FTC Hearings on Competition & Consumer Protection in the 21st Century

FTC Project No. P181201

Comments of the International Center for Law & Economics

Topic 12: Consumer Privacy

May 31, 2019

Authored by:

Geoffrey A. Manne (President & Founder, International Center for Law & Economics)

Kristian Stout (Associate Director, International Center for Law & Economics)

Dirk Auer (Senior Fellow, International Center for Law & Economics)

Alec Stapp (Research Fellow, International Center for Law & Economics)

I. Introduction

Digital privacy and data security are important ongoing concerns for lawmakers, particularly in light of recent, high-profile data breaches and allegations of data misuse. Understandably, in the wake of such incidents advocates regularly call for tighter restrictions on data collection and use. But, as we detail below, privacy is a highly complex topic comprising a wide variety of differing, and often conflicting, consumer preferences. While undoubtedly in need of ongoing assessment in the face of new challenges, the US federal government's sectoral, tailored model of privacy regulation remains the soundest method of regulating privacy.

Although the US does not have a single, omnibus, privacy regulation, this does not mean that the US does not have "privacy law." In the US, there already exist generally applicable laws at both the federal and state level that provide a wide scope of protection for individuals, including consumer protection laws that apply to companies' data use and security practices,[1] as well as those that have been developed in common law (property, contract, and tort) and criminal codes.[2] In addition, there are specific regulations pertaining to certain kinds of information, such as medical records, personal information collected online from children, credit reporting, as well as the use of data in a manner that might lead to certain kinds of illegal discrimination.[3]

Before engaging in a deeply interventionist regulatory experiment—such as intervening in the design of algorithms or imposing strict privacy regulations in contravention to revealed consumer preferences—there should be empirically justifiable reasons for doing so; in the language of economics, there should be demonstrable market failures

---

[1] *See, e.g.*, FTC Act, 15 U.S.C. § 45(a) et seq.

[2] PRIVACY-COMMON LAW, http://law.jrank.org/pages/9409/Privacy-Common-Law.html (last visited May 30, 2019).

[3] *See* Comments of the Association of National Advertisers on the Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, *available at* https://docplayer.net/93116976-Before-the-federal-trade-commission-washington-d-c-comments-of-the-association-of-national-advertisers-on-the.html. As the Association of National Advertisers notes:

> [T]he Health Information Portability and Accountability Act ("HIPAA") regulates certain health data; the Fair Credit Reporting Act ("FCRA") regulates the use of consumer data for eligibility purposes; the Children's Online Privacy Protection Act ("COPPA") addresses personal information collected online from children; and the Gramm–Leach–Bliley Act ("GLBA") focuses on consumers' financial privacy; the Equal Employment Opportunity Commission ("EEOC") enforces a variety of anti-discrimination laws in the workplace including the Pregnancy Discrimination Act ("PDA") and American with Disabilities Act ("ADA"); the Fair Housing Act ("FHA") protects against discrimination in housing; and the Equal Credit Opportunity Act ("ECOA") protects against discrimination in mortgage and other forms of lending.

Id. at 6.

in the provision of "privacy" (however we define that term), before centralized regulation co-opts the voluntary choices of consumers and firms in the economy.

It surely might be the case that some consumers, abstractly speaking, would prefer one-hundred percent perfect privacy and security. It is also a certainty that, faced with tradeoffs—including the price of services, the number of features, the pace of innovation, ease of use and convenience—consumers are willing to settle for some lesser degree of privacy and security.

The responsibility of lawmakers who wish to write rules that optimize that set of tradeoffs is two-fold. First, there must be a demonstration that actual failures to provide optimal privacy and security exist, *relative to consumers' revealed preferences.* Second, there must also be a demonstration that new legislation will not introduce new costs that dwarf the value they are designed to create.

As we detail below, the available evidence suggests that, at least at this time, there is no demonstrable failure in the market's provision of privacy protection or the existing legal regime's ability to regulate it. Moreover, the experimental and theoretical literature also demonstrates that many of the proposed regulatory interventions are at best useless, and at worst destructive.

Getting regulation right is always difficult, but it is all the more so when confronting evolving technology, inconsistent and heterogeneous consumer demand, and intertwined economic effects that operate along multiple dimensions—all conditions that confront online privacy regulation:

> [S]ecuring a solution that increases social welfare[] isn't straightforward as a practical matter. From the consumer's side, the solution needs to account for the benefits that consumers receive from content and services and the benefits of targeting ads, as well as the costs they incur from giving up data they would prefer to keep private. Then from the ad platform's side, the solution needs to account for the investments the platform is making in providing content and the risk that consumers will attempt to free ride on those investments without providing any compensation—in the form of attention or data—in return. Finally, the solution must account for the costs incurred by both consumers and the ad platform including the costs of acquiring information necessary for making efficient decisions.[4]

---

[4] David S. Evans, *Mobile Advertising: Economics, Evolution and Policy* at 45 (June 1, 2016), *available at* http://ssrn.com/abstract=2786123.

Given the complications confronting privacy regulation, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Commission has historically taken, and which has, generally, yielded a stable, evenly administered regime: case-by-case examination of actual privacy harms and a minimalist approach to ex ante, proscriptive or prescriptive regulations, coupled with narrow legislation targeted at unambiguously problematic uses of personal information. Following this approach will allow authorities to balance flexibility and protection.

This approach to privacy protection matches the United States' historic preference for light-touch regulation when dealing with highly dynamic markets. The Internet in the United States grew up around an ethos of "permissionless innovation"[5] in which firms were free to experiment with business models and service offerings, and consumers were essentially free to interact with those services they found valuable relative to the costs, both in terms of money and, relevant here, in terms of personal data.

