cases. First, the GDPR's large scale makes it appealing to study, but limits the set of suitable control countries. The GDPR covers 28 EU countries and another 3 European Economic Area countries. To put the problem starkly, a substantial idiosyncratic economic shock to the EU after May 2018 would bias many economic studies. Second, the GDPR has substantial spillovers outside of Europe because the regulation's scope includes not only EU firms but also non-EU firms that target EU residents. For instance, a Canadian ecommerce site that offers shipping to customers in the EU is also subject to the regulation. Third, the GDPR may have indirect spillovers outside of the EU as well. International firms may choose to roll out their GDPR compliance efforts globally due to cost efficiencies in treating their customers and data uniformly. Furthermore, the GDPR raised the attention paid to privacy worldwide and—to some extent—raised global commercial compliance standards to the EU's high standard. Bradford (2020) refers to such phenomena that in effect export EU policy globally as the "Brussels Effect."

GDPR researchers need to also reflect on the appropriate timing to use. The GDPR has two main start dates to consider: its passage in April 2016 and its enforcement deadline in May 2018. The GDPR affects all EU countries simultaneously, unlike past research that benefited from variation in the timing of privacy regulation (e.g., Miller and Tucker 2009). Most studies focus on the latter enforcement date, but some consider both. For instance, firms may have incurred compliance costs before and after the enforcement deadline. If consumer-facing compliance efforts come online after the deadline, the GDPR's effect on revenue may manifest after the deadline. In some cases, anticipatory compliance may attenuate GDPR impact estimates. In other cases, firms may have delayed compliance until the enforcement deadline or even later (see, e.g., Demirer et al. 2023). In sum, researchers should evaluate the relevant timing in their setting as a function of its underlying economics and its institutional realities.

Many GDPR papers use difference-in-differences as their identification strategy and most use non-EU countries (or units therein) as a control. For instance, Aridor, Che, and Salz (2023) examine data from travel web sites and argue that these have "separate, country-specific, versions of their web sites," so that the sites' requirement to comply with the GDPR is clear. Moreover, Aridor, Che, and Salz use non-EU travel web sites in Northern Hemisphere countries as a control group, so that these sites are both

exempt from the GDPR and should have similar seasonal demand for travel. Similarly, Jia, Jin, and Wagman (2021) examine the GDPR's effect on EU technology venture investment using the US as their primary control group, and a combination of remaining countries as a secondary control group for robustness. In this case, the free flow of capital between countries may create spillovers to the control group. Jia, Jin, and Wagman (2021) therefore argue that they would overestimate (underestimate) the GDPR's impact if the GDPR decreases (increases) investment outside the EU. Johnson, Shriver, and Goldberg (2023b) instead use a "panel differences" approach in their study of web site traffic. This approach is essentially a difference-in-differences strategy that uses the same web sites in the previous year as a control group. By construction, this approach rules out GDPR spillovers and accounts for firm-specific seasonal differences, but requires parallel trends across years.

Several GDPR papers instead apply identification strategies that do not depend on a control group. Some authors argue that a sudden change in an outcome after the GDPR can be attributed to the regulation. For web sites' use of technology vendors, Peukert et al. (2022) use essentially an interrupted time-series design, whereas Johnson, Shriver, and Goldberg (2023b) use before-after differences. An interrupted time-series design (see, e.g., McDowall, McCleary, and Bartos 2019) assumes that the counterfactual outcome continues its baseline (e.g., linear) time trend, as established pre-GDPR. This approach attributes post-GDPR changes in both the outcome's level and trend to the regulation. Lacking pre-trend data, Johnson, Shriver, and Goldberg instead compare outcome levels after the GDPR with a pre-GDPR baseline. The authors argue that unobserved time trends confound their estimates, so that short-run differences best reflect the causal impact of the GDPR. Other authors exploit variation in the degree of exposure to the GDPR. For example, Yuan and Li (2019) compare the financial performance of EU hospitals by whether the hospitals are more or less data-dependent. Chen, Frey, and Presidente (2022) use variation in industry-level exposure to the EU using trade data to calculate the share of output sold to EU countries. Finally, Godinho de Matos and Adjerid (2022) use a GDPR-related marketing field experiment in order to avoid an event-study style analysis entirely.

4.3.2 Variable Firm Compliance and Regulatory Enforcement

The European Commission (2019) status report on the GDPR acknowledges that the regulation fell short of its potential due to a lack of enforcement. The GDPR literature has shown variation in compliance efforts by industry, by country, by compliance requirement, by firm size, and over time. As a result, economists must critically examine the lessons that can be drawn from the GDPR in the context of variable compliance and enforcement.

In general, regulatory outcomes can be thought of as the product of

strategic interactions between firms and regulators. Compliance is costly to firms, and small and medium-sized firms in particular may lack the resources to comply. In surveys, a majority of firms reported that they were not compliant with the GDPR at the enforcement deadline and that their compliance efforts were a work in progress (TrustArc 2018). At the same time, enforcement is costly to the regulator, and country-level DPAs vary in resources (EDPB 2020). GDPR fines to date also show that country DPAs vary in their strictness and tactics. We can therefore expect a gap between the regulation as written and the reality on the ground.

GDPR enforcement and compliance are especially challenging for a number of reasons. Unlike vehicle emissions standards, for instance, GDPR compliance is multidimensional and compliance outcomes can be difficult to observe.[6] Moreover, the GDPR is complex and enumerates many compliance options (e.g., bases for data processing), which make some compliance elements subjective. In this sense, compliance can be described as a "cookbook" with more flexibility and options than a single "checklist" for all firms. Relatedly, compliance norms may arise gradually and evolve over time (see, e.g., Hils, Woods, and Böhme 2020; Lefrere et al. 2022).[7] Since personal data is pervasive, the GDPR can be considered to be a "law of the whole economy." Regulators must therefore set enforcement priorities.[8] Finally, privacy regulators, unlike antitrust regulators for example, lack enforcement experience and established precedent to draw upon.

The compliance literature emphasizes that regulators can ensure compliance using a combination of fines and the probability of receiving a fine (see, e.g., Polinsky and Shavell 2000). The above points may reduce the probability of receiving a fine. Perhaps to offset this, the maximum fines under the GDPR are large.

Nevertheless, the cost of strict GDPR compliance may exceed even the maximum fines in some industries. Web sites and the technology vendors that support them provide plausible examples. Many web sites rely on advertising to generate revenue and some research shows that ad prices double when ad impressions contain a cross-site cookie identifier for users (Johnson, Shriver, and Du 2020; Ravichandran and Korula 2019). Web sites may therefore resist complying on dimensions that jeopardize their revenue model.[9]

6. Of course, the observability of compliance outcomes also poses a problem for empirical research. In practice, data breaches are therefore useful entry points for regulators to select and investigate enforcement targets.

7. This poses a challenge if we treat the GDPR as an event study.

8. These priorities should flow from the regulators' democratic mandate, which may in turn constrain the regulators' enforcement targets. For instance, regulators may hesitate to crack down on domestic firms or firms that provide public goods like content creators.

9. Beyond limiting technology vendors, web site compliance strategies include notifying users of the presence of browser cookies, offering the user some consent choice, discontinuing the use of third-party cookies (at least prior to obtaining consent), and/or blocking EU users (Johnson, Shriver, and Goldberg 2023b; Lefrere et al. 2022; Skiera et al. 2022).

