MSI at the ARF

The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing: A Marketing Science Institute Report

May 1, 2024

The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing: A Marketing Science Institute Report

Jean-Pierre Dubé UNIVERSITY OF CHICAGO

Dirk Bergemann YALE UNIVERSITY

Mert Demirer MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Avi Goldfarb UNIVERSITY OF TORONTO

Garrett Johnson BOSTON UNIVERSITY

Anja Lambrecht LONDON BUSINESS SCHOOL

Tesary Lin BOSTON UNIVERSITY

Anna Tuchman NORTHWESTERN UNIVERSITY

Catherine Tucker MASSACHUSETTS INSTITUTE OF TECHNOLOGY

John G. Lynch UNIVERSITY OF COLORADO-BOULDER & MARKETING SCIENCE INSTITUTE*

ABSTRACT

In an era where firms are innovating and using more data than ever before for marketing purposes, there is a perceived need for enhanced regulation to protect consumers' privacy. We provide a perspective based on the academic marketing literature that evaluates the various benefits and costs of existing and pending government regulations and corporate privacy policies. We make two key points. First, regulators may want to avoid starting from the stance that data-based marketing and personalization are automatically harmful. Second, regulations and policies may have inadvertent consequences. On the demand side, privacy regulations and policies may exacerbate the digital exclusion of already marginalized segments of consumers. Further, consumers differ in whether and how they benefit from sharing versus not sharing specific data. On the supply side, regulation and policies may disproportionately disadvantage the competitiveness of entrpreneurs and small businesses. Technology platforms are proposing differential privacy solutions that mitigate some of these harms, but, again, in a way that might disadvantage small firms and entrepreneurs.

TABLE OF CONTENTS

INTRODUCTION

A number of recent initiatives have re-invigorated the debate about consumer digital privacy in the U.S. President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence highlights the Federal Government's commitment to enforce consumer protection laws and enact appropriate safeguards "against fraud, unintended bias, discrimination, infringements on privacy, and other harms from AI" (Biden, 2023). Specifically, the Executive Order states:

> *"My Administration cannot — and will not —tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice. From hiring to housing to healthcare, we have seen what happens when AI use deepens discrimination and bias, rather than improving quality of life."*

and

> *"Americans' privacy and civil liberties must be protected as AI continues advancing. Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires."*

As we write, 13 states in the U.S. have enacted comprehensive privacy laws that emulate the European General Data Protection Regulation (GDPR): California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia; 20 more states have active bills. In 2024, Google is purportedly discontinuing cookies that help track a consumer's browsing histories; however Google announced more delays in this process as recently as April 2024 due to competition concerns by the UK Financial Conduct Authority (Joseph 2024).

There are many good reasons for privacy regulation (Acquisti 2023). Computer science research shows that de-anonymizing putatively anonymized data can reveal a person's identity: even seemingly innocuous information such as a consumers's Netflix ratings of movies can be used to de-identify other much more sensitive data in other databases (Ohm 2010). In the extreme, some believe that using private data to target and disseminate harmful and potentially persuasive mis-information could undermine the functioning of western democracies (Sunstein 2019).

This paper synthesizes emerging empirical findings from the academic literatures in marketing and economics about the intended versus unintended consequences of existing and pending privacy regulations for consumer markets (see also Bleier, Goldfarb & Tucker 2020). Our aim is to provide governments and platforms an academic view of the trade-offs associated with these privacy measures. Recognizing and discussing these tradeoffs may allow business leaders and policymakers to achieve their goals without imposing a disproportionately high unintended cost. We do not consider the legal arguments for consumer privacy as a fundamental right.

The inherent **tradeoff between privacy and the usefulness of content** poses a challenge in the determination of optimized privacy regulations designed to protect. There is also a **tradeoff between privacy and competition and the ability to ensure fairness and nondiscrimination.**

As we discuss herein, personalized marketing is not automatically harmful, nor a zero-sum game in which value is transferred from consumers to firms.

Most of the unintended negative effects of privacy policies are due to how particular privacy-enhancing regulatory or platform actions reduce the usefulness of consumer data to both consumers and firms and *differentially* reduce the usefulness of consumer data for disadvantaged consumers or for smaller businesses. Many restrictions on consumer data could disadvantage marginalized consumers and could harm the competitiveness of consumer markets, stifling valuable product innovation and putting entrepreneurs and small businesses at the biggest disadvantage. Privacy regulations could in many ways primarily benefit the most privileged consumers who exhibit the strongest preferences for privacy measures. An emerging literature suggests ways that firms lack sufficient data to be more inclusive with their product and service offerings and/or to audit their algorithms for unintended biases. Before synthesizing the literature on unintended costs of privacy regulation, we lay out the intended benefits.

INTENDED BENEFITS OF DIGITAL MARKETING PRIVACY REGULATION

There are several important reasons why consumers need and would benefit from more oversight of the use of their personal data by marketers.

- *Firms may possess and act on incorrect information about consumers* which could harm the latter if such data use lacks transparency and the ability to correct (CFPB 2022a). A recent report by the US Government Accountability Office (2022) notes that "companies collect personal and transactional data to create consumer scores…to predict how consumers will behave in the future." These scores suffer from biases, due to social inequities and intrinsic bias in the data themselves, inaccuracies, due to out-of-date information. Their usage can lead to seemingly unfair differential treatment.
- *Firms may use personal data to discriminate unfairly against disadvantaged consumers* or protected classes (CFPB 2022b). For example, the U.S. Justice Department sued Meta "alleging that Meta's housing advertising system discriminates against Facebook users based on their race, color, religion, sex, disability, familial status and national origin" (Civil Rights Litigation Clearinghouse 2022). Class actions have been filed against healthcare companies for allegedly disclosing protected heatlh information to Meta's pixels, used to track individuals' browsing behavior (Asplund 2024). Even without an intent to discriminate, the predictive algorithms that govern online advertising may unfairly avoid serving groups of consumers and deny them full access to the digirtal economy (Lambrecht and Tucker 2019).
- *Firms may potentially price discriminate against consumers with higher valuations of a product or service.* Firms can infer consumer valuations from historic purchase data and use that information to choose personalized price or discount levels (Rossi, McCullough, and Allenby 1996). With more refined algorithmic personalized pricing, firms can unintentionally discriminate along socially controversial segment boundaries.

For example, Princeton Review charged higher prices in zip codes with many Asians (Agnwin, Mattu, and Larson 2015). Behaviorally-based price discrimination" (Fudenberg and Villas-Boas 2006) can lead to a "ratchet effect" even when consumers attempt to protect their privacy (Hart and Tirole 1988). The Council of Economic Advisors (2014) explains:

> *"Consumers have a legitimate expectation of knowing whether the prices they are offered for goods and services are systematically different than the prices offered to others."*

- *Current notice and consent regimes may not be sufficient to protect consumers.* "Notice and consent" has become a primary tool in privacy protection policy, motivated by the possibility that consumers may not always be able to protect themselves against the aforementioned harms. We enumerate two limitations of "consent" that places boundaries on how consumers' data are collected and used. First, sellers and buyers may have asymmetric information about the consequences from data sharing unforeseen by the buyer (Acquisti, Taylor, and Wagman 2016; Clark 2020; Ohm 2010). Second, "consent fatigue" undermines meaningful consideration of the consequences of sharing data. In digital markets, consumers are exposed to a large number of consent requests, often to get access to information on a website (Acquisti 2023; Borner 2022). Even those with a strong intrinsic preference for privacy may not exert the cognitive effort required to consider each of the numerous consent requests carefully or to consider all potential consequences of consent (cf. Moorthy, Ratchford, and Taldukar 1997). Miller and Tucker (2018) find that without any control over data, notice and consent alone can backfire and consumers may not adopt potentially beneficial products. Some legal scholars have argued that firms may incorporate legalese and disclosures into their terms of use that offer more protection to firms than to consumers: the "Behavioral Paradox of Boilerplate" (Wilkinson-Ryan 2017). Wilkinson-Ryan argues: "*the mere fact of fine print inhibits reasonable challenges to unfair deals*" because "*no one reads standard terms*."

These are questions regarding data privacy are distinct from questions regarding information security, such as corporate data breaches and identity theft by malign actors.

PERTINENT REGULATIONS AFFECTING MARKETING

Motivated by concerns like those above, the European Union already pro-actively launched the General Data Protection Regulation (GDPR) in 2018, with far-reaching implications for over 20 million companies spanning dozens of countries. GDPR puts a high bar on a firm's ability to collect and process the personal data of individual consumers and to guarantee transparency. For example, personal data such as sex and gender should only be collected and processed when it is necessary for the task. Similar data privacy laws have been implemented by Australia, Brazil, Canada, Chile, China, Egypt, India, Israel, Japan, Kenya, New Zealand, Nigeria, South Africa, South Korea, Switzerland, Thailand, Turkey, and the UK (Zafar 2023).

GDPR Article 3 created multiple individual rights including the right to access one's data, the right to be forgotten via erasure of one's data, the right to data portability, and the right to

be informed about data breaches. GDPR Article 5 requires of "data controllers"(firms) that: a) any processing of personal data should be lawful, fair, and transparent to the person; b) personal data should be collected only for a specific and limited purpose and not processed further beyond that purpose; c) individual data should be minimized in scope to only what is required for the original purpose; d) firms must ensure the accuracy of personal data, and when inaccuracies are identified, they are erased or rectified without delay; e) identifiable personal data are stored for no longer than strictly necessary; and f) processed in a way that ensures security of personal data and protects against accidental loss. GDPR Article 6 addresses the individual's consent to the collection of personal data, requiring that consent must be freely given, specific, informed and unambiguous.