This environment has been and continues to be essentially based on "opt-out." Many (if not most) services on the Internet are offered on the basis that user data can, within certain limits, be used by a firm to enhance its services and support its business model, thereby generating benefits to users. To varying degrees (and with varying degrees of granularity), services offer consumers the opportunity to opt-out of this consent to the use of their data, although in some cases the only way effectively to opt-out is to refrain from using a service at all. Over time online services have generally increased the extent of user control over the use of user data, and the type of controls have evolved as both technology and consumer preferences have changed. This trend appears to mirror general consumer preferences with respect to privacy,[6] and this evolution of business practice has concomitantly shaped user expectations regarding privacy online.[7]

---

[5] *See* A. THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (Mercatus Center George Mason University. 2016).

[6] *See* Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, 102 AM. ECON. REV. PAPERS & PROCEEDINGS 349 (2012) (Reporting the results of empirical research demonstrating that: "(1) Refusals to reveal information have risen over time, and (2) Older people are much less likely to reveal information than are younger people. Our data further suggest that though younger respondents have become somewhat more private over time, the gap between younger and older people is widening").

[7] *See* Adam Thierer, Public Interest Comment on Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change (Arlington, VA: Mercatus Center at George Mason University 2011) at 25 (listing a number of areas where competition between firms has spurred privacy protection).

The Commission has generally evidenced admirable restraint and assessed the relevant trade-offs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of ex ante privacy principles across industries is a fraught exercise as each industry—indeed each firm within an industry—faces a different set of consumer expectations about its provision of innovative services and offering of privacy protections.

This background reality does not mean that privacy practices and their regulation should never be debated, nor that a more prescriptive regime should never be considered. But any such efforts must begin with the collective wisdom of the agencies, scholars, and policy makers that have been operating in this space for decades, and with a deep understanding of the business realities and consumer welfare effects involved.

II. Privacy regulation, market failures, and regulatory restraint

In evaluating the contours of possible privacy legislation, it is crucial first to ask why—and even whether—such legislation is needed. And before imposing regulatory burdens it is crucial to question the underlying merits of politicized claims and political movements that may purport to represent overwhelming consumer interests but that may, in fact, do nothing of the sort.

Thus a vital question in the privacy protection space is whether and why markets operating without specific privacy regulation lead to a sub-optimal provision of privacy protection. Without starting with this inquiry, it is unclear what problems rules are needed to address; and without knowing its purpose, any rules are likely to be ineffective, at best, and may in fact make things worse, by increasing costs for consumers and businesses alike, mandating harmful prescriptions for alleged privacy harms, or exacerbating the risks of harm—or all of the above.

Particularly in the US, where privacy is treated both legally and socially as more of a consumer preference (albeit perhaps a particularly important one) than a fundamental right,[8] it is difficult to determine whether our current regime produces the "right" amount of privacy protection. It is not enough that advocates and particularly privacy-sensitive consumers think there should be more, nor is it enough that there have

[8] Except, of course, where it comes to *government* access to private information, e.g., under the Fourth Amendment. *See supra* notes 10-12 and accompanying text.

been some well-publicized violations of privacy. Indeed, the fact that revealed preferences in the market tend toward relatively *less* privacy protection is evidence that advocates (and some legislators) may be seeking to create privacy protection for which there is simply no demand, beyond their own idiosyncratic preferences. Absent a pervasive defect that suggests a broad disconnect between revealed and *actual* preferences,[9] and given the costs, we should be extremely cautious about adopting more invasive regulation.

With this in mind, it is important to look at the purported market failures that have been put forward to justify the adoption of privacy regulations. Doing so offers a hint as to whether privacy regulation is filling critical gaps in the market or whether, instead, certain elements of privacy regulation are white elephants that may cost more to society than the limited benefits they bring.

A. The conditions that potentially justify privacy regulation and the likelihood of their occurrence

1. Information asymmetry

One potential privacy failure stems from the fact that consumers may be insufficiently informed about firms' use of their personal information and about the potential risks that this entails. If this were the case, we would likely expect to see either or both of the following scenarios unfolding: (a) services offering relatively higher levels of privacy protection exit the market because of adverse selection; or (b) consumers offering "too much" private information because they underprice the costs associated with sharing data. Both of these outcomes are unlikely to occur in practice.

The notion that information asymmetries can lead to a "market for lemons" in which only lower quality goods or services are offered for sale was famously formalized by George Akerlof in his Nobel-winning article.[10] Akerlof argued that when products vary in quality but buyers are unable to ascertain the quality of a good before they make a purchase, potential sellers of higher quality goods will be unable to capture their investment in quality. As a result, such sellers will exit the market (or never enter) and the average quality of goods on the market will be lower than would be the case if buyers could ascertain quality in advance.

---

[9] And some of these have indeed been suggested, as we discuss in this section, *infra*.

[10] *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970).

This phenomenon is generally referred to as "adverse selection." The underlying intuition is that, because buyers cannot ascertain a good's actual quality, their reserve price is based on its expected quality. This discourages firms from selling high quality goods because they cannot obtain superior revenue from them. In turn, this further decreases the average quality of the goods that are sold. This has a knock-on effect on the price that consumers are willing to pay and the pool of goods that is sold.