However, regulators are concerned about the privacy harm of this industry's use of online identifiers and have repeatedly criticized this industry's level of compliance (AP 2019; CNIL 2019; DPC 2020; ICO 2019). Regulators complain that the industry loads vendor content and cookies prior to obtaining consent and that the industry's consent practices fall short of the GDPR's opt-in standard. Nevertheless, regulators did not fine this industry until the end of 2020. Several economic studies find that web sites cut the number of vendors and/or third-party cookies in May 2018, but also find that these returned to pre-GDPR levels within a few months (Johnson, Shriver, and Goldberg 2023b; Lefrere et al. 2022; Lukic, Miller, and Skiera 2023; Peukert et al. 2022). These papers wrestle with what policy lessons can be drawn as a result, and most focus on the short-run changes. For instance, Johnson, Shriver, and Goldberg argue that the post-GDPR rebound can not be attributed to the GDPR alone due to some combination of low compliance, shifting compliance norms, lack of enforcement, and the industry's exogenous growth.

Despite these prominent cases of low compliance in data-dependent industries, the GDPR did meaningfully change the compliance and enforcement environment within the EU. The GDPR and its large fines in particular caught the attention of European firms (Martin et al. 2019). Using data from Microsoft's cloud computing platform, Demirer et al. (2023) show that the GDPR had its intended impact of reducing data processing. Even US firms increased their attention to data privacy—as evidenced by mentions in publicly listed firms' annual reports—particularly for those firms with a presence in the EU (Boroomand, Leiponen, and Vasudeva 2022; Maex 2022). Before the GDPR, EU enforcement of some privacy laws on the books was low, so non-compliance was a viable strategy for firms (Martin et al. 2019). I emphasize this, because it again shows that economists should not assume that firms comply with the letter of the law where privacy regulation is concerned. However, the GDPR increased political pressure on data protection authorities to use their new powers to increase enforcement and thereby shifted firm beliefs about the probability of penalties (Martin et al. 2019).

Variable compliance and enforcement can obfuscate the lessons that can be drawn from empirical GDPR research. What is clear is that scholars should not assume uncritically that the GDPR *as written* actually happens *in practice*. Instead, scholars should investigate the reality of the GDPR on the ground. In particular, scholars must grapple with how firms comply with the GDPR in their setting. Cost-benefit analysis can illuminate the economics of a firm's compliance decisions. Scholars should also examine regulators' public statements and regulatory actions to understand the enforcement priorities in the setting of interest. On the consumer side, scholars should not assume, for instance, that consumers make use of their new data rights under the GDPR in economically meaningful quantities (DataGrail 2020; Presthus and Sørum 2021).

The literature grapples with these issues in several ways. Researchers look for domains where compliance activities are stronger or at least quantifiable. Finally, scholars acknowledge the variable nature of both compliance and regulation, and the difficulties this presents for generalizing from the short- and long-run impact of the GDPR.

4.3.3 GDPR's Impact on Data Observability

The GDPR limits personal data processing, which creates problems for empirical researchers. The GDPR may increase the cost of accessing data for researchers or prevent data access altogether (Greene et al. 2019).[10] When consent is the legal basis for collecting data, this introduces self-selection into the data. Consent-based selection is more challenging than data missingness alone, because an unknown quantity of individual data will be altogether absent from the database. These data issues pose a challenge for many applied microeconometricians who use individual-level data to deliver economic insight.

Researchers have navigated this problem with a variety of approaches. To begin, economists can still use non-personal data—like accounting or macroeconomic data—which the GDPR should not affect (Chen, Frey, and Presidente 2022; Jia, Jin, and Wagman 2021). Alternately, Zhao, Yildirim, and Chintagunta (2021) use individual data from a panel of consenting consumers to study the GDPR's impact on online search behavior. Though such panels are themselves selected—e.g., presumably panelists have a lower preference for privacy—the panels at least are complete.

Other researchers embrace the GDPR's impact on consent-based missingness as interesting in its own right. For instance, Aridor, Che, and Salz (2023) investigate the impact of the GDPR on online user data. Aridor, Che, and Salz obtain data from a marketing intermediary that sends offers to users on a large collection of online travel agency web sites around the world. These travel web sites share user-level, travel-related search data with the intermediary, which then makes targeted offers to users based on the user's predicted purchase probability. After the GDPR, the intermediary receives less data, which Aridor, Che, and Salz attribute to a segment of users who refuse consent for data sharing. Aridor, Che, and Salz show that the remaining consenting users are favorably selected in that they have longer search histories. Aridor, Che, and Salz attribute this to two explanations. First, privacy-sensitive users obfuscate their browsing histories (e.g., by clearing cookies), so that they appear as multiple user identifiers with short browsing histories prior to the GDPR. Second, user willingness to consent may be correlated with user's travel web site activity, for instance, because users who like the site may be more willing to both browse the site and provide

10. Relatedly, Yom-Tov and Ofran (2022) document a shift in clinical trials out of the EU and toward countries with weaker data protections after the implementation of the GDPR.

consent. After the GDPR, the intermediary can no longer see or sell to non-consenting users, which hurts its revenue. Aridor, Che, and Salz point out an interesting silver lining: as the consenting user data is longer and higher quality, the intermediary may have an easier time predicting user behavior and making successful offers to consenting users.

Goldberg, Johnson, and Shriver (2024) work with similar data from a large number of web sites globally from Adobe Analytics. Web sites use Adobe Analytics to measure outcomes like site visits, page views, and ecommerce revenue. Goldberg, Johnson, and Shriver show that these outcomes—as recorded by Adobe—fell by about 12 percent after the GDPR. As in Aridor, Che, and Salz (2023), Adobe may see less data because of non-consenting users after the GDPR. However, Adobe would also record less site data if the GDPR actually hurt the real outcomes for these sites. Goldberg, Johnson, and Shriver grapple with this identification problem by constructing bounds on the relative contributions of the consent and real effects of the GDPR to the drop in recorded site outcomes.

4.4 Literature Review

In this section, I review the economics literature on the GDPR. Section 4.4.1 examines the GDPR from the perspective of consumers. Section 4.4.2 turns to the GDPR's impact on firms. This literature is larger, so we first consider the GDPR's impact on firms' economic performance measures before diving deeper into the GDPR's impact on competition, innovation, the web, and marketing. Section 4.4.3 discusses the lessons learned about the GDPR's constituent parts and how they work in practice.

At the outset, I point out that the GDPR literature is still maturing. Five years after the enforcement deadline, a minority of economics papers have appeared in print. As such, many of the papers I discuss below are working papers, and will therefore continue to evolve in the future.

4.4.1 Impact on Consumers

The economics literature has explored the GDPR's consequences for consumers. However, privacy economists generally find that consumer privacy preferences are difficult to ascertain (see, e.g., Athey, Catalini, and Tucker 2017). One approach is to survey consumers and ideally to do so prior to the GDPR for a baseline comparison. For instance, Presthus and Sørum (2021) surveyed a cross-section of Norwegian university students annually from 2018 to 2020. However, this evidence failed to show the GDPR's expected improvements: the surveys show no increase in general awareness of privacy or perceived control over personal data.

Sobolewski and Paliński (2017) implement a stated preference discrete choice experiment prior to the GDPR. By surveying Polish university students, Sobolewski and Paliński obtain willingness-to-pay estimates for four

individual data rights under the GDPR.[11] This study reveals a similar average willingness to pay for the right to be forgotten, the right to object to profiling, and the GDPR's extended information obligations. However, the willingness to pay for data portability was negative and statistically insignificant. The authors provide an estimate of the welfare benefit of the GDPR by summing consumer willingness to pay for these four rights. Sobolewski and Paliński thus estimate that the GDPR provides a value of €6.50 per person per month.