Johnson (2023) summarizes several steps marketers have taken to comply with the law. The practical reality of the GDPR often falls short of the law as written. Discrepancies arise both as a function of firm discretion in compliance and regulator discretion in enforcement. While marketers largely avoided great disruption that some predicted, they arguably inhabit a legal gray area that regulators may continue to shrink in the future.

Unlike many other western democracies, the U.S. has not yet implemented a federal digital data policy that encompasses all sectors. Instead, a more decentralized patchwork of federal and state laws has emerged, along with industry-specific regulations that are enacted at the federal level but apply to specific sectors, such as HIPAA which governs health data. At the federal level, the American Innovation and Choice Online Act failed to pass due to concerns over security and feasibility (e.g., Editorial Board 2022). Most U.S. privacy measures have been implemented in a fragmented way across a variety of state laws like California's Consumer Protection Act (CCPA) and Colorado's Privacy Act (CPA). While the broad regulation is less strict in the U.S. than in Europe, there are some very clear sector- and product-specific regulations. For example, in credit markets, mortgage lenders are required to collect data about protected class attributes from their borrowers. By contrast, consumer lenders are largely prohibited from doing so (Bogen, Rieke, and Ahmed 2020).

Perhaps in anticipation of heightened regulations, many American firms have already voluntarily self-disciplined. In 2023, Google committed to the deprecation of third-party cookies in its Chrome Browser (Chrome has a 50% browser market share in the U.S.) and Apple's "Ask-Not-To-Track" option in its App Tracking Transparency (ATT) framework blocks apps from tracking an individual's behavior on other companies' apps and websites without the individual's explicit opt-in (Kesler 2023).

Many of the measures already implemented abroad, and pending or implemented in the U.S., generate unintended costs that need to be counterbalanced against the intended benefits. On the demand side, many of the key motivations for marketing privacy regulation relate to fairness and protection from discrimination. However, the most privileged consumers who are not at risk of exclusion in the digital marketplace may value privacy the most. For example Varian, Wallenberg, and Woroch (2005) found that richer and more educated households were more likely to sign up for "Do Not Call" lists.

Turning to the supply side of the market, regulators may need to balance the need for privacy against the provision of valuable content. Privacy measures like GDPR introduce non-trivial economic compliance costs that may be more difficult to bear for smaller firms.

Paradoxically, Europe's digital ad sector became more concentrated after GDPR, at least in the short run (Johnson, Shriver, and Goldberg 2023; Peukert et al. 2022) Similarly, measures to reduce off-site data-tracking will likely disproportionately increase costs for small businesses and entrepreneurs. While emerging privacy-enhancing technologies (PETs) seem promising as an alternative to all-out data bans, these approaches are still in their infancy and may be disproportionately costly to implement for smaller businesses. Emerging work on "comprehensible targeting policies" that represent a firm's targeting rule and data usage in a single sentence to comply with GDPR's "right to explanation" policies also show promise (Zhang 2024).

Before reviewing this evidence, we first review what we know about which consumers most value privacy — and why and when consumers are open versus averse to specific data sharing.

CONTINGENT CONSUMER DEMAND FOR PRIVACY

According to a recent Pew survey (Auxier et al 2019), "some 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits." Accordingly, Deloitte finds that "77% [of consumers] want the government to do more to regulate the way companies collect and use that data" (Arbanas et al. 2023). Pew finds this preference to be strikingly bi-partisan (Faverio 2023), with 68% support by Republican and Republican-leaning, and 78% support by Democrat and Democrat-leaning respondents. These stated preferences for privacy appear to be at odds with revealed preference for privacy implied by the fact consumers regularly share highly personal information about themselves, especially on social media.

Therefore, sweeping statements that consumers do or do not value privacy are unhelpful because they overlook the role of context. Privacy preferences depend on the situation and the individual. Moreover, surveys typically focus mostly on information security concerns (e.g., fraud, sharing with malign actors, etc.) that are not tied to marketing and issues of privacy. Surveys rarely ask about specific marketing tactics associated with the broad "privacy" label. Most surveys do not provide clear guidance to regulators about which consumers believe they would benefit by reducing online retailer personalization, by removing access to data from prior months on the same website, or by blocking an online merchant's ability to track the consumer's path from clicking on an ad to a purchase of the advertised product.

CONSTRUCTED PREFERENCES, CHOICE ARCHITECTURE AND THE PRIVACY PARADOX

The fact that consumers say they value privacy but behave in ways that suggest otherwise is sometimes called the"*privacy paradox*" (e.g., Spiekerman et al 2001, Goldfarb and Que 2023). However, the fact that stated preferences do not align with actual behavior is not unique to privacy. One of the most robust results in social psychology is the modest correlation between individuals' attitudes toward some object or issue and their behavior related to that issue (Ajzen et al. 2018). General attitudes predict composites of multiple behaviors; but are weakly related to single behaviors.

More germane to the problem of privacy policy, one would expect inconsistencies between stated and revealed preferences if a) some survey responses do not reflect enduring privacy preferences, b) some stated preference for privacy are overstated and reflect social desirability bias, or c) enduring and stable preferences exist, but vary in predictable ways across contexts and behaviors aligned with those preferences that are not examined in surveys.

Some consumers may have weak privacy preferences. At least some consumers likely lack strong, pre-existing privacy preferences. Lack of strong pre-established preferences produces high sensitivity to context of both answers to questions about privacy valuation and overt privacy-relevant behaviors. When consumers lack strong prior preferences and privacy concerns are not salient, other salient consumer goals dominate, like reading a story on a website that can only be accessed by consenting (cf. Bakos, Marotta-Wurgler and Trossen 2014, Chin and Beckett 2021; Dalmia and Diehl 2024).

When consumers lack pre-determined attitudes or cannot retrieve them in the moment, they "construct" preferences on the spot. The hallmark of constructed preferences is that behaviors or survey responses are highly sensitive to seemingly minor changes in context or question wording (Bettman, Luce, and Payne 1998; Feldman and Lynch 1988; Schwarz 1999, Simmons, Bickart, and Lynch 1993).

When preferences are constructed, even privacy behaviors can be sensitive to seemingly irrelevant details. Firms typically use some form of "choice architecture" or "nudges" (Thaler and Sunstein 2021) to make it more likely that consumers will disclose. For instance, an opt-in policy that uses "no" as the default option for data tracking leads to much lower consent than an opt-out policy that uses "yes" as the default option for data tracking (Johnson, Bellman, and Lohse 2002). Choice architecture can help consumers or can help firms take advantage of consumers constructing their privacy preferences. In August 2018, for instance, 57.4% of EU websites used design patterns to nudge consumers into sharing data (Utz et al. 2019). In the same way, the specific choice architecture can bias any conclusions one draws about privacy preferences measured from consumer consent requests (e.g., Lin and Strulov-Shlain 2023). Government regulators should avoid basing privacy regulations on survey evidence collected in common contexts where consumers' privacy preferences were likely constructed on the spot and sensitive to "nudging."

Larsen (2023) finds a substantial association between stated privacy concerns and measures of social desirability bias. He argues "A social norm that suggests everyone should be concerned about privacy could cause some subjects to change their answers for impression management (i.e., to give positive impressions to others), self-deception (i.e., to feel better about themselves), or identity definition. This overstatement can create social desirability bias (SDB) and change the relationships between privacy attitudes and various behaviors."

Privacy preferences are weaker for younger, less educated, and lower income consumers. Lin and Strulov-Schlain (2023) measured privacy preferences for Facebook users who proved to be highly heterogeneous in their willingness-to-pay for sharing their data with prospectvie advertisers. Richer, more educated, and older consumers tended be willing to pay more for privacy. Moreover, those with lower value for privacy were more sensitive to choice architecture via anchors used in valuation questions. Large anchoring effects suggest a lack

of stable, previously formed preferences. Anchoring effects were larger for lower-income, less educated, and younger consumers than for richer, more educated, and older ones.

These same facts can support quite different policy conclusions. Lower-income, younger, and less educated consumers may be right to give privacy lower priority than do richer, more educated, and older consumers. For the former group, the gains from data sharing may outweigh possible risks from privacy loss. If so, one can argue that current privacy regulation is being tilted towards the concerns of the privileged.

The counterargument is that the younger, less educated, and poorer consumers might be wrong to assign low value to their privacy if, for instance, they do not understand the consequences of sharing their data. Mrkva et al (2021) show that choice architecture has larger effects on more disadvantaged, lower-knowledge consumers. In that case, more stringent and paternalistic regulation that does not rely on consent-based frameworks may be more effective (e.g., Acquisti, Brandimarte, and Hancock 2022). Alternatively, less paternalistic measures such as global privacy control ("GPC") would allow consumers to set their privacy preferences at the browser level, as proposed in the CCPA. However, GPC still uses a choice-architecture to obtain consent.[1]

PRIVACY PREFERENCES AND WELFARE ANALYSIS

The aforementioned discussion could be taken to imply that policymakers and platforms should make it harder for consumers to agree to disclose. We disagree on the basis of the heterogeneity in the marketplace.

Acquisti (2023) and Goldfarb and Que (2023) argue that privacy is not about concealment (cf. Posner 1981), but about **boundary regulation**. Altman (1977) construed privacy as encompassing both information sharing and information hiding, along with individuals' ability to choose dynamically between these two actions based on the context.