Some authors have recently voiced concerns that something similar might be occurring in the case of personal data.[11] They argue that consumers are unable to ascertain the quality of a firms' privacy policy *ex ante*. As a result, firms may have insufficient incentives to introduce consumer-friendly policies.[12]

There are problems with this story, however. First and foremost, firms' privacy policies are generally hidden in plain sight. For users that really care about privacy, all the information they require is readily available. And it is hardly any more of a secret when firms change their privacy policies: experts pay attention to these changes, summarize them, and pass them through to consumers in more easily digestible formats. A recent example of this phenomenon occurred when the EU's General Data Protection Regulation (GDPR) go-live date was approaching, and articles about privacy policy updates abounded.[13]

But even less obvious privacy policy changes have previously garnered popular attention. Electronic Frontier Foundation, a digital rights advocacy organization, has tracked changes to Facebook's privacy policy for years, to take one example.[14] And in response to this scrutiny, Facebook has made changes over the years to accommodate user concerns.[15] Of course, Facebook has also made other mistakes in its handling of user data—Cambridge Analytica, to take one recent example—but even in that case,

---

[11] *See, e.g.,* Tony Vila, Rachel Greenstadt & David Molnar, *Why We Can't Be Bothered to Read Privacy Policies*, ECONOMICS OF INFORMATION SECURITY 143 (2004).

[12] *Id.*

[13] *See, e.g.*, Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED, May 24, 2018, *available at* https://www.wired.com/story/how-gdpr-affects-you/.

[14] *See, e.g.*, Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUNDATION, Apr. 28, 2010, *available at* https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly; https://www.eff.org/deeplinks/2010/04/facebook-timeline; Kurt Opsahl & Rainey Reitman, *The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads*, ELECTRONIC FRONTIER FOUNDATION, Apr. 22, 2013, *available at* https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads.

[15] Juliette Garside, *Facebook Bows to Pressure on Privacy Setting for New Users*, THE GUARDIAN, May 22, 2014, *available at* https://www.theguardian.com/technology/2014/may/22/facebook-privacy-settings-changes-users.

the failures that occurred were discovered after the company had *already* changed the way it altered data in order to alleviate user concerns.

To the extent that consumers actually care about the privacy of their information, and short of fraud or deception (both of which are addressed by existing tort, consumer protection, and criminal laws), they are able to find out what policies apply to their information and to take steps to mitigate if needed. In some cases this means simply refusing to interact with a service that offers an insufficient take-it-or-leave it privacy policy. Indeed if concern for privacy is sufficiently strong, even a mere *lack* of information about a services' policies can induce users to exit the market, thus pushing against the market for lemons.

In other cases, however, the reality of consumer knowledge means simply employing the widely available self-help tools that address most users' concerns. Most users "pay" for online services by having their data collected and then seeing targeted ads or having that information sold for other uses. Those who wish to avoid such data collection or use must generally pay for the products directly, but often they have options to do just that. Among other things, those consumers can generally pay by purchasing services that don't collect or use data in objectionable ways (for example, self-hosted or other paid email services instead of Gmail) or by using services that may have lower quality or other, different characteristics, but that don't collect data (for example, search engines that don't collect data but may not be as effective as those that do). Similarly, there are a number of third-party mechanisms (like ad-block applications, VPNs, or incognito browsing) that can minimize the exposure of data at some cost to underlying product functionality.

The entities that supply these third-party services, of course, have strong incentives to ensure that users are aware of the privacy practices of the primary services they frequent, and thus they, too, assist in overcoming any information asymmetries that may persist. Meanwhile, the FTC and other consumer protection regulators undertake to educate consumers regarding privacy and data security risks and mechanisms to address them,[16] and have undertaken numerous enforcement actions against firms that they believe have misled or defrauded consumers with respect to the use of personal information.

The unlikelihood of a market for lemons in privacy is compounded by the fact that most online consumers are best viewed as repeat purchasers. Users of social networks, such as Facebook, Instagram, and LinkedIn, generally provide new information on a

---

[16] *See, e.g.*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/topics/privacy-identity-online-security (last visited May 30, 2019).

regular basis. As soon as a platform uses consumers' data in a way that harms them, those same consumers are more likely to defect if they believe the firm is likely to continue its substandard protection of data. The #DeleteFacebook campaign in the wake of the Cambridge Analytica data breach demonstrates this consumer response.[17]

Furthermore, it is not always the case that offering more privacy protective services is more expensive for firms, and thus they may in some cases have an incentive to offer them even without pressure from consumers. For example, retaining consumer data for long periods of time increases the costs of storage; collecting, storing, and processing more and different types of data is expensive, and in many cases it is not readily monetizable.

> Consider the manufacturer that exercises market power by skimping on quality in order to pad profits. Why do profits increase when, for example, a cookie maker uses less sugar or inferior cocoa powder, or an automobile manufacturer uses low quality paint or electronics? *Ceteris paribus*, profits rise because inferior inputs tend to mean lower costs. In this manner, a reduction in quality with the price held constant is analogous to an increase in price.
>
> Contrast this situation with an online publisher that decides to collect and mine additional consumer data. Distinct from the reduction in quality scenarios above, the online publisher does not profit automatically by reducing consumer privacy. Taking additional consumer data is not the same as skimping on quality, because collecting, storing, and analyzing data is an *additional cost*.[18]

While it is certainly true that this dynamic may have limited effect where data may simply be sold or where its very use is part of the services offered (e.g., many social networks), it remains the case that the adverse selection effect is dampened to the extent that "lower quality" does not equate with "lower price."

It must be noted, however, that lack of full information *can* lead to a potential "moral hazard" problem. In this case, the information that consumers may lack (or care sufficiently about) concerns other people or broader public goods. Under these conditions, users may share too much information or willingly take on too much risk of

---

[17] Tiffany Hsu, *For Many Facebook Users, a 'Last Straw' That Led Them to Quit*, N.Y. TIMES, Mar. 21, 2018, *available at* https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html.

[18] James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1135 (2013).

information exposure—the so-called "moral hazard"—either because they don't know of the effect beyond themselves, or because they don't internalize these costs.