Other economic papers speak to the consumer welfare impact of the GDPR or show objective improvements in consumer privacy. Janßen et al. (2022) argue that the GDPR hurts consumer surplus by reducing innovation in consumer products. To show this, they use a structural demand model to examine the consumer consequences of the GDPR to the app market. In theoretical work, Ke and Sudhir (2022) and Wang, Xu, and Zhang (2022) investigate the welfare consequences of the GDPR for both firms and consumers.

The GDPR should improve consumer privacy by improving data security and reducing data processing. These objective improvements in privacy may be difficult to quantify across firms and at large scale. Nevertheless, Demirer et al. (2023) show that EU firms reduce both their data storage and computation activity on Microsoft's cloud service after the GDPR. Moreover, these effects grew over time such that, in the GDPR's second year, data storage in the EU fell by 26 percent and "compute" (i.e., core-hours of cloud computation) fell by 15 percent relative to the US. As we will see in Section 4.4.2.3, several researchers find that web sites reduced data sharing after the GDPR, though these privacy improvements were short-lived. A small segment of consumers appears to be exercising their consent privilege by opting out of data collection online (Aridor, Che, and Salz 2023; Goldberg, Johnson, and Shriver 2024).

By drawing attention to data protection, the GDPR may have influenced how firms measure and report their data-protection activities. For example, the GDPR's data-breach notification requirement should have reduced the number of data breaches.[12] Indeed, GDPR research finds increased firm demand for cybersecurity-related skills for both employees (Koutroumpis, Ravasan, and Tarannum 2022) and board members (Klein, Manini, and Shi 2022). Nevertheless, the impact on data breaches would be challenging to evaluate empirically, as the notification requirement should also increase the number of breaches that firms both notice and report. Similarly, the GDPR's encryption requirement should reduce the privacy risk from data breaches. Despite this, Miller and Tucker (2011) show that (public) data-breach inci-

11. See Presthus and Sørum (2019) for related survey evidence.

12. Romanosky, Telang, and Acquisti (2011) show that state-level breach disclosure laws in the US reduced identity theft caused by data breaches by 6.1 percent.

dents actually increased after the American medical sector adopted data encryption.

4.4.2 Impact on Firms

Several scholars document that the GDPR harmed a variety of firms' outcomes including: profits, revenue, investment, market exit, and entry. I first discuss the evidence for firm performance before turning to the GDPR's impact on competition (Section 4.4.2.1), innovation (Section 4.4.2.2), the web (Section 4.4.2.3), and marketing (Section 4.4.2.4).

Multiple studies examine accounting data and attribute a reduction in firms' profit and/or revenue to the GDPR. For instance, Koski and Valmari (2020) examine nearly 267,000 EU and US firms from 2014 to 2018. The authors use difference-in-differences with US firms as a control and 2018 as the treatment year. Koski and Valmari find a statistically insignificant effect on profit margins in their full sample, but a statistically significant −1.9 percent reduction in profit margins among data-intensive sectors in the EU (i.e., information and communications, banking, and other financial services). Chen, Frey, and Presidente (2022) examine almost 700,000 firms across 61 countries and 34 industries. By comparing firms by their sector's revenue exposure to the EU, they attribute a decline in profits and a reduction in sales by the firm's degree of GDPR exposure. Yuan and Li (2019) use difference-in-differences to compare the financial performance of hospitals in the EU by the importance of information, communication, and telecommunication to their business. They find lower operating revenue (scaled by total assets) for more data-intensive hospitals during the GDPR's transition period from passage to enforcement (2016–2018).

Survey evidence finds that firms incurred and continue to incur significant costs in order to comply with the GDPR. The International Association of Privacy Professionals (IAPP 2017) estimated that Fortune 500 global firms would spend $7.8 billion on compliance.[13] DataGrail (2020) finds that 74 percent of small- and mid-sized organizations spent more than $100,000 on compliance. Five years after the GDPR, IAPP (2023) found that the average European privacy budget was €1.1 million, the annual base salary for EU privacy professionals was €98,893, and the number of privacy technology vendors (368) had grown almost eightfold since 2017.

Recent research on the GDPR illuminates firm's compliance cost. Demirer et al. (2023) estimate that the GDPR was equivalent to a 20 percent tax on the cost of data storage. Koutroumpis, Ravasan, and Tarannum (2022) examine the impact of the GDPR in the United Kingdom by comparing sectors by their share of regulatory enforcement cases. Koutroumpis, Ravasan, and Tarannum find that the demand for cyber-related labor increases

13. The IAPP figure extrapolates from survey evidence in the IAPP and Ernst and Young (2017) report.

by 52 percent in more scrutinized sectors. Accounting research by Maex (2022) finds that the GDPR improved proxies of firms' internal information quality, which indirectly improved firms' operational efficiency (i.e., the efficiency of deploying inputs to generate sales). Still, Maex finds that the regulatory burden of the GDPR exceeded this benefit such that firms' operational efficiency fell on net.

Jia, Jin, and Wagman (2021) show that the GDPR reduced investment for EU technology ventures.[14] Using the difference-in-differences strategy described in Section 4.3.1, they find that the number of EU venture deals fell by 26 percent after the GDPR enforcement deadline. Jia, Jin, and Wagman also document that the most affected firms are: early-stage ventures, data-related ventures, business-to-consumer (versus business-to-business) ventures, and ventures in the healthcare and finance industries. These patterns are consistent with a GDPR effect as we may expect the GDPR to have greater effects for ventures that use data, especially consumer data, health data (i.e., special category data), and in heavily regulated industries. Jia, Jin, and Wagman (2020) build on this research by examining differences between EU and foreign investors. Jia, Jin, and Wagman find an increase in investor home bias post-enforcement: that is, foreign investment in EU technology ventures falls by more than local investment. Jia, Jin, and Wagman argue that this is consistent with foreign investors having greater uncertainty about the financial consequences of the GDPR.

Several papers show that the GDPR harms economic dynamism. Koutroumpis, Ravasan, and Tarannum (2022) find that sectors that receive greater scrutiny from the British data protection authority exhibit a 12 percent relative reduction in market entry and a 13 percent relative increase in market exit. Janßen et al. (2022) show a larger impact on both entry and exit for mobile apps on the Android platform after the enforcement deadline. Janßen et al. examine app data from the Google Play Store using a before-after comparison and supplement their findings by surveying German app developers. Relatedly, Kircher and Foerderer (2021) document a small increase in closures of US app startups post-GDPR as well as a small reduction in venture capital transactions for US app startups relative to US enterprise software startups.

4.4.2.1 Impact on Competition

Several observers warned of a potential trade-off between privacy regulation and competition (e.g., Brill 2011; Goldfarb and Tucker 2012; Phillips 2019). Indeed, the GDPR literature repeatedly confirms this hypothesis. In general, regulation can impact competition if firms experience returns to scale in compliance. For privacy regulation, consent requirements may also

14. Note that Lambrecht (2017) also finds a reduction in venture investment in certain sectors after the EU's e-Privacy Directive.

favor large established firms if consumers are more likely to provide consent to such firms (Campbell, Goldfarb, and Tucker 2015) or to consent to smaller lists of third-party data recipients. Gal and Aviv (2020) and Geradin, Karanikioti, and Katsifis (2020) discuss several potential channels through which the GDPR may affect competition.