People who say "I have nothing to hide" nonetheless tilt their laptop screen away from strangers seated next to them on a plane. The same people might gladly share their laptop screens with colleagues on collaborative Zoom calls or upload confidential Zoom call transripts to ChatGPT for summarization. People who prefer that their work colleagues not know about a health condition might wish that HIPPA medical privacy regulations made it easier to share their unified health histories with new specialists or with family members and their doctors. Nissenbaum (2004) refers to this phenomenon of wanting disclosed information to be used only in approved contexts as "contextual integrity."

The welfare analysis of privacy restrictions and their costs and benefits must consider these nuances in privacy preferences. A key insight from this work is that the value of data sharing

[1] As discussed below, data-tracking bans or restrictions do not lower the cost to consumers of sharing data when they have instrumental reasons to want to share with some but not all businesses. In contrast, policies such as data portability, give the consumer agency to share data when it is to their advantage (CFPB 2023). GPC might lower costs for consumers with very strong intrinsic privacy preferences to avoid sharing with any businesses. However, it is not obvious how consumers should make tradeoffs if they value a website remembering their browsing history as they search for a flight to Europe; but do not want to be bombarded with re-targeted ads for a trip after they have already taken it.

or privacy to consumers often depends on the economic context. For instance, the privacy harm resulting from data disclosure can be significant in the case of location data that reveals visits to abortion clinics in politically conservative states (Ng 2022). In other situations, the value consumers receive from sharing data can be immense, as exemplified by OpenAI's development of generative artificial intelligence models using public and private data sources.

Different consumers can have distinct preferences when facing the same data usage scenario. Richer households may prefer to not to reveal their higher willingness to pay, while poorer households may benefit from revealing their lower willingness to pay. We should therefore expect heterogeneous welfare effects of data sharing for different data usage scenarios and different consumer subgroups.

A complication for consumer welfare analysis is the fact that privacy costs include both **instrumental and intrinsic** components (Lin 2022). When consumers decide not to share data for fear of receiving higher prices, their preferences for privacy are instrumental, connected to concrete consequences of personal data usage. Consumers can also experience a pure psychological cost of sharing data. For instance, they may not like companies knowing their locations 24/7 regardless of how their data will be used. While the instrumental preference heterogeneity can be tied to economic rationales, the intrinsic preferences for sharing data are harder to predict and less understood.

The heterogeneity of privacy preferences across consumers and the fact that privacy preferences can be intrinsic and instrumental is a reason for consent-based privacy regimes. An approach that broadly restricts data transmission or makes it costlier will likely not be the answer. Regulators should consider the key concept of boundary regulation, not raising the cost of data exchanges that, in some instances, benefit consumers. Moreover, certain industry solutions such as browser-level Global Privacy Controls seem well suited for consumers with strong "intrinsic" privacy preferences to say "no" to all such requests. Research is needed to devise ways to allow those with instrumental privacy preferences to provide meaningful "batched consent" to efficiently and selectively decline some requests and accept others.

ACCESS TO CONSUMER DATA CAN INCREASE VALUE

Personalized marketing is not automatically harmful. One of the most contentious aspects of the use of personal data for marketing purposes is the targeting of marketing offers. Firms use customer data for personalization of all elements of the marketing mix from advertising, to personalized experiences in the sales channel, to personalized pricing. While some regulators have acknowledged the potential benefits to consumers from the personalization of communications, products and offers (e.g., Council of Economic Advisors 2014, pp.7-8), most privacy laws inevitably limit the potential for such personalized marketing.

The consensus on the perceived impact of personalized pricing is mostly negative. The popular press has been rife with dire headlines like "How Online Shopping Makes Suckers of Us All" (Useem 2017) and "How Retailers Use Personalized Prices to Test What You're Willing

to Pay" (Mohammed 2017). While, in reality, documented examples of such personalized pricing are scarce, even public officials have expressed concerns: "[differential pricing] transfers value from consumers to shareholders, which generally leads to an increase in inequality and can therefore be inefficient from a utilitarian standpoint"(Council of Economic Advisors 2015, p. 6). Some have even questioned the legality of personalized pricing (Ramasastry 2005). In general, personalized marketing has become a lightning rod for allegations of unfair marketing practices and consumer harm.

This is not to say that data-based marketing could not harm consumers. Personalized marketing could exclude segments of the population from valuable communications or, indirectly, through higher and possibly regressive prices. But, research shows that the social impact of data-based personalized pricing is theoretically ambiguous and does not per se lead to harm just as it does not per se increase social value. First, given that it is literally impossible for a firm to be able to predict with 100% certainty each customer's true willingness-to-pay, personalized pricing today is at best a very granular form of third-degree price discrimination (or segmented pricing). Economic theory shows that a monopolist using third-degree price discrimination can increase the value created for consumers so long as the total quantity of consumers served strictly increases (e.g., Varian 1989). In short, price discrimination is not a zero-sum game between a firm and its consumers – it can be win-win. Bergemann et al (2015) demonstrate that the exact circumstances under which price discrimination can increase both consumer value and firm value depends on the nature of the consumer segments defined by the data available.

Turning to a competitive marketplace with competing firms all using personalized pricing, Bergemann et al (2023) show that a similar intuition applies even in oligopoly settings. However, unlike the monopoly setting, the tendency for oligopoly price discrimination to increase consumer value *in equilibrium* is further enhanced by a potential strategic motive. When firms exhibit asymmetric strong and weak segments, the personalization of prices can trigger price wars and even a prisoner's dilemma where all firms' profits decline to the benefit of consumers who enjoy lower prices (e.g., Stole 2007).

A growing empirical literature has provided several examples of settings where personalized pricing can be beneficial to consumers. Moreover, many of these case studies find that the most disadvantaged consumers are most likely to be charged the lowest prices. Dubé and Misra (2023) find that personalized pricing leads to lower prices charged for over 60% of the customers for a large digital human resources platform, with the smallest enterprise customers being the most likely to obtain a lower price. DellaVigna and Gentzkow (2019) find that supermarket prices in poor neighborhoods are 8% higher than they would be if large chains allowed for more granular geographic price differences across stores in a given city. Allcott et al (2019) find that willingness-to-pay for healthy and unhealthy nutrients is increasing and decreasing, respectively, in a household's income. Therefore, personalized pricing could help reduce nutritional inequality. Glenn, Dubé, and Kavanagh (2022) discuss a similar public policy implication of personalized pricing as a way to help low-income households afford municipal fines and fees to avoid defaulting and accumulating municipal debt. Arslan, Tereyağoğlu, and Yılmaz (2023) find that switching from uniform to variable pricing of National Football League tickets increased primary-market ticket sales more for hometown teams with lower income and higher income diversity, *"supporting the criticism that traditional fixed pricing strategies favor the customers with higher income*" (p. 4453).

Personalized marketing has also been found to be socially beneficial in several non-price settings. The California SNAP program found that it could more than double the number of eligible individuals who enrolled for food stamps under a personalized e-mail campaign using personally identifiable information and large language models than under campaigns using a single, uniform creative design (Misra 2020).

Similarlly, Chinese privacy regulations that would ban the use of personal data in home page recommendations would lead to a lower incidence of buying recommended products on Alibaba, a decrease that was more pronounced for niche merchants and consumers with unusual tastes (Sun et al 2023). Consumers listen to increasingly diverse music after adopting a streaming service with a recommendation algorithm (Datta, Knox, and Bronnerberg 2018). These results are broadly consistent with Anderson's (2006) "long tail" thesis that digital marketing can move commerce from a market for "hits" to a more inclusive market that allows for market creation and the matching of customers with less common needs and sellers prepared to meet those needs and succeed at a lower volume that a niche market provides.

ACCESS TO CONSUMER DATA STIMULATES INNOVATION AND COMPETITION FROM ENTREPRENEURS AND SMALL BUSINESSES

Technology reduces the cost of collecting, storing, and analyzing data. These advances have enabled substantial innovation in many sectors of the economy including healthcare, retail, financial services, and digital marketing. The increased ability to analyze large quantities of data has contributed to the recent advances in artificial intelligence.

The increased availability of data has been particularly valuable to digital advertising and the ability to automate personalized ad campaigns. Targetability has driven much of the popularity of digital advertising —- and social media advertising in particular —- because it makes digital advertising more efficient than traditional media used for a mass audience. As a result of this growing popularity, digital advertising now constitutes the majority of ad spending (Cramer-Flood 2021).

Individual-level targeting is often implemented using user data that are shared across applications, most notably 'offsite data' (i.e., data collected off the advertising platform) such as browsing history, past purchase events, and other online user actions. Nearly every major advertising platform today offers a way to track such 'offsite' data with user identifiers such as third-party cookies and integrate it into the platform's ad delivery. For example, online retailers can choose to transmit browsing behavior and purchase data to Meta with with a pixel.[2] The retailer can use these data to target ads on Meta's social media platforms, like Facebook and Instagram.

[2] A pixel is defined as "a 1×1 pixel graphic used to track user behavior, site conversions, web traffic, and other metrics similar to a cookie." (Cookie Pro Knowledgebase 2021). Recently, Meta increasingly relies on CAPI (Conversion API) to facilitate matching and measurement (and avoid blocking by the browser).