In the modern data economy it is often the case that data about one person can reveal information about other people; the Cambridge Analytica kerfuffle demonstrated this. A study by MIT students showed that men's sexual orientation can be predicted by an analysis of social network sites such as Facebook, even if they do not share information about their sexuality. In this case, the inference was possible because data analytics reveal that homosexual men have proportionally more gay friends than straight men, which allows one to predict sexual orientation based solely on the sexuality of their friends (information that the friends may have revealed, even if a particular user chose not to).[19]

Given certain data that may correlate with certain personal characteristics, it is possible that information about a person can be gleaned, at least to some extent, from information shared by others. It may also be the case, for similar reasons, that national security or the protection of other interests (say, trade secrets) could also be compromised to some extent by the sharing of data, and thus that these interests may also not be sufficiently taken account of in individuals' data sharing decisions.

This externality may be positive or negative, and, of course, the sign and magnitude of the effect can depend upon users' idiosyncratic privacy preferences with respect to each aspect of information. Which effect predominates overall or in any particular instance is unclear. While advocates of strong privacy protections assume that negative externalities predominate, there really is no reason to think this is correct, and there is no evidence that we know of to suggest it is. Indeed, while there may be externalities from the collection and use of personal information, there are also externalities from *limits* on them to the extent they contribute to innovation. As Jones and Williams have shown, the social benefits of R&D are significantly larger than the internalized, private benefits.[20]

And, at the same time, individuals' preferences to *withhold* information or otherwise prevent it being shared may not account for the benefits such sharing would confer, even in cases where most of us would agree that the information at issue seems precisely the sort that should be protected. To take one example from a recent FTC

---

[19] *See* Justin P. Johnson, *Targeted Advertising and Advertising Avoidance*, 44 RAND J. ECON. 128 (2013).

[20] Charles I. Jones & John C. Williams, *Measuring the Social Return to R&D*, 113 Q. J. ECON. 1119 (1998) (estimating that the social return to R&D investment far exceeds the private return, meaning existing incentives for innovation are already lower than optimal).

workshop on the issue,[21] consumers may (understandably) strongly prefer to keep hidden from their social network connections ads that could appear indicating that the user purchased a home HIV test kit, if such data is used by the network to target ads to the users' connections. It may be that the revelation that the user bought an HIV test imposes a high cost on the user. But it may also be that the revelation would alert the user's sexual partners to their risk of infection and cause them to take their own precautions. Under these circumstances, the net benefit from the sharing of the information may be quite positive, even though the user may not take account of those external benefits.

2. The ignorance of consumers

Relatedly, the ignorance of users regarding the purported importance of threats to their personal information has been suggested as another justification for relatively more-heavy-handed, mandated privacy protections. At the core of this concern is that it is not just that consumers are unable to properly ascertain whether a firm will protect their personal information, but, more fundamentally, they might not even be aware that privacy protection and data security are relevant or important issues.[22] Under this framing, mandating privacy disclosures and other default behaviors (like opt-in) by firms not only serves to inform consumers about each firm's specific privacy policy, but also to raise awareness about privacy issues in general and provide presumptive protections against oversharing that runs counter to consumers' actual best interests.

However, the idea that most (or even many) consumers are entirely ignorant of privacy issues seems at odds with current developments in the area of privacy protection. The fact that the Cambridge Analytica scandal occupied the front pages of newspapers for weeks, slowed user growth on the Facebook platform, and wiped billions off Facebook's market capitalization is a testament to the importance that consumers attach to privacy issues.[23]

---

[21] FTC Workshop on Informational Injury, Transcript at 84-86 (Dec. 12, 2017), *available at* https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf.

[22] *See* Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016).

[23] *See* Rupert Neat, *Over $119bn Wiped Off Facebook's Market Cap After Growth Shock*, THE GUARDIAN, July 26, 2018, *available at* https: //www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock.

Of course, a small minority of consumers may indeed be ignorant of privacy issues. Thankfully, they will almost certainly be protected by the operation of the relatively more privacy-conscious consumers existing in the same market. An analogy with the monopoly pricing of traditional goods is useful here. Just because one consumer has an exceedingly high valuation for a good does not mean that firms, even monopolists, will be able to extract that agent's entire consumer surplus. Monopolies almost systematically leave some buyers with consumer surplus. To attract marginal consumers, a monopolist must forgo profits on its inframarginal users (i.e. charge them a price that is lower than their reserve).[24] This remains true so long as the monopolist cannot perfectly price discriminate at reasonable cost. A similar dynamic applies to so-called "contracts of adhesion," which, although typically unread and un-negotiated by the majority of consumers, nevertheless are found to offer largely efficient combinations of terms and prices because they must offer competitive terms to the particularly sensitive (marginal) consumers who *do* read them.[25]

The same logic applies to privacy protection. Although a small subset of users may be totally ignorant of privacy issues, firms cannot cash in on this ignorance because they are unable to identity these ill-informed users and write-up a separate privacy policy for them. This applies *a fortiori* when there is competition between online firms to attract them. Just as consumers do not need to shop around to get competitive prices in markets for physical goods, each individual does not have to be aware of a firms' privacy policy to benefit from competitive terms.[26] In other words, a committed minority of privacy-conscious individuals enable relatively less informed agents to enjoy a competitive level of privacy protection.

The virtuous influence that highly-informed consumers exert on their peers is likely to be even more pronounced when markets present network effects, as is often the case with online platforms. Network effects occur when a consumer's utility for a good is, at least in part, a function of the expected number (and quality) of other agents using the same product.[27] Although it is often mentioned that network effects

---

[24] *See* H.R. VARIAN, MICROECONOMIC ANALYSIS 236 (W.W. Norton. 1992).