Many researchers find that the GDPR disproportionately hurts smaller firms (e.g., Bessen et al. 2020; Chen, Frey, and Presidente 2022; Jia, Jin, and Wagman 2020; Koski and Valmari 2020; Maex 2022; Zhao, Yildirim, and Chintagunta 2021). Johnson, Shriver, and Goldberg (2023b) and Peukert et al. (2022) focus on the privacy-competition trade-off question. Both find that the market for technology vendors that serve web sites became more concentrated right after the GDPR's enforcement deadline. This provides evidence for a new anticompetitive mechanism: when privacy regulation restricts business-to-business data transfers, firms may prefer to retain their larger vendors. Contrary to Campbell, Goldfarb, and Tucker (2015), Johnson, Shriver, and Goldberg find no evidence that consent drives this increased concentration. However, the simple explanation is that sites rarely make the list of third-party data firms prominent when requesting consent. On the other hand, Goldberg, Johnson, and Shriver (2024) provide indirect evidence that smaller web sites obtain lower consent rates, which would limit the profitable use of data by these smaller firms.

4.4.2.2 Impact on Innovation

Goldfarb and Tucker (2012) argue that a trade-off exists between privacy and innovation. They support their argument with numerous studies focusing on the online-advertising and healthcare sectors. Supported by interviews of startups and lawyers in 2018, Martin et al. (2019) point out that the GDPR can both support and suppress innovation. For instance, the interviews suggested that the GDPR spurred privacy-related innovation as well as increased demand for "regulation-exploiting innovation"—that is, diffusing compliance management software and encryption capabilities. However, Martin et al. also document claims that the GDPR led startups to abandon products, discouraged entrepreneurs, and limited innovators' access to input data (e.g., for artificial intelligence applications).

The empirical evidence for the GDPR's impact on innovation is somewhat mixed. As we have seen at the top of Section 4.4.2, the GDPR reduced technology venture funding and hurt market dynamism. Bessen et al. (2020) survey artificial intelligence startups. Bessen et al. find that GDPR imposes costs on these firms in terms of adding new position(s), reallocating resources, and deleting data. Despite the GDPR's requirements on firms, Bessen et al. find that the use of various data protection methods does not differ by whether the firm has customers in Europe. Venkatesan, Arunachalam, and Pedada (2022) provide evidence that the GDPR increased the return on assets from acquisitions of AI technology companies—particularly for acquisitions

related to customer experience and cybersecurity. Perhaps counter to expectations, Chen, Frey, and Presidente (2022) find that patenting among IT service firms increased 30 percent, though this figure is imprecisely estimated.

Blind, Niebel, and Rammer (2023) examine innovation using an annual survey of German firms from 2011 to 2020. Examining the 2018 survey, Blind, Niebel, and Rammer note that 35.0 percent of firms report that data protection regulation hampers their innovation activities, whereas only 4.7 percent report the opposite. Perhaps in contrast with other GDPR research, the share of firms that report either an innovation-facilitating or innovation-complicating role seems to increase with firm size. Blind, Niebel, and Rammer also find that the GDPR shifts innovation to become more incremental and less radical in nature.

4.4.2.3 Impact on the Web

The web uses personal data to personalize web sites, content, and advertising. At a basic level, the Internet requires IP addresses—which the GDPR considers to be personal data—to function. For researchers, the Internet and web sites therefore provide an opportunity to study an industry that is both targeted by the regulation and provides data for empirical study.

Researchers have examined the GDPR's impact on site traffic, site vendor use, site content creation, Internet infrastructure, and online search. Several researchers find that the GDPR reduced sites' use of vendors and/or data sharing using third-party cookies (Johnson, Shriver, and Goldberg 2023b; Lefrere et al. 2022; Lukic, Miller, and Skiera 2023; Peukert et al. 2022). Several computer science researchers concur with these findings (e.g., Libert, Graves, and Nielsen 2018; Urban et al. 2020). Wang, Jiang, and Yang (2023) show that a large publisher saw a modest reductions in ad revenue, though the authors attribute the small effect size to high user-consent rates. Despite these issues, or perhaps due to the rapid post-GDPR bounce-back, Lefrere et al. (2022) find no impact on news and media web sites' production of new content or social sharing of that content. Using data from Adobe Analytics, Goldberg, Johnson, and Shriver (2024) argue that real web site page views and ecommerce revenue from EU users falls by at least about 0.5 percent post-GDPR due to degraded marketing capabilities. Using third-party site-traffic data, Schmitt, Miller, and Skiera (2021) find a larger (5–10 percent) reduction in site visits, Congiu, Sabatino, and Sapi (2022) find an even larger (15 percent) reduction in 2019, but Lefrere et al. find that EU site traffic measures are relatively stable except for a small decline in page views per user.[15] Finally, Zhao, Yildirim, and Chintagunta (2021) examine the brows-

15. These authors assume that their data fully captures real site outcomes (i.e., the ground truth). Nevertheless, it is unclear how their data sources—SimilarWeb (Congiu, Sabatino, and Sapi 2022; Schmitt, Miller, and Skiera 2021) and Alexa web information services (Lefrere et al. 2022)—address traffic from non-consenting users (see Section 4.3.3). In particular, SimilarWeb explains that it somehow models traffic using a variety of data sources, which include

ing behavior of a panel of online users. Zhao, Yildirim, and Chintagunta find that EU users increase their online search intensity after the GDPR relative to their non-EU counterparts.

The GDPR limits international data transfers—particularly to the majority of countries that do not meet the EU's adequacy requirements. As such, we might expect that the GDPR affected data flows between the EU and the rest of the world. Zhuo et al. (2021) investigate this possibility by obtaining data at the Internet's infrastructure level to monitor physical investments in international data flows. However, Zhuo et al. find no GDPR effect in the EU on the Internet's interconnectivity layer. This finding is further notable because it arises despite the reductions—albeit modest—in site traffic and vendor use documented above. Though the authors lack more granular data on the type of data flows, the authors suggest that growth in, for instance, data-heavy video traffic may mask the observed reduction in other web-related data flows. Relatedly, Demirer et al. (2023) find that the GDPR's impact on cloud storage and computing were modest at first but grew over time. This may explain the perhaps contrasting result in Demirer et al. that firms that used cloud-based web services exhibit much greater reductions in both cloud storage and computing.

4.4.2.4 Impact on Marketing

The GDPR was expected to reduce firms' marketing capabilities and thereby limit matching between firms and consumers. In particular, the GDPR's data processing restrictions were expected to hurt personalized marketing channels like email and online display advertising. Consistent with this, Goldberg, Johnson, and Shriver (2024) find larger reductions in recorded EU site traffic originating from email or display ad clicks relative to visits that directly navigate to the web site. Wang, Jiang, and Yang (2023) find that the GDPR degraded online display ad performance including ad click-through and conversion rates. Aridor, Che, and Salz (2023) highlight that the GDPR can limit personalized marketing opportunities, but favorably selected data from consenting users can improve the firm's individual marketing response predictions.

Godinho de Matos and Adjerid (2022) and D'Assergio et al. (2022) examine email permissioning campaigns. Many marketers sought to bring their marketing consent up to the GDPR standard by running a permissioning campaign to (re-)obtain consent. Godinho de Matos and Adjerid run a marketing field experiment with a large European telecommunications firm. This firm sent out a permissioning email in the treatment group, and sent that email after a delay in the control group. Godinho de Matos and Adjerid show that the permissioning campaign succeeded at increasing the share

site analytics data (which must exclude non-consenting users) shared by web sites as well as a panel of browser extension users.

of consumers to which the firm can market. Moreover, Godinho de Matos and Adjerid show that the firm was able to subsequently both increase the marketing messages it sent to treated consumers and increase revenue from these consumers.

D'Assergio et al. (2022) collect and categorize 1,506 different permissioning emails. They find that 29 percent of these emails tried to persuade users (e.g., with discount offers or discussing benefits of data sharing), 35 percent only used an informative approach, and 20 percent combined both approaches. D'Assergio et al. also partner with a European firm to run an email field experiment. The authors find evidence that persuasive tactics can improve opt-in rates and that combining this with informative tactics can further improve opt-in rates. However, the authors find no significant differences in the amount of personal data shared across conditions.