The increase in data available to businesses has generated a surge in the launch of valuable, disruptive new products for consumers, mostly sold by small businesses and entrepreneurs. Consider the craft beer revolution which has seen the niche segment of craft beers surge from a mere 4% of U.S. sales to over 20% since 2005 (Bronnenberg Dubé, and Joo 2022). This disruption from emerging brands sold by small entrepreneurs is not exclusive to beer *(13D Research 2017).*

> *"In 2016, the top 20 consumer packaged goods companies saw flat sales, while smaller firms averaged 2.9% growth. This follows four years, 2011 to 2015, in which large consumer packaged goods (CPG) companies lost an estimated $18 billion in market share to craft manufacturers."*

Recent CPG growth has become increasingly concentrated amongst new brands sold by smaller businesses, with 16,000 smaller CPG companies generating 19% of total 2018 U.S. sales, a $2 billion (2 percentage point) increase over 2017 (eMarketer Editors 2019).

Prior to the advent of digital marketing, cost considerations by producers and retailers favored sellers of popular products with mass appeal (Alba et al. 1997; Anderson 2006). The costs of launching a new niche brand has declined dramatically with the advent of targetable digital advertising. Digital advertising costs a fraction of the budget needed for traditional television campaigns, saving small U.S. entrepreneurs $163 billion annually; over two-thirds of them would lack a cost-effective means to advertise without the online medium (Kerrigan and Keating 2019). In short, digital advertising has eroded the massive barriers to entry driven by television and other mass media costs that used to be required to build a new consumer brand (cf. Bain 1954, Bronnenberg, Dhar, and Dubé 2009, Caves and Porter 1977, Schamalensee 1982, Sutton 1991).

Research has shown that personalization can facilitae the competitiveness of niche brands. Korganbekova and Zuber (2023) found that privacy restrictions in Safari and Chrome *"... disproportionately hurt price responsive consumers and small/niche product sellers"* on an e-commerce retail platform. Similarly, Sun et al. (2023) found that eliminating personalization had particularly negative effects for niche merchants and for consumers with unusual tastes, as discussed earlier.

The online advertising industry illustrates a tension between privacy and data economy in the GDPR and similar regulations. The ad industry controversially relies on cross-site/app identifiers, which includes third-party cookie identifiers and mobile ad identifiers. Cross-site/app identity creates significant value for advertisers by improving targeting, measurement, and optimization.

The 'offsite data' believed to be at the heart of the effectiveness of digital advertising have become increasingly difficult to track with the advent of the EU's GDPR and such company-initiated policies as Google's deprecation of third-party cookies and Apple's ATT. Consider Meta's Facebook and Instagram platforms, which account for 20% of total U.S. advertising spending (Cramer-Flood 2023). The lack of offsite data would limit the information available to a third-party advertiser to a user's browsing and clicking behavior on the platform itself, as opposed to the user's browsing and purchase behavior offsite on the advertiser's website or app. These restrictions potentially disadvantage smaller businesses disproportionately since

nine out of ten small businesses predominantly use digital advertising, especially on Facebook (Kerrigan and Keating 2019).

Wernerfelt et al. (2024) report a large-scale randomized experiment using 70,000 campaigns on Meta's Facebook and Instagram platforms that measures the incremental profits associated with the use of offsite data in the design of digital advertising placement rules. The results indicate that over 90% of advertisers would experience an increase in the cost per incremental customer acquired through advertising if the campaign was limited to onsite data instead of offsite data, with a median increase of 35% ($42 to $57). More striking, the smallest advertisers have considerably more effective advertising than large advertisers: cost per incremental converter of $12.38 versus $71.06. The smallest advertisers are also harmed considerably more by the loss in access to offsite data in their campaign design. The median small advertiser loses 25 incremental customers per $1,000 spent on advertising, while the median large advertiser only loses 5.

These unintended consequences of privacy regulation and the stifling of innovation echo findings from Goldfarb and Tucker (2011) that early European privacy regulation (the European Union's e-Privacy Directive EC/2002/58) was associated with a 65% decrease in the effectiveness of online advertising. The literature finds that, without cookies, the value created by advertising *falls* by between 4% and 70%. The majority of these studies find that ad prices double or triple when a cookie is present. Johnson et al. (2020) find that this value is roughly proportionately shared with market participants along the supply chain: i.e., advertisers, publishers, and ad tech intermediaries. In this regard, privacy regulation creates a privacy-for-content tradeoff for consumers.

Without cross-site/app identity, consumers enjoy less free content (e.g., Johnson et al. 2023; Kircher & Foerderer 2023a,b). It is probable that GDPR hurt the European advertising-supported software industry—an industry that has been particularly innovative in the U.S. and China over the past two decades. Besides harming the advertising industry, the regulations have stifled innovation with an associated decline in new firms, venture capital investment, and new apps (Jia, Jin, and Wagman 2021; Janssen et al 2022). In healthcare, privacy protection of patients could discourage healthcare IT adoption efforts, and consequently lead to worse health outcomes (Adjerid et al 2016, Derksen, McGahan, and Pongeluppe 2021, Miller and Tucker 2009, 2011). In financial services, there is evidence that measures aimed at increasing security and privacy can lead to a low take-up of innovations such as online banking (Lambrecht, Seim, and Tucker 2011). Substantial empirical evidence suggests a tradeoff between privacy and innovation (Goldfarb and Tucker 2012), though firms may adapt to privacy restrictions by innovating in ways that do not involve data (cf. Agrawal, Gans, and Goldfarb 2019).

A broader concern with privacy restrictions that limit or ban the use of data used for advertising is that they could inadvertently increase concentration in the advertising market. Past work has already found that digital advertising markets became more concentrated in EU countries shortly after the implementation of GDPR (Peukert et al 2022; Johnson et al 2023), with Google and Facebook both experiencing an increase in market share. More recently, when Apple launched ATT, it used a different prompt for Apple apps than it did for for apps made by other companies (Competition and Markets Authority 2021). This distinction likely led to differential opt-in rates for Apple apps versus apps run by other advertising platforms,

potentially giving Apple more access to targetable user data. Regulators shouldconsider this trade-off between individual consumers' preferences for privacy and the possibility of increased concentration, which could lead to higher prices for digital advertising, the primary marketing channel for small businesses. These unintended consequences are non-trivial when we consider the recent wave of innovation in craft product launches that have disrupted various consumer goods categories.

PRIVACY AND INCLUSIVENESS OF MARKETING

Recent work on the economics of digital privacy has focused on the extent to which data-based marketing can harm individuals and groups, particularly those from disadvantaged groups or protected classes. In some settings, discriminatory practices may be illegal. In the U.S., disparate treatment on the basis of someone's protected class status is prohibited in markets for housing, credit, employment, public accommodations and voting. As a result, even when targeted marketing that discriminates on sensitive consumer attributes is permissible, firms may prefer to avoid it due to concerns that such practices may be perceived as unfair or unethical. Sometimes, the algorithms themselves can learn to discriminate absent any deliberate intent by the marketer (Netzer, Lemaire, and Herzenstein (2019), or a cold start problem in algorithmic learning can lead to uneven outcomes for minority relative to majority groups (Lambrecht and Tucker 2024).

In a global advertising campaign, Facebook's bidding algorithm was more likely to serve ads for STEM careers to men than women even though the algorithm was blind to gender (Lambrecht and Tucker 2019). Younger women who are likely to be in the stage of their life when they choose a career were the least likely to be shown an ad. This unintended algorithmic outcome turned out to be driven by the higher equilibrium prices charged for impressions to young females on digital advertising auctions. Consequently, a uniform advertising budget would mechanically reach more men than women, reinforcing gender disparities in STEM. One potential remedy would consist of running a targeted advertising campaign that separates men and women. However, legistlation aimed at ensuring equal access to employment prevented the advertiser from ensuring equal outcomes by by running those separate campaigns.

Uneven outcomes in digital markets can also be a result of human decisions. Online matching platforms rely on ratings of buyers and sellers. A study of an online freelance worker platform found that female freelancers received lower rating scores than men (Bairathi et al 2023). This gap may be due to discrimination and reflect the stereotypes of those individuals who submitted the ratings.. The gap is wider in countries with lower gender equality, in markets with lower female labor force participation rates, and in job categories with weaker female representation.

Paradoxically, the policy objective of privacy protection and the policy objective of nondiscrimination can be in conflict (Ali et al. 2019). Many privacy policies discourage the collection and storage of such personal attributes as race and gender. However, without knowing a customer's race and gender, it would be difficult to determine if digital marketing is

discriminating unfairly (King et al. 2023; Wachter 2020). Nor can firms readily correct for the bias in algorithms that do not use those attributes for prediction, but use correlated attributes that lead to bias in offers (e.g., Ascarza and Israeli 2022).

Thus, banning the collection of data may prevent marketers from detecting and preventing uneven treatment and discriminatory outcomes for disadvantaged groups or protected classes. In the STEM ad campaign discussed above, algorithmic bias could only be detected by virtue of the fact that Facebook tracks gender and age — even though these variables were not used for targeting in the campaign. Similarly, gender discrimination on the freelance worker platform could only be detected due to the platform collecting from freelancers information on their gender. For a similar reason, the racial justice organization Color of Change requests explicitly that tech companies routinely measure "racial and demographic differences regarding user experience" and avoid the use of data that "is the product of real-world prejudice or further perpetuates discrimination (ColorOfChange 2021)."

TOO LITTLE DATA FOR DISADVANTAGED CONSUMERS: IS PRIVACY A BENEFIT FOR THE PRIVILEGED?