[25] *See, e.g.,* Douglas G. Baird, *The Boilerplate Puzzle*, 104 MICH. L. REV. 933, 936 (2006) (noting that "[t]he sophisticated buyer provides protection for those that are entirely ignorant").

[26] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. 207, 214-15 (1996) ("[I]t is foolish to complain about contract terms. These all are mediated by price. 'Better' terms (as buyers see things) support higher prices, and sellers have as much reason to offer the terms consumers prefer (that is, the terms that consumers find cost-justified) as to offer any other ingredient of their products. It is essential to enforce these terms if markets are to work.").

[27] *See, e.g.,* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 96 (1994).

are self-reinforcing (adding users to a network will attract even more users), the inverse is also true. One group of users leaving a network may cause the whole platform to enter a "death spiral."[28] For this reason, online platforms are likely to be particularly wary of losing users for privacy-related reasons. More generally, the self-reinforcing nature of network effects also explains why user adoption is such a crucial metric for firms operating in the digital economy.[29]

Finally, even if it transpires that consumers are globally ignorant of privacy issues, top-down regulation is still unlikely to be the solution. Two scenarios are possible. A first possibility is that users do not attach any value to privacy matters, even when they are perfectly informed. If this is the case, then there is no scope for privacy regulations to improve consumer welfare; consumers are simply indifferent to the use that is made of their personal information.

A second possibility is that users would attach some value to privacy matters if only they were properly informed—in other words, there is some latent demand for privacy protection. But, unless there are widespread monopoly market failures, firms have an incentive to ferret out this preference, seize upon this latent demand, and, because of the pressures of competition, provide the welfare-maximizing level of privacy protection. This second scenario seems to be supported by empirical evidence.[30]

The upshot is that users being uninformed does not amount to a privacy market failure, so long as there is actual or potential competition for their patronage.

a. Revealed consumer preferences demonstrate heterogeneous demand different types of privacy

It is also important to recognize that apparent indifference to a variety of potential privacy harms may not, in fact, be the result of ignorance, but rather an informed preference. When consumers do decide to join or remain on a platform, it may be safe to assume—especially now that several high-profile data breaches have occurred—that their decisions to do so account for the expected losses that they may suffer with regards to their personal information.[31] In other words, these consumers are, at the

---

[28] *See* David S. Evans & Richard Schmalensee, *Debunking the Network Effects Bogeyman*, 40 REGULATION 36 (2017). *See also,* Joseph Farrell & Paul Klemperer, *Coordination and lock-in: Competition with switching costs and network effects*, 3 HANDBOOK OF INDUSTRIAL ORGANIZATION, 63 (2007).

[29] *See* Michael L. Katz & Carl Shapiro, *supra* note 27, at 96.

[30] *See generally* Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. (2011).

[31] It is demonstrably true inasmuch as consumers continue to use Facebook, Google et al now that they know more about the potential for data breaches ¨and misuse. However, in surveys consumers contradict

very least, revealing that they value the services of a platform more than the expected "price" they might pay through the unauthorized revelation of their information. Barring severe information asymmetries (which seems implausible following the aforementioned data breaches),[32] it is likely reasonable to conclude that data security issues are priced into consumers' dealings with online platforms.

In fact, research has consistently demonstrated that, when asked about different, specific types of privacy protections, consumers reveal a low preference for strong protections relative to other goods, like discounted or free services.[33] And even in situations where the information at stake might be very sensitive, people seem unwilling to pay very much to keep it private.[34]

Not only do *specific* privacy attitudes toward different kinds of information differ significantly *within* people, *general* privacy attitudes are highly heterogeneous *across* people. To capture general privacy preferences, privacy scholar Alan Westin developed the Privacy Segmentation Index (PSI), which categorizes people as either

---

themselves: Kimberly
Collins, *As Consumers Expectations Rise, Brands Find New Data to Personalize Experience*, CLICKZ, Sept. 17, 2018, *available at* https://www.clickz.com/as-consumer-expectations-rise-brands-find-new-data-to-personalize-experience/216842/. Once again, revealed preferences do not match elicited preferences.

[32] *See*, *supra*, at notes 10-21, and accompanying text.

[33] Alessandro Acquisti and Jens Grossklags, *When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, Workshop on the Economics of Information Security Proceedings 15 (2007) ("most subjects happily accepted to sell their personal information even for just 25 cents"); Sören Preibusch, Dorothea Kübler, and Alastair R. Beresford, P*rice Versus Privacy: An Experiment Into the Competitive Advantage of Collecting Less Personal Information*, 13(4) A.R. ELECTRONIC COM. RES. 423 (2013) ("[w]hen consumers were offered a tradeoff between price and privacy, the vast majority of customers chose to buy from the cheaper, more privacy-invasive, firm; this firm got both a larger market share and higher revenue."); Christian Happ, André Melzer, and Georges Steffgen, *Trick With Treat – Reciprocity Increases the Willingness to Communicate Personal Data*, 61 COMPUTERS HUM. BEHAV. 372 (2016) ("1,208 participants were asked to reveal their personal password…[M]ore than one-third of the participants were willing to do so [in exchange for a chocolate bar].").

[34] *See* Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, T*he Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RES. 254, 263 (2011) ("The premium for 'high privacy' batteries ranged from 3-5% of the product cost, while the premium for the sex toy ranged from 7-10% … [W]e found statistically significant privacy premiums of roughly 60 cents for both products."); *See also* Scott J. Savage and Donald M. Waldman, *Privacy Tradeoffs in Smartphone Applications*, 137 ECON. LETTERS 171 (2015) ("Results show that the representative consumer is willing to make a one-time payment for each app of about $2.28 to conceal their browser history, $4.05 to conceal their contacts, $1.19 to conceal their location, $1.75 to conceal their phone's identification number, and $3.58 to conceal their texts. These valuations vary for different segments of society").