4.4.3 Elements of the GDPR in Practice

One challenge in studying the GDPR is that the regulation contains so many elements. Since these elements were all applied at once, the event-study nature of most GDPR research limits how much can be learned about the GDPR's constituent parts. Nevertheless, unpacking these elements is useful for evaluating the regulation and designing effective privacy regulation. Several researchers have shown patterns that appear to reveal some consequences of the GDPR's design decisions and features of the regulation in practice.

The GDPR intended to harmonize data regulation within the European Union, and this was thought to be a source of efficiencies for firms that serve multiple EU countries (European Commission 2012). However, we have seen that regulators vary in their resources and enforcement strategies. Several authors have found that the size of the GDPR's impact is correlated with firms' beliefs about regulatory strictness specific to data protection at the country level (Goldberg, Johnson, and Shriver 2024; Jia, Jin, and Wagman 2020, 2021; Johnson, Shriver, and Goldberg 2023b). To establish this, these studies use a European Commission (2008) survey of data processors by EU country that asked whether their local data protection regulator was more or less strict than regulators in the rest of the EU. By this metric, the strictest data regulators are Germany and Sweden, and the laxest regulators are Bulgaria and Greece. Though this regulatory strictness measure is dated, it appears to predict the depth of the GDPR's impact.[16]

Other research examines international spillovers from the GDPR. Peukert et al. (2022) highlight the spillovers to non-EU residents using web site data collected from the vantage point of a US user. Non-EU residents see the largest vendor reductions on web sites located in the EU that serve primarily an EU audience. This suggests that EU-focused firms roll their compliance

16. Though country-level strictness is correlated with per capita income, these papers show that the strictness result is robust to including income as a model covariate.

efforts to all their consumers, which benefits their (limited) foreign audience. Non-EU web sites cut their vendors vis-à-vis US users, though by very little for sites that primarily serve a non-EU audience.

Johnson, Shriver, and Goldberg (2023b) instead scan web sites from the perspective of a French user, using a VPN service. They find that—from the perspective of an EU user—foreign sites with a small share of EU users make deeper cuts to their vendors than sites that primarily serve EU users. Johnson, Shriver, and Goldberg attribute this pattern of results to the design of the GDPR fines, which reach 4 percent of a firm's *global* revenue. In particular, the benefit of exploiting user data is relatively small for sites with a small share of EU users, but otherwise equivalent sites would face the same fine. Perhaps due to these differing incentives, Johnson, Shriver, and Goldberg remark that EU firms here do less to protect EU residents than non-EU firms.[17]

Sørum and Presthus (2020) examine the GDPR's data access and portability rights by initiating personal data access requests from 15 firms. They find that almost all these firms responded quickly and provided personal data, though the data provided fell short of the letter of the law (i.e., all eight items regarding data access under Article 15).

Finally, several researchers show that firms that rely more on consumer data and sensitive data exhibit greater harms from the GDPR (e.g., Jia, Jin, and Wagman 2021; Li, Yu, and He 2019). This may oversimplify the picture for certain industries though, as established firms with experience handling sensitive data may instead have lower adjustment costs. Koski and Valmari (2020) discuss this lower adjustment cost as a potential explanation for their findings.

4.5 Future Opportunities for Research

The GDPR is an important and relatively recent regulation. We will undoubtedly see more related research in the future. In the conclusion, I suggest some directions for future research. Below, I suggest two key opportunities for privacy research. Section 4.5.1 enumerates recent and future privacy-related changes to regulation and technology platforms. Section 4.5.2 introduces privacy-enhancing technologies and discusses opportunities for economists to improve these technologies and study their adoption.

4.5.1 More Privacy Regulations and Changes on the Horizon

Though the GDPR received most of the literature's attention in recent years, several other regulations and interventions have since passed or are

17. Note that Lefrere et al. (2022) complement these two studies by scanning 909 news and media publisher web sites from the vantage point of both EU and US users. Lefrere et al. largely confirm the above results using third-party cookies as their dependent variable.

on the horizon. Nevertheless, compliance and enforcement issues (Section 4.3.2) loom large here: the realized privacy results will vary.

First of all, the GDPR remains a worthwhile subject of research. Future research may extend beyond the GDPR's enforcement deadline. Given the GDPR's compliance and enforcement issues, future crackdowns may present opportunities to study the impact of the GDPR. For instance, potential "mini" GDPR events include regulator enforcement deadlines, regulatory actions (see, e.g., Koutroumpis, Ravasan, and Tarannum 2022), major court decisions, voluntary changes in compliance strategies (e.g. self-regulatory changes), and private actions (e.g., noyb 2022).[18] Also, the United Kingdom is considering whether to revisit the GDPR in light of that country's exit from the EU. This may provide opportunities to study the impact of undoing certain elements of the GDPR.

Second, proposed and enacted regulations worldwide provide additional opportunities for research. Many countries have passed, enforced, and/or updated privacy regulation since the GDPR was passed, including: Bahrain, Brazil, Burkina Faso, China, India, Israel, Japan, Kenya, Mauritius, New Zealand, Nigeria, Qatar, Singapore, South Africa, South Korea, Switzerland, Thailand, Turkey, and Uganda. As of early 2023, Greenleaf (2023) counts 162 countries with data privacy laws, which grew by 42 countries since 2017. The EU passed the Digital Services Act and Digital Markets Act in 2022, which contain relevant provisions. For instance, the Digital Services Act largely bans targeted online ads to children under 18. The EU's proposed ePrivacy Regulation will build on the GDPR by establishing particular privacy regulations for electronic communication in the EU. The ePrivacy Regulation will build on its predecessor—the ePrivacy Directive—which Goldfarb and Tucker (2011) and Lambrecht (2017) study. In the US, Congress has considered several privacy laws while nine states have enacted comprehensive privacy laws as of June 2023: California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Virginia, and Utah. For instance, Abis et al. (2022) study the California Consumer Privacy Act and its impact on voice-AI firms. Also, the Federal Trade Commission (FTC) has telegraphed its desire to more aggressively protect consumer privacy with its 2022 Advanced Notice of Proposed Rule-making on "Commercial Surveillance and Data Security."

Third, some large technology firms responded to increased privacy-related regulatory scrutiny by instituting related changes on their platforms. These changes can mitigate non-compliance issues by instituting platform rule changes that, to a greater extent, force firms on their platform to comply.

18. For example, Johnson, Shriver, and Goldberg (2023b) examine the French regulators' enforcement deadline for web sites (April 2021) as well as a self-regulatory update to the web vendor industry's consent mechanism (Fall 2020). These results (in an online appendix) show that these GDPR-like events replicated the authors' key findings: the GDPR simultaneously reduces vendor use and increases vendor market concentration.

For instance, Apple's "App Tracking Transparency" forced apps to request user opt-in consent for what Apple terms "tracking" as of April 2021. Some research examines the resulting consequences for apps and advertisers on Apple's platform (Kesler 2022; Li and Tsai 2022). In response to two alleged violations of the US Children's Online Privacy Protection Act, other researchers examine the impact of Google removing personalized ads from children's games on Android (Kircher and Foerderer 2023) and all forms of personalization for child-directed content on YouTube (Johnson et al. 2023a).

4.5.2 Privacy-Enhancing Technologies

Privacy-enhancing technologies (PETs) offer a potential solution for the tension between privacy and the data economy. The United Kingdom defines PETs as "technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals" (ICO 2022). Examples of PETs include: differential privacy, federated learning, on-device computation, zero-knowledge proof, and secure multi-party computation.