Algorithmic exclusion occurs when individuals are excluded from algorithmic processing, meaning that the algorithm cannot make a prediction about them, preventing a firm from screening them for offers and communications to earn their business. In short, marketing databases may lack information about disadvantaged segments because the conditions that lead to societal inequality can also lead to corrupted, missing, and fragmented data (Lin and Misra, 2022). Digital marketing algorithms are highly sensitive to missing and fragmented data (Tucker 2023). Certain segments of the population live in literal *data deserts* in which missing or fragmented data about them make it impossible for algorithms to make a prediction about them. Consequently, marginalized consumer segments may be the most likely to be excluded from algorithmic recommendations of offers and communications.

Several factors contribute to the emergence of such data deserts. *Data sparsity* can be a problem for marginalized segments of the population (Neumann et al 2024; Tucker 2022, 2023). Firms have much more fragmented, erroneous, and incomplete data about poorer consumers and minorities than about wealthier white consumers. The result of living in a data desert is that poorer consumers are excluded from the digital economy. In this regard, many privacy restrictions may be misguided by focusing on limiting consumer data rather than lessening the marketing digital divide through greater data inclusion for the less privileged or creating incentives for data brokers to unify data records for less privileged consumers.

The quantity and scope of data about an individual reflects their "digital footprint." Every time we interact with digital technology, we potentially create data. However, digital footprints are both a result of access to technological devices that record data, and jobs that allow individuals to interact easily with technology. For instance, the city of Boston launched

the "Street Bump" app to automate the detection of potholes and the deployment of repair services by tracking when a driver with the app drives over a pothole. The program unexpectedly led to much higher rates of pothole repairs in wealthy neighborhoods than in poor neighborhoods. Poorer residents were less likely to own a smartphone or engage with apps (Tucker 2023). Similarly, Goldfarb and Tucker (2017,p.4) explain: "John Hancock announced an insurance discount for ratepayers that wear a Fitbit to enable exercise tracking (Mearian 2015). Such discounts will disproportionately benefit the wealthy given that (1) the wealthy are more likely to adopt such technology (e.g. Vogels 2021) or (2) the wealthy are more fit (e.g. Deaton and Paxson 1999)." In online credit markets, Freedman and Jin (2017) show how online information about social networks can help people secure credit, with the implications for inequality depending on how social network depth correlates with socioeconomic status. Lee, Yang, and Anderson (2024) study the use of grocery store purchse data to allow financial institutions to extend credit to consumers who lack credit scores.

Data fragmentation can be another obstacle to obtaining reliable data for certain consumer segments (Tucker 2022, 2023). Most company databases derive from disparate sources. Diverse data sets typically need to be matched using keys such as name, phone number, or email address. Such keys are often less stable for those facing unpredictable economic circumstances, such as instability in housing and one's home address. Since data about disadvantaged populations are often more fragmented (misspellings, missing fields, lack of stable identifiers, etc.), their records are often more difficult to link over time or across datasets.

Neumann et al (2024) find that many large data brokers were unable to predict age or gender accurately for a large portion of the respondents tracked in their panels, with records often missing as opposed simply to exhibiting bias. Missing and/or biased data tended to be associated with low wealth, education, and home ownership, with missing being particularly problematic as brokers simply cannot offer predictions about these individuals. Using voting records from North Carolina as a public census of adults, a leading data broker was less able to provide any matching prediction about an individual's age for Hispanic, Asian, and Black voters than for White voters. Age predictions were more likely to be incorrect for Black Americans. Similarly, Kaplan, Mislove, and Sapieżyński (2017) found that Experian, a leading consumer credit database used to profile consumers eligible for marketing offers, was 50% less likely to contain information about Hispanic and Asian individuals than White individuals, meaning the former are more likely to be excluded from offers based on credit scores. Blattner and Nelson (2021) show that credit scores are statistically noisier indicators of default risk for historically under-served groups who lack credit histories.

Similarly, the heterogeneity in consumers' privacy preferences discussed above can skew data-driven inferences, thereby negatively affecting both consumers and organizations. In clinical trials, for instance, the lack of ability to recruit minority participants leads to noisy estimates of new treatments' efficacy and side effects that these minorities experience. The Mayo Clinic reports that these imprecise estimates led to increases in US healthcare expenditure by $1.2 trillion in 2003-2006 (Ma et al. 2021).

The implications of such data deserts depend on the context. Consumers may be harmed if they lack a predictive score in markets like credit, employment or public services. Of course, consumers could benefit from a data desert if it shields them from excessive state or

corporate surveillance. In general, however, this work puts a very different light on privacy policy recommendations motivated to protect marginalized groups by minimizing what firms know. Privacy "protections" could exacerbate data deserts and the marginalization of consumer segments. Arguably, policymakers should be examining how to level the playing field by giving firms more equal understanding of poorer and richer consumers.

PRIVACY POLICY COMPLIANCE COSTS DISPROPORTIONATELY BURDEN SMALL BUSINESSES

Our discussion thus far has focused on the demand side of the market and how consumers are affected by ways privacy restrictions limit digital marketing. We now turn to the supply side of the market and the impact of privacy regulations on businesses that rely on digital marketing. GDPR offers a useful case study into some of the short and medium-term effects on markets and competition. In spite of the benefits of GDPR to consumers in the form of increased privacy and transparency, Johnson (2023) reviews dozens of papers that consider the economic impact of the GDPR. To date, this literature largely documents the economic harms of the GDPR. These include harms to firm performance, competition, innovation, the web, and marketing. GDPR also increased the cost of collecting and storing data by requiring firms to enhance data protection, imposing penalties in cases of data breaches, and requiring firms to be more transparent to consumers about tracking and data usage.

A case study of one of the largest global cloud-computing providers between 2015 and 2021 provides a detailed account of how over 100,000 firms bound by the GDPR adjusted their monthly data storage and computation usage in response (Demirer et al 2024). The set of firms spans most major industries, from manufacturing to finance, as well as both domestic EU firms subject to the GDPR and domestic US firms not subject to the GDPR. EU firms store, on average, 26% less data than comparable US firms two years after the GDPR. Interestingly, EU firms decrease their computation relative to comparable US firms by 15%—-implying that firms became less data-intensive after GDPR. These effects were more pronounced in countries with stricter enforcement policies.

Using an econometric analysis of firms' production functions, data and computation are found to be strong complements in production, with elasticities of substitution ranging from 0.44 (non-software services) to 0.34 (manufacturing). The production function analysis also suggests that GDPR increased average total data storage costs by 20%, especially for firms in the software sector (24%), followed by manufacturing (18%) and services (18%). Most notably, GDPR, costs increased disproportionately more for smaller firms.

The most recent EU Data Protection Act recognizes the differential compliance burden for small businesses (Beveridge 2024). Its requirements are lessened small and medium businesses.

A PATH TOWARDS ACCEPTABLE DATA PROCESSING

Privacy regulation steers both the data economy and firm compliance by defining what constitutes acceptable data processing. For instance, HIPAA specifies health data storage and transfer requirements between covered parties which can include encryption, de-identification, written agreements, and breach notification. COPPA restricts processing children's data, but establishes a safe harbor program for firms to coordinate self-regulation. The GDPR prioritizes privacy while imposing substantial compliance costs on firms because the GDPR defines personal data broadly, imposes multiple data-related responsibilities on firms, and prescribes a high consent standard for many marketing purposes. Forward-looking privacy regulation should consider the role of privacy-enhancing technologies in defining acceptable data processing.

PRIVACY-ENHANCING TECHNOLOGIES (PETS)

PETs promise to protect privacy while still allowing value-creating data use. PETs include diverse technologies such as adding noise to data (i.e., differential privacy), grouping consumers into cohorts (e.g., *K*-anonymity), decentralizing data processing (e.g., federated learning, on-device computation), limiting data flows (e.g., zero-knowledge proof) and privacy-safe data combination (e.g., secure multi-party computation). For example, the US Census is using differential privacy to add noise to its public statistics in order to fulfill its legal obligation to protect privacy. Google is using federated learning to implement keyboard next word predictions (Hard et al 2018). PETs may also provide solutions to the problem that one cannot police algorithmic discrimination without knowing individuals race, gender, and other sensitive data fields (Juarez and Korolova (2023).

The online advertising industry seeks to to replace cross-site/app identifiers with PETs. Google's "Privacy Sandbox" consists of multiple technologies that aim to preserve many of the benefits of cross-site/app identity in online advertising while offering superior privacy protection to consumers (Google 2022). These initiatives include technologies for ad targeting (Topics API, Protected Audience API), ad measurement (Attribution Reporting API), and fraud detection (Privacy StateTokens). Website and adtech vendor adoption of these technologies is growing (Johnson and Neumann 2024). In addition, Microsoft has proposed its own approach to privacy-centric advertising, which it calls the Ad Selection API. Facebook and Mozilla jointly proposed their Interoperable Private Attribution (IPA) approach to privacy-safe, cross-device ad measurement. Apple has already released PETs for advertisers; though these provide only basic ad measurement so far (SKAdNetwork). This new privacy-centric approach is revolutionizing how marketing practitioners approach digital advertising (Geng, Dawson, and Nair, 2023; Johnson et al., 2022; Runge and Seufert, 2021). Korganbekova and Zuber (2023) show that a privacy preserving algorithm reduces (but does not eliminiate) the tendency for privacy restrictions to differentially harm small sellers and price-sensitive consumers.

Though promising, several scholars have discussed the limitations of PETs. For insance, PETs may have competitive consequences because fewer data observations may require greater

transformation to protect individual privacy. Differential privacy (Dwork, 2006) is particularly controversial. Adding noise to data creates challenges for inference (Komarova & Nekipelov, 2020). Differential privacy may be better suited to simple applications rather than broad use (Blanco-Justicia et al. 2022, and Williams & Bowen 2023). As a consequence, many real world applications choose permissive privacy parameters that effectively sacrifice privacy for utility (Blanco-Justicia et al., 2022; Williams and Bowen, 2023). For these reasons, several scholars criticize the use of differential privacy in the US census (Hotz et al., 2022).