"privacy fundamentalists," "privacy unconcerned," or "privacy pragmatists" based on their answers to a series of privacy-related questions.[35]

"Fundamentalists" are those who believe that it is almost never okay for people to trade their privacy for commercial benefits and that the government should regulate (and generally prohibit) such exchanges.[36] "Pragmatists" are those who believe that under the right circumstances it is reasonable to exchange personal information for some tangible benefit and that the current level of government privacy regulation is roughly sufficient.[37] The "unconcerned" are those people who, as Westin jokingly described them, would "give you any information you want about their family, their lifestyle, their travel plans" for a 5-cent discount.[38]

Acxiom and DMA recently conducted a survey that used the PSI methodology.[39] It found that 58 percent of respondents were "privacy pragmatists," 19 percent were "unconcerned," and 24 percent were "fundamentalists."[40] This breakdown is in line with other PSI surveys that have been conducted over the last 25 years, as shown in Figure 1.

---

[35] See, e.g., Ponnurangam Kumaraguru and Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies* at 5, Institute for Software Research International (2005).

[36] *Id.*

[37] *Id.*

[38] Alan F. Westin, Testimony on *Opinion Surveys: What Consumers Have to Say About Information Privacy* before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection (May 2001).

[39] Greg Sterling, *Survey: 58% Will Share Personal Data Under the Right Circumstances*, MARKETING LAND, June 20, 2018 *available at* https://marketingland.com/survey-58-will-share-personal-data-under-the-right-circumstances-242750

[40] *Id.*

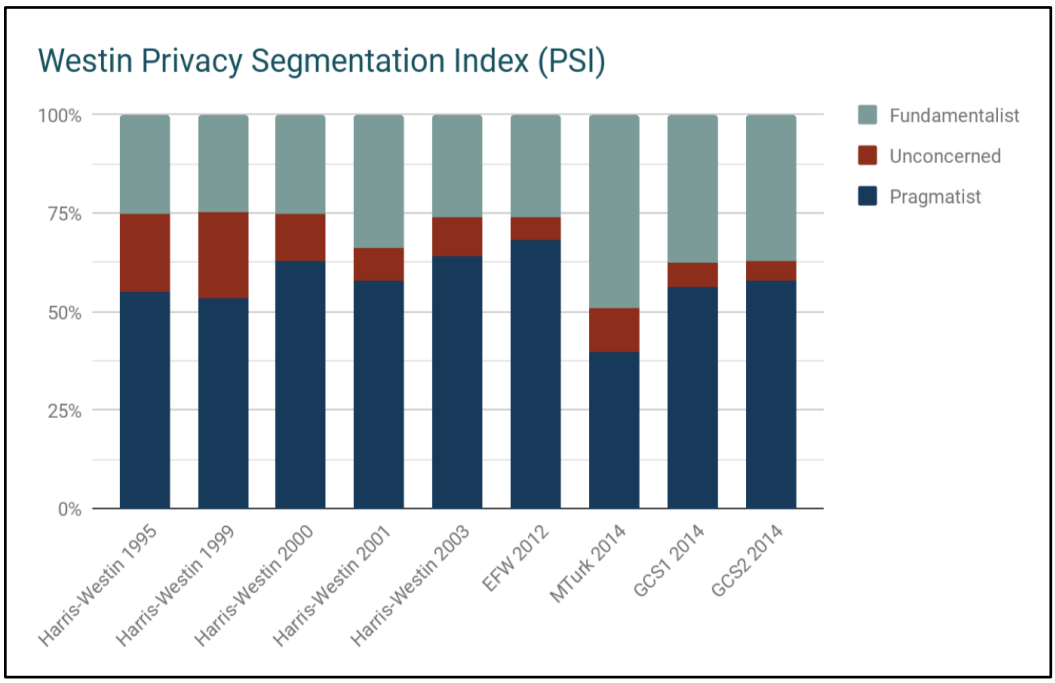

Figure 1. *Sources: Kumaraguru and Cranor;*[41] *Egelman et al.;*[42] *and Woodruff et al.*[43]

Thus, general privacy attitudes have been stable over the previous quarter century, with about 60 percent pragmatists, 25 percent fundamentalists, and 15 percent unconcerned. Further, on average, 75 percent of those surveyed believe that the status quo approach in the US at least adequately protects their privacy, if not overprotects it. And, according to a survey by the National Telecommunications and Information Administration, the trend in recent years is that major concerns related to online privacy and security risks have been decreasing and a smaller percentage of households have been avoiding online activities due to privacy or security concerns.[44]

In sum, these studies belie the notion that there is either rising public concern around privacy issues or a demand for additional regulation.

---

[41] Kumaraguru and Cranor, *supra* note 35.

[42] Serge Egelman, Adrienne Porter Felt, and David Wagner, *Choice Architecture and Smartphone Privacy: There's a Price for That*, Workshop on the Economics of Information Security (2012).

[43] Allison Woodruff et al., *Would a Privacy Fundamentalist Sell their DNA for $1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences*, Tenth Symposium on Usable Privacy and Security, USENIX Association (2014).

[44] Rafi Goldberg, Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds, NTIA, Aug. 20, 2018 *available at* https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

3. Data monopolies

Several of the dynamics discussed above turn on the presence of product market competition to ameliorate the effects of perceived defects like information asymmetry. Thus, the possibility that, at least in certain markets, "data monopolies" tend to emerge presents another potential justification for imposing relatively more onerous privacy requirements. The premise is that markets that rely heavily on consumer data are inherently prone to monopolization. This is notably said to stem from so-called "data network effects," and allegedly results in insufficient privacy protection for users.[45] A closer inspection of numerous digital markets suggests that this concern is overstated, however.