In particular, differential privacy (Dwork 2006) is a controversial, but popular, example of a PET in practice. Roughly speaking, related methods inject noise into data statistics or the data itself in order to satisfy the differential privacy criterion that protects individuals in the data. Blanco-Justicia et al. (2022) and Williams and Bowen (2023) provide both an introduction to, and a critical review of, differential privacy. These authors point out several limitations that limit the broad use of differential privacy and note that many real-world applications choose permissive privacy parameters that effectively sacrifice privacy for utility. Moreover, Komarova and Nekipelov (2020) note that differential privacy creates challenges for inference by transforming data sets.

Economists can contribute to research on PETs. More fundamental research is required on how to design PETs. Economists in particular can help map out the privacy versus value-creation frontier of PETs (e.g., Hotz et al. 2022). For instance, in marketing applications, scholars have proposed methods to optimally transform the data (Li et al. 2022) or generate synthetic data (Anand and Lee 2023; Schneider et al. 2018) to provide privacy guarantees while retaining data utility on certain dimensions. Economists also can study the adoption and consequences of PETs just as they study other innovations like artificial intelligence and cloud computing (e.g., Zolas et al. 2020). PETs too can have competitive consequences, for instance, because smaller quantities of data are more likely to reveal an individual's data. In the case of online advertising, Johnson, Runge, and Seufert (2022) predict significant consequences of applying PETs for both practitioners and researchers.

PETs are now gaining practical use. For instance, the US Census will add

noise to its data before computing its public statistics (i.e., differential privacy) in order to fulfill its legal obligation to not reveal information about individuals in the census. Some have argued that PETs can aid in GDPR compliance efforts (e.g., Cummings and Desai 2018). As well, Google's Privacy Sandbox proposes PETs as alternatives to browser cookies and mobile ad identifiers (Google 2022). Still, privacy regulations and proposed regulations have largely ignored these developments to date. For instance, the FTC's request for public comment on "Commercial Surveillance and Data Security" only mentions PETs in passing.[19]

4.6 Conclusion

The GDPR represents an opportunity for economists to understand the consequences of an economy-wide privacy regulation. However, the GDPR poses several challenges for economic research. First, the GDPR made a global impact as it covers both EU firms and non-EU firms that target EU residents. The GDPR also created substantial global spillovers, so researchers may struggle to find a suitable control group that is both excluded from the regulation and comparable to the EU. Second, the variability of firm compliance and regulatory enforcement under the GDPR complicates the generalizations that we can draw from the literature. Third, the GDPR sought to limit personal data processing and to allow privacy-sensitive consumers to opt out of data processing. This, in turn, can limit empirical researchers' access to data and can introduce consent-based self-selection into the observed data.

The economic literature on the GDPR examines multiple facets of the regulation and its impact. The GDPR presented a novel opportunity for economists to empirically investigate long-held hypotheses like the consequences of privacy regulation for competition and innovation. Most GDPR research points to the GDPR hurting firm outcomes and disproportionately harming smaller and more data-dependent firms. For consumers, the literature illuminates objective improvements in privacy and surveys consumers for their views on the GDPR. The literature also explores the consequences of the GDPR's design elements including its international spillovers.

Looking back at the GDPR literature, one potential criticism is that the literature has documented the *unintended* consequences, but perhaps neglected the *intended* consequences of the GDPR. In particular, we want to better understand the privacy benefits to consumers and rigorously quantify these benefits. As well, we want to better understand and quantify the gains in data protection. To be fair, these are difficult subjects to evaluate

19. The request for comment contains 95 questions. The final question asks about the "potential obsolescence of any rulemaking" and references the privacy-related innovations in the online ad industry.

convincingly with the data at hand, though Demirer et al. (2023) represents a notable exception.

The GDPR and privacy regulation more generally offer several more directions for research. First, Section 4.2 lists many elements of the GDPR that have received little attention so far. Second, more attention should be paid to understanding the strategic interactions between firms and regulators. We would like to better understand which enforcement strategies—e.g., fines, notices, choice of targets, establishing legal precedent—are effective in ensuring compliance. Third, the GDPR literature has so far neglected the GDPR's anticipated impact assessments like those of the European Commission (2012) as well as industry-funded studies like Christensen et al. (2013) and Deloitte (2013). These predictions identify lingering questions like the GDPR's impact on employment. Finally, we wish to better understand how to design effective privacy regulation and improve upon existing regulation like the GDPR. In particular, continued research can explore how to limit the unintended consequences of privacy regulation.

Policy makers and regulators around the globe continue to wrestle with how to regulate privacy effectively in the modern data economy. Research can continue to illuminate their task. As the GDPR continues to evolve in practice, this will present more opportunities to study the law. New privacy laws worldwide also represent opportunities for research. Recent breakthroughs in commercializing privacy-enhancing technologies promise to limit certain trade-offs between privacy and the data economy. More research is needed to understand the novel trade-offs that these technologies present as well as the economic consequences of adopting these technologies.

References

Abis, S., M. Canayaz, I. Kantorovitch, R. Mihet, and H. Tang. 2022. *Privacy Laws and Value of Personal Data*. Technical report, EPFL.

Acquisti, A., C. Taylor, and L.Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54 (2): 442–92.

Anand, P. and C. Lee. 2023. "Using Deep Learning to Overcome Privacy and Scalability Issues in Customer Data Transfer." *Marketing Science* 42 (1): 189–207.

Aridor, G., Y.-K. Che, and T. Salz. 2023. "The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR." *RAND Journal of Economics*. Forthcoming.

Athey, S., C. Catalini, and C. Tucker. 2017. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." NBER Working Paper 23488. Cambridge, MA: National Bureau of Economic Research.

Autoriteit Persoonsgegevens. 2019. "AP: veel websites vragen op onjuiste wijze toestemming voor plaatsen tracking cookies." https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veelwebsites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies.

Bessen, J. E., S. M. Impink, L. Reichensperger, and R. Seamans. 2020. "GDPR and the Importance of Data to AI Startups." SSRN 3576714.
Blanco-Justicia, A., D. Sánchez, J. Domingo-Ferrer, and K. Muralidhar. 2022. "A Critical Review on the Use (and Misuse) of Differential Privacy in Machine Learning." *ACM Computing Surveys* 55 (8): 1–16.
Blind, K., C. Niebel, and C. Rammer. 2023. "The Impact of the EU General Data Protection Regulation on Innovation in Firms." *Industry and Innovation*. https://doi.org/10.1080/13662716.2023.2271858.
Boroomand, F., A. Leiponen, and G. Vasudeva. 2022. "Does the Market Value Attention to Data Privacy? Evidence from US-listed Firms under the GDPR." Wharton Mack Institute working paper.
Bradford, A. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.
Brill, J. 2011. "The Intersection of Consumer Protection and Competition in the New World of Privacy." *Competition Policy International* 7 (1): 7–23.
Cameron, A. C., and P. K. Trivedi. 2005. *Microeconometrics: Methods and Applications*. Cambridge University Press.
Campbell, J., A. Goldfarb, and C. Tucker. 2015. "Privacy Regulation and Market Structure." *Journal of Economics & Management Strategy* 24 (1): 47–73.
Carrière-Swallow, Y., and V. Haksar. 2019. *The Economics and Implications of Data An Integrated Perspective*. Technical report, International Monetary Fund.
Chen, C., C. B. Frey, and G. Presidente. 2022. "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally." The Oxford Martin Working Paper Series on Technological and Economic Change.
Christensen, L., A. Colciago, F. Etro, and G. Rafert. 2013. "The Impact of the Data Protection Regulation in the EU." Intertic Policy Paper, Intertic.
Commission Nationale de l'Informatique et des Libertés. 2019. "Online Targeted Advertisement: What Action Plan for the CNIL?" https://www.cnil.fr/en/online-targetedadvertisement-what-action-plan-cnil.
Congiu, R., L. Sabatino, and G. Sapi. 2022. "The Impact of Privacy Regulation on Web Traffic: Evidence from the GDPR." *Information Economics and Policy* 61: 101003.
Cummings, R., and D. Desai. 2018. "The Role of Differential Privacy in GDPR Compliance." In *FAT* '18: Proceedings of the Conference on Fairness, Accountability, and Transparency*. ACM.
D'Assergio, C., P. Manchanda, E. Montaguti, and S. Valentini. 2022. "The Race for Data: Gaming or Being Gamed by the System?" SSRN 4250389.
Data Protection Commission. 2020. *Report By The Data Protection Commission on the Use of Cookies and Other Tracking Technologies*. Technical report, Data Protection Commission.
DataGrail. 2020. *The Age of Privacy: The Cost of Continuous Compliance*. Technical report.
Deloitte. 2013. *Economic Impact Assessment of the Proposed General Data Protection Regulation*. Technical report, December.
Demirer, M., D. J. Hernández, D. Li, and S. Peng. 2023. "Data, Privacy Laws, and Firm Production: Evidence from GDPR." Work in progress.
Dwork, C. 2006. "Differential Privacy." In *Automata, Languages and Programming*, edited by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, 1–12. Berlin, Heidelberg: Springer Berlin Heidelberg.
European Commission. 2008. "Flash Eurobarometer 226: Data Protection in the European Union: Data Controllers' Perceptions." https://data.europa.eu.
European Commission. 2012. "Impact Assessment Accompanying the document