FORWARD-LOOKING REGULATION

Regulators are monitoring developments in PETs with interest. For instance, the British and Canadian privacy regulators released reports discussing PETs (Information Commissioners Office 2022; Office of the Privacy Commissioner of Canada 2017). The British Competition and Markets Authority (CMA) is taking a leading role in monitoring Google's Privacy Sandbox. This investigation seeks comments from stakeholders and includes a testing phase to critically examine the real-world performance of these new technologies. This regulatory oversight ensures that the privacy-centric future of digital advertising better balances industry and consumer stakeholders.

Forward-looking regulation must grapple with PETs. Though the US is considering federal privacy regulation, regulatory proposals to date (to our knowledge) omit PETs. For instance, the FTC's request for public comment on "Commercial Surveillance and Data Security" only mentions PETs in passing.

Since PETs are costly for firms to implement, forward-looking regulation should consider how to incentivize PET adoption and innovation. For instance, regulation could include appropriate PET use as a sufficient legal basis for data processing. In particular, regulation could stipulate that firms can forego costly consent collection if they employ PETs. In settings where consent plays an important role, regulation could incentivize PET adoption by permitting consent defaults that advantage data collection (e.g., opt-out rather than opt-in consent). In contrast, the French regulator CNIL has stated that the consent standard should be the same for Privacy Sandbox-enabled online advertising as third-party cookies.

CONCLUSION

Herein, we have summarized the key themes of relevant academic marketing literature which are informative for thinking about governmenent and business privacy policies. In particular, public policy needs to weigh the trade-offs between the costs and benefits to consumer data privacy restrictions. A similar balanced approach has been recommended in the past in the discussion of the trade-offs between innovation and privacy (e.g., Goldfarb and Tucker 2012).

Many current privacy policies reduce the usefulness of consumer data to both consumers and firms. In our review, these policies may impose the biggest costs on disadvantaged consumers and small businesses and entrepreneurs. On the demand side, these policies weaken personalized marketing, which can reduce value creation to consumers with non-mainstream tastes and, in some instances, exclude marginalized consumer segments. On the supply side, these regulations can stifle innovation and reduce the competitiveness of markets, especially

for small businesses and entrepreneurs. While Privacy Enhancing Technologies offer potential to reduce some of these documented costs to consumers and firms, these technologies are likely to advantage larger firms.

REFERENCES

13D Research (2017) Why CPG Goliaths have only begun their fall. What I Learned This Week. Accessed March 25, 2024. https://latest.13d.com/why-cpg-giants-have-only-begun-their-fallamazon-walmart-ecommerce-price-war-560c1d9e7b7a.

Acquisti A (2023) The economics of privacy at a crossroads. In The Economics of Privacy, Goldfarb A, Tucker C (eds). University of Chicago Press and NBER.

Acquisti A, Brandimarte L, Hancock J (2022) How privacy's past may shape its future. *Science*. 375(6578):270–272.

Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. *Journal of Economic Literature*. 54(2):442–492.

Adjerid I, Acquisti A, Telang R, Padman R, Adler-Milstein J (2016) The impact of privacy regulation and technology incentives: the case of health information exchanges. *Management Science*. 62(4):1042–1063.

Agrawal A, Gans J, Goldfarb A (2019) Economic policy for artificial intelligence. In: Lerner J, Stern S, eds. Innovation Policy and the Economy. Vol 19.

Ajzen I, Fishbein M, Lohmann S, Albarracín D (2018) The influence of attitudes on behavior. *The handbook of attitudes, volume 1: Basic principles*. Oct 10:197-255.

Alba J, Lynch, J, Weitz B, Janiszewski C, Lutz R, Sawyer A, Wood S (1997) Interactive home shopping: Consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *Journal of Marketing*. 61 (July), 38-53

Ali M, Sapiezynski P, Bogen M, Korolova A, Mislove A, Rieke A (2019) Discrimination through optimization: How Facebook's ad delivery can lead to biased outcomes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1-30.

Allcott H, Diamond R, Dubé JP, Handbury J, Rahkovsky I, Schnell M (2019) Food deserts and the causes of nutritional inequality. *Quarterly Journal of Economics*. 134(4):1793–1844.

Altman, I. (1977) Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3): 66-84.

Anderson, C (2006) *The Long Tail: Why the Future of Business Is Selling Less of More*. New York: Hyperion.

Angwin C, Mattu S, Larson J(2015), Test prep is more expensive – for Asian students. *The Atlantic*, September 3, 2015. https://www.theatlantic.com/education/archive/2015/09/princeton-review-expensive-asian-students/403510/

Arbanas J, Silverglate PH, Hupfner S, Loucks J, Raman P, Steinhart M (2023), Data privacy and security worries are on the rise, while trust is down. *Deloitte's Connected Consumer Survey 2023*, accessed at https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html on 3-25-2024

Arslan HA, Tereyağoğlu N, Yılmaz Ö (2023) Scoring a touchdown with variable pricing: Evidence from a quasi-experiment in the NFL ticket markets. *Management Science* 69(8):4435-56.

Ascarza E, Israeli A (2022) Eliminating unintended bias in personalized policies using bias-eliminating adapted trees (BEAT). *Proceedings of the National Academy of Sciences*. 119(11).

Asplund, John (2024) VillageMD facing privacy lawsuit over use of Meta's 'Pixels', *Crain's Chicago*, April 11, 2024. Accessed at https://www.chicagobusiness.com/health-pulse/villagemd-facing-privacy-lawsuit-over-use-metas-pixels?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter-Health-BreakingNews-20240411 on April 11, 2024.

Auxier B, Rainie L, Anderson M, Perrin A, Kumar M, Turner E (2019) Americans and privacy: Concerned, confused and feeling lack of control over their personal information," *Pew Research Center,* Nov. 15, 2019. Accessed at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ on 3-25-2024.

Bain JS (1954) Conditions of entry and the emergence of monopoly. In *Monopoly and Competition and Their Regulation*, E. H. Chamberlin, ed. (London: Macmillan, 1954), 215-41.

Bairathi M, Lambrecht A, Zhang X (2023). Gender Disparity in Online Reputation: Evidence from an Online Freelance Platform. Working paper.

Bakos Y, Marotta-Wurgler F, Trossen DR (2014) Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies* 43(1):1-35.

Bergemann D, Brooks B, Morris S (2015). The limits of price discrimination. *American Economic Review*. 105(3):921–957.

Bergemann D, Brooks B, Morris S (2023) "On the alignment of consumer surplus and total surplus under competitive price discrimination," Yale University Working Paper.

Bettman JR, Luce MF, Payne JW (1998) Constructive consumer choice processes. *Journal of consumer research*, 25(3):187-217.

Beveridge, C (2024) European data act – key provisions and their implications. March 13, 2024 blog post. Available at https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/european-data-act-key-provisions-and-their-implications#

Biden, Joseph R. (2023). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. October 30, 2023. Available at link.

Blanco-Justicia A, Sánchez D, Domingo-Ferrer J, Muralidhar K (2022) A critical review on the use (and misuse) of differential privacy in machine learning. *ACM Computing Surveys*. 55(8):1—16.

Blattner L, Nelson S (2021) How costly is noise? Data and disparities in consumer credit. arXiv preprint arXiv:2105.07554. 2021 May 17.

Bleier A, Goldfarb A, Tucker C (2020) Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*. 7(3):466-80.

Bogen M, Rieke A, Ahmed S (2020) Awareness in practice: tensions in access to sensitive attribute data for antidiscrimination. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, Jan 27 2020 (pp. 492-500).

Borner P (2022) Consent fatigue. Blog post, The Data Privacy Group, June 13, 2022, available at link.

Bronnenberg BJ, Dhar SK, Dubé JP (2009) Brand history, geography, and the persistence of brand shares. *Journal of Political Economy* 117(1):87-115.

Bronnenberg BJ, Dubé JP, Joo J (2022), "Millennials and the takeoff of craft brands: Preference formation in the U.S. beer industry," *Marketing Science* 41(4):710-732. https://doi.org/10.1287/mksc.2022.1371

Buckman JR, Adjerid I, Tucker C (2023) Privacy regulation and barriers to public health. Management Science. 69(1):342-50.

Caves RE, Porter ME (1977) From entry barriers to mobility barriers: Conjectural decisions and contrived deterrence to new competition*. *The Quarterly Journal of Economics*, *91*(2), 241–261. https://doi.org/10.2307/1885416

Chin A, Beckett DH (2021) Don't watch me read: How mere presence and mandatory waiting periods affect consumer attention to disclosures. *Behavioural Public Policy*. ;5(2):202-21.

Civil Rights Litigation Clearinghouse (2022), "Resource: Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising, June 21, 2022, available at https://clearinghouse.net/resource/3807/

Clark, C (2020) How "notice and consent" fails to protect our privacy. New America blog post, March 23, 2020, available at link.

ColorOfChange (2021) A Framework for Combating Race-Based Online Harms: Anti-Racism in the Digital Economy. Color Of Change, June 2021. Accessed January 4, 2024. https://colorofchange.org/wp-content/uploads/2021/06/FINAL-BTS-Tech-Framework.pdf.