For a start, it is wrong to assume that data-intensive products necessarily lead to winner take all situations, akin to those that may occur in the presence of network effects. As Hal Varian aptly demonstrates, unlike network effects, data does not produce value in and of itself.[46] Instead, data must be analyzed to create value. As a result, companies cannot merely outcompete their rivals by acquiring superior or larger datasets: they must also hire the best data engineers and "learn by doing."[47] Because of this, there is no necessary data "positive feedback loop" and an industry's heavy reliance on data does not necessarily lead to higher concentration. For instance, brick and mortar retailers make heavy use of their consumers data and yet there is no reason to believe that these markets are particularly prone to concentration.

And, even where there are network effects, there is little reason to believe that this would make data-reliant markets less competitive. Although some scholars have voiced fears that network effects may lead to highly concentrated markets, not all markets with network effects will eventually tip towards a single winning firm.[48] Moreover, in those cases where network effects do lead to lopsided market distributions, potential competition from smaller competitors or new entrants may constrain the behavior of incumbents. In this case, the presence of network effects might merely substitute competition "in the market" with competition "for the market."[49]

---

[45] *See* Maurice E Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275, 283 (2018).

[46] *See* Hal Varian, *Artificial Intelligence, Economics, and Industrial Organization*, *in* THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA 15 (2018).

[47] *Id.*

[48] This is especially true in the presence of heterogeneous consumer preferences and differentiated products. *See* Shapiro & Katz, *supra* note 27, at 106.

[49] *See* Sami Hyrynsalmi, Arho Suominen & Matti Mäntymäki, *The Influence of Developer Multi-homing on Competition Between Software Ecosystems*, 111 J. SYS. & SOFTWARE 119, 119-27 (2016).

In other words, these effects do not necessarily prevent entry by more-efficient and/or innovative rivals,[50] nor do they preclude the creation of another market entirely through disruptive innovation.[51] And, as the basic premise of this RFC demonstrates, privacy is certainly one dimension along which these firms continue to compete. There exist privacy-oriented alternatives to browsers[52] and search engines,[53] for example, and even in the cellphone market—which is often characterized as a duopoly of iOS and Android[54]—Apple touts its more protective approach to security and privacy as a major feature of its iPhones.[55]

The notion that network externalities may benefit user privacy is also backed by economic findings concerning two-sided markets. In a highly acclaimed paper, Mark Armstrong has shown that competition between multi-sided platforms may result in particularly intense competition to acquire single-homing users (who are present on only one of many competing platforms).[56] This is often, though not always, the case for users of social networks, search engines, game consoles and of online retail platforms. Because there will be intense competition to attract these exclusive consumers (often resulting in zero nominal prices), any latent demand for privacy protection is likely to be met by competing firms.

There is thus little reason to believe that the presence of network effects would necessarily lead to inferior privacy protections for users. On the contrary, as has already been mentioned, network effects are a double-edged sword that are likely to result in platforms catering closely to the needs of privacy-conscious users and thus benefiting all other users on the network.[57]

Moreover, there is reason to believe that the competitive process itself is fully capable of protecting privacy interests. In their empirical study of consumer preferences and firm behavior with respect to consumer privacy protections, Tsai et al. found that

---

[50] *See* E. Glen Weyl & Alexander White, *Let the Best "One" Win: Policy Lessons from the New Economics of Platforms*, 10 COMPETITION POL'Y INT'L, 28 (2014).

[51] *See, e.g.*, Thibault Schrepel, *L'innovation de Rupture: De Nouveaux Défis Pour le Droit de la Concurrence*, 42 REVUE LAMY CONCURRENCE 141, 143 (2015).

[52] *See, e.g.*, *About Us*, BRAVE, https://brave.com/about/ (last visited May. 30, 2019).

[53] *See, e.g.*, DUCKDUCKGO, https://duckduckgo.com/about.

[54] Greg Sterling, *US Market Becoming a Smartphone Duopoly*, MARKETING LAND, July 23, 2018.

[55] *See, e.g.,* David Nield, *All the Ways iOS 12 Will Make Your iPhone More Secure*, WIRED, July 8, 2018.

[56] *See* Mark Armstrong, *Competition in Two-sided Markets*, 37 RAND J. ECON. 678 (2006).

[57] *See* Evans & Schmalensee, *supra* note 28.

> businesses may use technological means to showcase their privacy-friendly privacy policies and thereby gain a competitive advantage. In other words, businesses may direct their policies and their information systems to strategically manage their privacy strategies in ways that not only fulfill government best practices and self-regulatory recommendations, but also maximize profits.[58]

The market is the best disciplining force for correcting firms that stray from consumer preferences. Firms are driven by the profit motive, which is to say that if the non-ad supported, privacy-oriented products that already exist—and that comport with the notion of, for example, an opt-in regulatory requirement—were actually offering a service that consumers desired at a price they were willing to bear, those services would thrive, and the less privacy-sensitive options would be forced to shift their practices. No barriers to entry, regulatory impediments or the like prevent such services from operating or succeeding, other than, it seems, lack of consumer demand (particularly in light of the research noted above suggesting that firms would be willing to profit from providing greater levels of privacy).