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data." Commission Staff Working Paper. Technical report, European Commission.

European Commission. 2019. "Data Protection Rules as a Trust-Enabler in the EU and Beyond—Taking Stock." Communication from the Commission to the European Parliament and the Council, European Commission.

European Data Protection Board. 2020. "Contribution of the EDPB to the Evaluation of the GDPR under Article 97." Technical report, European Data Protection Board.

Ferracane, M. F., B. M. Hoekman, E. van der Marel, and F. Santi. 2023. "Digital Trade, Data Protection and EU Adequacy Decisions." EUI, RSC, Working Paper, 2023/37, Global Governance Programme-505, European Centre for International Political Economy (ECIPE).

Gal, M. S., and O. Aviv. 2020. "The Competitive Effects of the GDPR." *Journal of Competition Law and Economics* 16 (3): 349–391.

Geradin, D., T. Karanikioti, and D. Katsifis. 2020. "GDPR Myopia: How a Well-Intended Regulation Ended Up Favouring Large Online Platforms—The Case of Ad Tech." *European Competition Journal* 17 (1): 1–46.

Godinho de Matos, M., and I. Adjerid. 2022. "Consumer Consent and Firm Targeting after GDPR: The Case of a Large Telecom Provider." *Management Science* 68 (5): 3330–3378.

Goldberg, S., G. A. Johnson, and S. Shriver. 2024. "Regulating Privacy Online: An Economic Evaluation of fhe GDPR." Forthcoming in *American Economic Journal: Economic Policy*.

Goldfarb, A., and C. Tucker. 2011. "Privacy Regulation and Online Advertising." *Management Science* 57 (1): 57–71.

Goldfarb, A., and C. Tucker. 2012. "Privacy and Innovation." *Innovation Policy and the Economy* 12 (1): 65–90.

Google. 2022. "The Privacy Sandbox: Technology for a More Private Web." https://privacysandbox.com.

Greene, T., G. Shmueli, S. Ray, and J. Fell. 2019. "Adjusting to the GDPR: The Impact on Data Scientists and Behavioral Researchers." *Big Data* 7 (3): 140–162.

Greenleaf, G. 2023. "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." *Privacy Laws and Business International Report* 181 (1): 2–4.

Hils, M., D. W. Woods, and R. Böhme. 2020. "Measuring the Emergence of Consent Management on the Web." In *Proceedings of the ACM Internet Measurement Conference, IMC '20*, 317–332. New York, NY: Association for Computing Machinery.

Hotz, V. J., C. R. Bollinger, T. Komarova, C. F. Manski, R. A. Moffitt, D. Nekipelov, A. Sojourner, and B. D. Spencer. 2022. "Balancing Data Privacy and Usability in the Federal Statistical System." *Proceedings of the National Academy of Sciences* 119 (31): e2104906119.

Information Commissioner's Office. 2019. "Update Report into Adtech and Real Time Bidding." Technical report.

Information Commissioner's Office. 2021. "Guide to the General Data Protection Regulation (GDPR)." Technical report, Information Commissioner's Office.

Information Commissioner's Office. 2022. "Privacy-Enhancing Technologies (PETs)." Chapter 5 in *Draft Anonymisation, Pseudonymisation and Privacy-Enhancing Technologies Guidance*. Information Commissioner's Office.
International Association of Privacy Professionals. 2017. "Global 500 Companies To Spend $7.8b on GDPR Compliance." https://iapp.org.
International Association of Privacy Professionals. 2023. "GDPR at Five." https://iapp.org/media/pdf/resource_center/gdpr_at_five.pdf.
International Association of Privacy Professionals and Ernst & Young. 2017. "IAPP-EY Annual Privacy Governance Report 2017." Technical report.
Janßen, R., R. Kesler, M. E. Kummer, and J. Waldfogel. 2022. "GDPR and the Lost Generation of Innovative Apps." NBER Working Paper 30028. Cambridge, MA: National Bureau of Economic Research.
Jia, J., G. Z. Jin, and L. Wagman. 2020. "GDPR and the Localness of Venture Investment." SSRN 3436535.
Jia, J., G. Z. Jin, and L.Wagman 2021. "The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment." *Marketing Science* 40 (4): 661–684.
Johnson, G. A., T. Lin, J. Cooper, and L. Zhong. 2023a. "COPPAcalypse? The YouTube Settlement's Impact on Kids Content." SSRN 4430334.
Johnson, G. A., J. Runge, and E. Seufert. 2022. "Privacy-Centric Digital Advertising: Implications for Research." *Customer Needs and Solutions* 9 (1): 49–54.
Johnson, G. A., S. Shriver, and S. Goldberg. 2023b. "Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR." *Management Science* 69 (10).
Johnson, G. A., S. K. Shriver, and S. Du. 2020. "Consumer Privacy Choice in Online Advertising: Who Opts Out and At What Cost to Industry?" *Marketing Science* 39 (1): 33–51.
Jones, M. L., and M. E. Kaminski. 2020. "An American's Guide to the GDPR." *Denver Law Review* 98(1).
Ke, T. T., and K. Sudhir. 2022. "Privacy Rights and Data Security: GDPR and Personal Data Markets." *Management Science* 69 (8).
Kesler, R. 2022. "The Impact of Apple's App Tracking Transparency on App Monetization." SSRN 4090786.
Kircher, T., and J. Foerderer. 2021. "Does EU-Consumer Privacy Harm Financing of US-App-Startups? Within-US Evidence of Cross-EU-Effects." In *Proceedings of the 42nd International Conference on Information Systems (ICIS)*, 12–15. Association for Information Systems (AIS).
Kircher, T., and J. Foerderer. 2023. "Ban Targeted Advertising in Apps? An Empirical Investigation of the Consequences for App Development." *Management Science*. Forthcoming.
Klein, A., R. Manini, and Y. Shi. 2022. "Across the Pond: How US Firms' Boards of Directors Adapted to the Passage of the General Data Protection Regulation." *Contemporary Accounting Research* 39 (1): 199–233.
Komarova, T., and D. Nekipelov. 2020. "Identification and Formal Privacy Guarantees." arXiv preprint arXiv:2006.14732.
Koski, H., and N. Valmari. 2020. "Short-Term Impacts of the GDPR on Firm Performance." ETLA Working Papers.
Koutroumpis, P., F. Ravasan, and T. Tarannum. (2022). "(Under) investment in Cyber Skills and Data Protection Enforcement: Evidence from Activity Logs of the UK Information Commissioner's Office." SSRN 4179601.
Lambrecht, A. 2017. "E-privacy Provisions and Venture Capital Investments in the EU." Working paper.