Competition and Markets Authority (2021) Mobile ecosystems market study: Appendix I considering the design and impacts of competition on Apples ATT changes. December 14, 2021 https://assets.publishing.service.gov.uk/media/61b86aeb8fa8f5037778c3b8/Appendix_I_-_Considering_the_impacts_of_Apples_ATT.pdf

Consumer Financial Protection Bureau (2022a) Hold credit reporting companies accountable for incorrect reports and shoddy service. January 5, 2022. Link

Consumer Financial Protection Bureau (2022b) CFPB targets unfair discrimination in consumer finance. March 16, 2022. Link

Consumer Financial Protection Bureau (2023) 12 CFR Parts 1001 and 1033 [Docket No. CFPB-2023-0052] RIN 3170-AA78 Required Rulemaking on Personal Financial Data Rights https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf

Cookie Pro Knowledgebase (2021) "Tracking Pixel." Accessed March 26, 2024. https://www.cookiepro.com/knowledge/tracking-pixel/#:~:text=A%20tracking%20pixel%2C%20also%20known,from%20banner%20ads%20to%20emails.

Council of Economic Advisors (2014) Big data: Seizing opportunities, preserving values. Report, Council Econ. Advisors, Washington, DC., p.65. Accessed at https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

Council of Economic Advisors (2015) Big data and differential pricing." Report, Council Econ. Advisors, Washington, DC. February 2015 https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf

Cramer-Flood E (2023) Meta's ad revenue share vastly exceeds its share of consumer time. eMarketer, July 28, 2023. https://www.emarketer.com/content/meta-s-ad-revenue-share-vastly-exceeds-its-share-of-consumer-time.

Dalmia M and Diehl K (2024) Privacy is important, but is it thought about? USC Marshall School of Business Research Paper Sponsored by iORB, No. Forthcoming, Available at SSRN: https://ssrn.com/abstract=4796954

Datta H, Knox G, Bronnenberg B (2018) Changing their tune: How consumers' adoption of online streaming affects music consumption and discovery. *Marketing Science*. 37(1):5-21.

Deaton AS, Paxson C (2001) Mortality, education, income, and inequality among American cohorts. In *Themes in the Economics of* Aging pp. 129-170. University of Chicago Press.

DellaVigna S, Gentzkow M (2019) Uniform pricing in us retail chains. *The Quarterly Journal of Economics*. 134(4):2011-2084.

Demirer M, Hernández DJ, Li D, Peng S. (2024) Data, privacy laws and firm production: Evidence from the GDPR. National Bureau of Economic Research; (No. w32146). Available at https://www.nber.org/system/files/working_papers/w32146/w32146.pdf

Derksen L, McGahan A, Pongeluppe L (2022) Privacy at what cost? Using electronic medical records to recover lapsed patients into HIV care. In *NBER Workshop on the Economics of Privacy* 2022 Mar 19.

Dubé JP, Misra S (2023) Personalized pricing and consumer welfare. *Journal of Political Economy*. 131(1):131-89.

Dwork C (2006). Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, Languages and Programming* (pp. 1—12). Berlin, Heidelberg: Springer Berlin Heidelberg.

Editorial Board (2022) "Breaking Big Tech Bad: A Senate antitrust bill would harm consumers and U.S. innovation." Wall Street Journal, June 5, 2022. https://www.wsj.com/articles/breaking-big-tech-bad-senate-judiciary-committee-bipartisan-antitrust-bill-facebook-meta-google-twitter-11654113174. Accessed March 25, 2024.

eMarketer Editors (2019) CPG industry struggles to find growth—eMarketer trends, forecasts & statistics. eMarketer, February 12, 2019.

Faverio M (2023), "Key findings about Americans and data privacy," *Pew Research Center,* Oct. 18 2023, accessed at https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/ on 3-25-2024.

Feldman JM, Lynch JG (1988) Self-generated validity and other effects of measurement on belief, attitude, intention, and behavior. *Journal of Applied Psychology*. 73(3):421-435.

Freedman S, Jin G (2017). The information value of online social networks: Lessons from peer-to-peer lending. *International Journal of Industrial Organization.* 2017, 1;51:185-222.

Fudenberg D, Villas-Boas JM (2006) Behavior-based price discrimination and customer recognition. *Handbook on Economics and Information Systems*, 1, pp.377-436.

GDPR (2020) General Data Protection Regulation. https://gdpr.eu/tag/gdpr/

Geng, T., Dawson, M., & Nair, H. (2023). Effectively Combining the Event and Aggregate Summary Reports from the Privacy Sandbox Attribution Reporting API for Improving Ad-Measurement Fidelity. Technical report, Google Ads.

Glenn B, Dubé JP, Kavanagh SC (2022) Segmented pricing for fines and fees. GFOA, January 27, 2022.

Goldfarb A, Que VF (2023) The economics of digital privacy. *Annual Review of Economics*. 15:267-86.

Goldfarb A, Tucker C (2011) Privacy regulation and online advertising. *Management Science*. 57(1):57-71.

Goldfarb A, Tucker C (2012) Privacy and innovation. In *Innovation Policy and the Economy*. Vol 12. Eds. Lerner J, Stern S. NBER, University of Chicago Press, 65-90.

Goldfarb A, Tucker C. (2017) Inequality, privacy and digital market design. Chapter in *Fair by Design,* Eds. Scott Kominers and Alex Teytelboym, Oxford University Press.

Google (2022). The privacy sandbox: technology for a more private web. https://privacysandbox.com.

Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, Eichner H, Kiddon C, Ramage D (2018) Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604. 2018 Nov 8.

Hart OD, Tirole J (1988) Contract renegotiation and Coasian dynamics. *The Review of Economic Studies*. 55(4):509-40

Hotz VJ, Bollinger CR, Komarova T, Manski CF, Moffitt RA, Nekipelov D, Sojourner A, Spencer BD (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 (2022) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. In Privacy-enhancing technologies (PETs) chapter 5. Information Commissioner's Office.

Janssen R, Kesler R, Kummer ME, Waldfogel J (2022) GDPR and the lost generation of innovative apps. NBER Work. Pap. 30028.

Jia J, Jin GZ, Wagman L (2021) The short-run effects of the general data protection regulation on technology venture investment. *Marketing Science*. 40(4):661–684.

Joseph S. (2024) Google delays third-party cookies demise yet again. *Digiday*, April 23, 2024. https://digiday.com/marketing/google-delays-third-party-cookie-demise-yet-again/. Accessed April 24, 2024.

Johnson, EJ, Bellman S, Lohse GL (2002) Defaults, framing and privacy: Why opting in-opting out, *Marketing Letters,* 13 (1), 5–15.

Johnson GA (2023) Economic research on privacy regulation: Lessons from the GDPR and beyond. In Economics of Privacy chapter 4. Eds. Goldfarb A, Tucker C. University of Chicago Press.

Johnson GA, Lin T, Cooper J, Zhong L (2023) COPPAcalypse? The YouTube settlement's impact on kids content. Available at SSRN 4430334.

Johnson GA, Neumann N (2024) The advent of privacy-centric digital advertising: Tracing privacy-enhancing technology adoption. https://pep.gmu.edu/wp-content/uploads/sites/28/2024/04/Johnson-Neumann.pdf

Johnson GA, Runge J, Seufert E (2022) Privacy-centric digital advertising: Implications for research. *Customer Needs and Solutions*. 9(1):49—54.

Johnson GA, Shriver SK, Du S (2020) Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science*. 39(1):33—51.

Johnson GA, Shriver SK, Goldberg SG (2023) Privacy and market concentration: intended and unintended consequences of the GDPR. *Management Science*. 69 (10): 5695-5721.

Juarez M, Korolova A. (2023) You can't fix what you can't measure": Privately measuring demographic performance disparities in federated learning. In Workshop on Algorithmic Fairness through the Lens of Causality and Privacy 2023 Jun 4 (pp. 67-85). PMLR.

Kaplan L, Mislove A, Sapieżyński P (2017) Measuring Biases in a Data Broker's Coverage. FTC Conference, July 2017. Accessed at Link on 3-26-2024.

Kesler R (2023) The Impact of Apple's App Tracking Transparency on App Monetization. Available at SSRN: Link.

Kerrigan, K., and R. Keating (2019) "Online Advertising Delivers BIG Benefits for Small Businesses." SBE Council, September 10, 2019. https://sbecouncil.org/2019/09/10/online-advertising-delivers-big-benefits-for-small-businesses/. Accessed March 25, 2024.

King J, Ho D, Gupta A, Wu V, Webley-Brown H (2023) The Privacy-Bias Tradeoff: Data Minimization and Racial Disparity Assessments in US Government. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* 2023 Jun 12 (pp. 492-505).

Kircher T, Foerderer J (2023a) Ban targeted advertising in apps? an empirical investigation of the consequences for app development. *Management Science*, (pp. to appear).

Kircher T, Foerderer J (2023b) Does privacy undermine content provision and consumption? evidence from educational YouTube channels. SSRN working paper.

Komarova T, Nekipelov D (2020) Identification and formal privacy guarantees. arXiv preprint arXiv:2006.14732.

Korganbekova M, Zuber C (2023) Balancing user privacy and personalization. Northwestern University Working Pape, October 8, 2023.

Lambrecht A, Seim K, Tucker C (2011) Stuck in the adoption funnel: The effect of interruptions in the adoption process on usage. *Marketing Science* 30(2):355-367. https://doi.org/10.1287/mksc.1100.0613

Lambrecht A, Tucker C (2019) Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads. *Management Science*. 65(7):2966-2981.