Lefrere, V., L. Warberg, C. Cheyre, V. Marotta, and A. Acquisti. 2022. "The Impact of the GDPR on Content Providers: A Longitudinal Analysis." SSRN.
Li, D., and H.-T. Tsai. 2022. "Mobile Apps and Targeted Advertising: Competitive Effects of Data Exchange." SSRN 4088166.
Li, H., L. Yu, and W. He. 2019. "The Impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management* 22 (1): 1–6.
Li, S., M. J. Schneider, Y. Yu, and S. Gupta. 2022. "Reidentification Risk in Panel Data: Protecting for k-anonymity." *Information Systems Research* 34 (3):1066–1088.
Libert, T., L. Graves, and R. K. Nielsen. 2018. "Changes in Third-Party Content on European News Websites after GDPR." Technical report, Reuters Institute for the Study of Journalism.
Lukic, K., K. M. Miller, and B. Skiera. 2023. "The Impact of the General Data Protection Regulation (GDPR) on the Amount of Online Tracking." SSRN 4399388.
Maex, S. A. 2022. "Modern Privacy Regulation, Internal Information Quality, and Operating Efficiency: Evidence from the General Data Protection Regulation." PhD dissertation, Temple University.
Martin, N., C. Matt, C. Niebel, and K. Blind. 2019. "How Data Protection Regulation Affects Startup Innovation." *Information Systems Frontiers* 21 (6): 1307–1324.
McDowall, D., R. McCleary, and B. Bartos. 2019. *Interrupted Time Series Analysis*. Oxford University Press.
Miller, A. R. 2024. "Privacy of Digital Health Information." In *The Economics of Privacy*, edited by Avi Goldfarb and Catherine Tucker. Chicago, IL: University of Chicago Press. This volume.
Miller, A. R., and C. Tucker. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." *Management Science* 55 (7): 1077–1093.
Miller, A. R., and C. E. Tucker. 2011. "Encryption and the Loss of Patient Data." *Journal of Policy Analysis and Management* 30 (3): 534–556.
noyb. 2022. "noyb Aims to End "Cookie Banner Terror" and Issues More than 500 GDPR Complaints." https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issuesmore-500-gdpr-complaints.
Peukert, C., S. Bechtold, M. Batikas, and T. Kretschmer. 2022. "Regulatory Spillovers and Data Governance: Evidence from the GDPR." *Marketing Science* 41 (4): 318–340.
Phillips, N. 2019. "Keep it: Maintaining Competition in the Privacy Debate." Remarks for Internet Governance Forum.
Polinsky, A. M., and S. Shavell. 2000. "The Economic Theory of Public Enforcement of Law." *Journal of Economic Literature* 38 (1): 45–76.
Prasad, A., and D. R. Perez. 2020. "The Effects of GDPR on the Digital Economy: Evidence from the Literature." *Informatization Policy* 27 (3): 3–18.
Presthus, W., and K. F. Sønslien. 2021. "An Analysis of Violations and Sanctions following the GDPR." *International Journal of Information Systems and Project Management* 9 (1): 38–53.
Presthus, W., and H. Sørum. 2019. "Consumer Perspectives on Information Privacy following the Implementation of the GDPR." *International Journal of Information Systems and Project Management* 7 (3): 19–34.
Presthus, W., and H. Sørum. 2021. "A Three-Year Study of the GDPR and the Consumer." In *14th IADIS International Conference Information Systems 2021. International Association for Development of the Information Society*.
Ravichandran, D., and N. Korula. 2019. "Effect of Disabling Third-Party Cookies on Publisher Revenue." Technical report, Google Inc.

Romanosky, S., R. Telang, and A. Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30 (2): 256–286.

Schmitt, J., K. M. Miller, and B. Skiera. 2021. "The Impact of Privacy Laws on Online User Behavior." arXiv preprint arXiv:2101.11366.

Schneider, M. J., S. Jagpal, S. Gupta, S. Li, and Y. Yu. 2018. "A Flexible Method for Protecting Marketing Data: An Application to Point-of-Sale Data." *Marketing Science* 37 (1): 153–171.

Skiera, B., K. Miller, Y. Jin, L. Kraft, R. Laub, and J. Schmitt. 2022. "The Impact of the General Data Protection Regulation (GDPR) on the Online Advertising Market." https://www.gdpr-impact.com/.

Sobolewski, M., and M. Paliński. 2017. "How Much Consumers Value On-Line Privacy? Welfare Assessment of New Data Protection Regulation (GDPR)." University of Warsaw Faculty of Economics Sciences Working Paper.

Sørum, H., and W. Presthus. 2020. "Dude, Where's My Data? The GDPR in Practice, from a Consumer's Point of View." *Information Technology and People* 34 (3): 912–929.

TrustArc. 2018. *GDPR Compliance Status: A Comparison of US, UK and EU Companies*. Technical report. TrustArc.

Urban, T., D. Tatang, M. Degeling, T. Holz, and N. Pohlmann. 2020. "Measuring the Impact of the GDPR on Data Sharing in Ad Networks." In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (ASIA CCS '20). ACM.

Venkatesan, R., S. Arunachalam, and K. Pedada. 2022. "Short Run Effects of Generalized Data Protection Act on Returns from AI Acquisitions." Working paper. https://conference.nber.org/conf_papers/f161612.pdf.

Wang, P., L. Jiang, and J. Yang. 2023. "The Early Impact of GDPR Compliance on Display Advertising: The Case of an Ad Publisher." *Journal of Marketing Research* (April 11).

Wang, X., F. Xu, and F. Zhang. 2022. "Consumer Privacy in Online Retail Supply Chains." SSRN 3912642.

Williams, A. R., and C. M. Bowen. 2023. "The Promise and Limitations of Formal Privacy." *WIREs Computational Statistics* (May 9). https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/wics.1615.

World Bank. 2021. *World Development Report 2021: Data for Better Lives*. The World Bank.

Yom-Tov, E., and Y. Ofran. 2022. "Implementation of Data Protection Laws in the European Union and in California Is Associated with a Move of Clinical Trials to Countries with Fewer Data Protections." *Frontiers in Medicine* 9.

Yuan, B., and J. Li. 2019. "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation." *International Journal of Environmental Research and Public Health* 16 (6).

Zhao, Y., P. Yildirim, and P. K. Chintagunta. 2021. "Privacy Regulations and Online Search Friction: Evidence from GDPR." SSRN 3903599.

Zhuo, R., B. Huffaker, kc claffy, and S. Greenstein. 2021. "The Impact of the General Data Protection Regulation on Internet Interconnection." *Telecommunications Policy* 45 (2): 102083.

Zolas, N., Z. Kroff, E. Brynjolfsson, K. McElheran, D. N. Beede, C. Buffington, N. Goldschlag, L. Foster, and E. Dinlersoz. 2020. "Advanced Technologies Adoption and Use by US Firms: Evidence from the Annual Business Survey." NBER Working Paper 28290. Cambridge, MA: National Bureau of Economic Research.