Lambrecht A, Tucker C (2024) Apparent algorithmic discrimination and real-time algorithmic learning in digital search advertising (April 1, 2024). Available at SSRN: https://ssrn.com/abstract=3570076 or http://dx.doi.org/10.2139/ssrn.3570076

Larson RB (2023). Privacy concerns and social desirability bias. *International Journal of Market Research*, 0(0). https://doi.org/10.1177/14707853231222810

Lee JY, Yang J, Anderson E (in press) Using grocery data for credit decisions. *Management Science*, forthcoming.

Lin T (2022) 'Valuing intrinsic and instrumental preferences for privacy'. *Marketing Science* 41(4):663–681.

Lin T, Misra S (2022) Frontiers: the identity fragmentation bias. *Marketing Science*. 41(3):433-440.

Lin T, Strulov-Shlain A (2023) 'Choice architecture, privacy valuations, and selection bias in consumer data'. *University of Chicago, Becker Friedman Institute for Economics Working Paper* (2023-58).

Ma M., Gutiérrez DE, Frausto JM, Al-Delaimy WK (2021), Minority representation in clinical trials in the United States: trends over the past 25 years. In *Mayo Clinic Proceedings*, Vol. 96, Elsevier, pp. 264–266.

Mearian L (2015) Insurance company now offers discounts — if you let it track your Fitbit. Computerworld, April 17, 2015, https://www.computerworld.com/article/1362502/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html

Miller AR, Tucker C (2009) Privacy protection and technology diffusion: The case of electronic medical records. *Management Science* 55(7):1077-1093.

Miller AR, Tucker CE (2011) Can health care information technology save babies? *J. Political Econ.* 119(2):289–324.

Miller AR, Tucker CE (2018) Privacy protection, personalized medicine, and genetic testing. *Management Science* 64(10):4648-4668. https://doi.org/10.1287/mnsc.2017.2858

Misra S (2020) "Algorithmic nudges," *University of Chicago Working Paper*.

Mohammed R (2017) How retailers use personalized prices to test what you're willing to pay. Harvard Bus. Rev., October 20, 2017,.

Moorthy S, Ratchford BT, Talukdar D (1997) Consumer information search revisited: Theory and empirical analysis. *Journal of Consumer Research*. 23(4):263-77.

Mrkva K, Posner NA, Reeck C, Johnson EJ (2021) Do nudges reduce disparities? Choice architecture compensates for low consumer knowledge. *Journal of Marketing*. 85(4):67-84.

Neumann N, Tucker CE, Kaplan L, Mislove A, Sapiezynski P (2024) Data deserts and black boxes: The impact of socio-economic status on consumer profiling. Forthcoming *Management Science*.

Netzer O, Lemaire A, Herzenstein M (2019(When words sweat: Iden*tifying signals for loan default in the text of loan applications.* Journal of Marketing Research. (6):960-980.

Ng A (2022) 'A uniquely dangerous tool': How Google's data can help states track abortions. *Politico,* July 18, 2022, https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906

Nissenbaum H (2004) Privacy as contextual integrity. *Wash. Law Rev.* 79(1):119–57

Office of the Privacy Commissioner of Canada (2017). *Privacy Enhancing Technologies — A Review of Tools and Techniques*. Technical report, Office of the Privacy Commissioner of Canada.

Ohm, P., (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law. Rev., 57, p.1701.

Peukert C, Bechtold S, Batikas M, Kretschmer T (2022) Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*. 41(4):746-68.

Ramasastry A (2005) Websites that charge different customers different prices: Is their 'price customization' illegal? Should it be? *FindLaw*, June 20. https://supreme.findlaw.com/legal-commentary/websites-that-charge-different-customers-different-prices.html

Rossi PE, McCulloch RE, Allenby GM (1996) *The value of purchase history data in target marketing*. *Marketing Science*. 15(4):321-40.

Runge J, Seufert E (2021) Apple is changing how digital ads work. are advertisers prepared? *Harvard Business Review*.

Schmalensee R (1982) Product differentiation advantages of pioneering brands. *American Economic Review* 72(3):349-65.

Schwarz N (1999) Self-reports: How the questions shape the answers. *American psychologist*, 54(2):93.

Simmons CJ, Bickart BA, Lynch JG (1993) Capturing and creating public opinion in survey research, *Journal of Consumer Research*, 20(2): 316–329, https://doi.org/10.1086/209352

Spiekermann S, Grossklags J, Berendt B (2001) E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior. In EC '01: *Proceedings of the 3rd ACM Conference on Electronic Commerce* 38(45):38–39.

Stole LA (2007) "Price Discrimination and Imperfect Competition." In *Handbook of Industrial Organization*, vol. 3, edited by Armstrong M, Porter RH, 2221–2299. Amsterdam: North-Holland.

Sun T, Yuan Z, Li C, Zhang K, Xu J (2023) The value of personal data in internet commerce: A high-stakes field experiment on data regulation policy. *Management Science*. https://doi.org/10.1287/mnsc.2023.4828

Sunstein C (2019), *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press).

Sutton J (1991) *Sunk costs and market structure: Price competition, advertising, and the evolution of concentration*. MIT Press.

Thaler RH, Sunstein CR (2021) *Nudge: The Final Edition.* Yale University Press.

Tucker C (2022) "The economics of privacy: An agenda." *Economics of Privacy*. University of Chicago Press.

Tucker C (2023) "Algorithmic exclusion: The fragility of algorithms to sparse and missing data." *Brookings. Center on Regulation and Markets at Brookings*. 1-26.

Useem, J (2017) How online shopping makes suckers of us all." Atlantic, May 15. https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/

Utz C, Degeling M, Fahl S, Schaub F, Holz T (2019) (un)informed consent: Studying gdpr consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 973–990.

United States Government Accountability Office (2022). Consumer data: Increasing use poses risks to privacy," Sept. 13, 2022, accessed at https://www.gao.gov/products/gao-22-106096 on 3-25-2024

Varian HR (1989) "Price Discrimination." In *Handbook of Industrial Organization*, vol. 1, edited by Schmalensee R, Willig R, 597–654. Amsterdam: NorthHolland.

Varian H, Wallenberg F, Woroch W (2005) 2005. The demographics of the do-not-call list [security of data]. *IEEE Security & Privacy*, 3(1): 34-39.

Vogels E (2021) Digital divide persists even as Americans with lower incomes make gains in tech adoption. Pew Research Center, June 22, 2021. https://www.pewresearch.org/short-reads/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/

Wachter, S (2020), Affinity profiling and discrimination by association in online behavioral advertising. *Berkeley Technology Law Journal* 35 (2):367-430.

Wernerfelt N, Tuchmann A, Shapiro B, Moakler R A (2024) Estimating the Value of Offsite Data to Advertisers: Evidence from Meta. *Northwestern University Working Paper*.

Wilkinson-Ryan T (2017) The perverse consequences of disclosing standard terms. *Cornell Law Review*, 103:117.

Williams AR, Bowen CM (2023) The promise and limitations of formal privacy. *WIREs Computational Statistics*, (pp. e1615).

Zafar, F (2023) 18 countries with GDPR-like data privacy laws. Yahoo! Finance, September 14, 2023. https://finance.yahoo.com/news/18-countries-gdpr-data-privacy-121428321.html. Accessed March 25, 2024.

Zhang W (2024) Optimal comprehensible targeting. University of Chicago Booth School Working Paper. https://walterwzhang.github.io/research/jmp

* AUTHOR NOTE

Jean-Pierre Dubé, is James M. Kilts Distinguished Service Professor of Marketing and Charles E. Merrill Faculty Scholar at the Booth School of Business at the University of Chicago and corresponding author, email Jean-Pierre.Dube@chicagobooth.edu. Dirk Bergemann is Douglass and Marion Campbell Professor of Economics at Yale University. Ford Foundation International Career Development Assistant Professor at MIT's Sloan School of Management. Mert Demirer is the Ford Foundation International Career Development Assistant Professor and an Assistant Professor of Applied Economics at the MIT Sloan School of Management. Avi Goldfarb is the Rotman Chair in Artificial Intelligence and Healthcare and a professor of marketing at the Rotman School of Management, University of Toronto. Garrett Johnson is Assistant Professor of Marketing at Boston University's Questrom School of Business. Anja Lambrecht is Professor of Marketing at the London Business School. Tesary Lin is Assistant Professor of Marketing at Boston University's Questrom School of Business. Anna Tuchmann is Associate Professor of Marketing at Northwestern University's Kellogg Graduate School of Management. Catherine Tucker is the Sloan Distinguished Professor of Management at MIT Sloan. John G. Lynch is University of Colorado Distinguished Professor at the Leeds School of Business at the University of Colorado Boulder, and Executive Director of the nonprofit Marketing Science Institute.

MSI convened this group to consolidate key conclusions emerging from an expanding body of academic research studying effects of privacy regulations on marketing firms and on consumers. The aim of this paper is to inform delberations and decisions of technology platforms, digital marketing firms, and regulators. The authors thank the participants of a Marketing Science Institute / Brookings Institution workshop on intended and unintended effects of privacy regulation, including speakers Sanjay Paitnik, Tom Wheeler, and Alessandro Acquisti and the members of the audience who participated in the discussion. The views expressed are those of the authors and do not represent the views of the Brookings Institution or other workshop participants.

THE MARKETING SCIENCE INSTITUTE

A member-supported nonprofit founded in 1961, MSI bridges leaders in industry and academia to stimulate, support, and disseminate academic research that advances the scientific practice of marketing.