Firms in technology-intensive industries, moreover, frequently find it difficult to maintain dominance in a market, which puts further pressure on those firms to compete on price and quality. The classic example is Schumpeterian competition, in which firms leapfrog one another in a series of short-lived monopolies, each achieved through technological advance and maintained only so long as the then- monopolist can maintain its advantage. While this may bear the superficial hallmarks of monopoly, such dynamic competition in technology markets is actually perfectly consistent with strong competition and procompetitive outcomes.[59] Each successive "winning" firm must be committed to investing its profits in developing new and better technologies in order to try to preempt or co-opt the next technological wave and maintain its position.

Further, particularly in markets characterized by high degrees of technological change, potential competition can operate as effectively as—or even *more* effectively than—actual competition to generate competitive market conditions:

> [I]n industries... where technological change is rapid, competition for the market may provide more benefits to consumers than competition in the

---

[58] Janice Y. Tsai, et al., *supra* n. 30 at 266.

[59] *See, e.g.*, Thomas M. Jorde and David J. Teece, *Antitrust Policy and Innovation: Taking Account of Performance Competition and Competitor Cooperation*, 147 J. INSTIT'L & THEORETICAL ECON. 118 (1991). Note also that "competition for the market" can be as constraining as within-market competition. See Harold Demsetz, *Industry Structure, Market Rivalry and Public Policy*, 16 J. L. & ECON. 1 (1973).

> market. Where competition for the market is important, the number of competitors in the market at any point does not usefully measure the extent to which competitive processes underlie market behaviour.[60]

As applied here, if privacy-protections are important to consumers, firms in technology-heavy industries that are competing for the market have a sharp interest in meeting that consumer demand. The fact that at any given time only a single, or only a few, firms comprise an industry does not mean that the industry is not responsive to consumers' preferences—for privacy as for all other aspects of the products and services they consume.

4. Exploitative and anticompetitive data usage

Some scholars have argued that firms may use personal data to charge "exploitative" prices to consumers.[61] The claim is that this allegedly undesirable practice is facilitated by access to personal information that may allow firms to more effectively price discriminate, anticipate consumer demand, and charge supra-competitive prices despite there being ostensible competition in the market. There are important objections to these assertions.

First and foremost, critics routinely miss the fact that, absent significant barriers to entry, no firm can expect to earn supra-competitive profits for an indefinite period of time. This includes profits derived from data-driven price discrimination. The reason for this is straightforward. One firm earning high profits will inevitably attract entry from competitors and/or encourage consumers to switch towards rival firms. This arbitrage ultimately leads to lower prices and to more privacy practices that comport with user expectations as a quality dimension of competition.

Second, even if a firm could price discriminate without the threat of arbitrage, high-value consumers would have huge incentives to withhold their personal information and/or send deceptive signals that they are low-value purchasers. When this is the

---

[60] Neil Quigley, *Dynamic Competition in Telecommunications: Implications for Regulatory Policy* 17, C.D. HOWE INSTITUTE COMMENTARY, no. 194 Feb. 2004, *available at* https://www.cdhowe.org/pdf/commentary_194.pdf. *See also* A.E. Kahn, *Telecommunications: The Transition from Regulation to Antitrust*, 5 J. TELECOMM. & HIGH TECH. L. 159 (2006); Jason Pearcey & Scott J. Savage, *Actual and Potential Competition in International Telecommunications* 4 (Working Paper, Oct. 21, 2015), *available at* https://www.montana.edu/jpearcy/papers/ISR_Web.pdf ("Overall, these results suggest that incumbent firms reduce their price when potential competition increases…."); Harold Demsetz, *Id.*

[61] *See* Stucke, *supra* note 45, at 293 (2018). *See also,* Curtis R Taylor, *Consumer Privacy and the Market for Customer Information*, RAND J. ECON. 631 (2004).

case, the ability to acquire detailed consumer information may, counterintuitively, lead to lower prices and higher consumer welfare.[62]

III. The costs of departing from current approaches to privacy regulation

All regulation comes at a cost. Even well-intentioned regulation designed to protect the privacy of individuals must be evaluated in terms of both the benefits it provides to individuals as well as the costs to those same individuals, the firms they contract with, and social welfare.

To begin with, there are clear benefits to information sharing that must be taken into account. Since the dawn of the Internet, free digital services have created significant consumer surplus and this trend continues today: Recent research using both survey and experimental methodologies has consistently found substantial benefits for consumers from sharing information in exchange for free (or subsidized) digital products.

Allcott et al., for example, studied the price that Facebook users were willing to accept in order to abstain from using the service for four weeks.[63] In the study, the median willingness-to-accept (WTA) from participants was $100.[64] The WTA estimate means that "[a]ggregated across an estimated 172 million US Facebook users, the mean valuation implies that four weeks of Facebook generates $31 billion in consumer surplus in the US alone."[65]

Corrigan et al. reported similar results of "a series of three non-hypothetical auction experiments where winners are paid to deactivate their Facebook accounts for up to one year."[66] In their conclusion, the researchers said, "Though the populations sampled and the auction design differ across the experiments, we consistently find the

---

[62] *See* Taylor, *supra* note 61, at 643 (2004).

[63] Hunt Allcott, Luca Braghieri, Sarah Eichmeyer, and Matthew Gentzkow, *The Welfare Effects of Social Media*, NBER Working Paper No. 25514 (2019).

[64] Id. at 5. Note, this was not just cheap talk—the study followed through and paid a randomly-selected portion of the users to deactivate their accounts for four weeks. *Id.*

[65] *Id.*

[66] Jay R. Corrigan et al., H*ow much is social media worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (2018).

average Facebook user would require more than $1,000 to deactivate their account for one year."[67]

Brynjolfsson et al. reviewed the benefits of "several empirical examples [of technology that implicates privacy concerns] including Facebook and smartphone cameras" and then "estimate[d] their valuations through incentive-compatible choice experiments."[68] The study found considerable benefits that are currently excluded from national accounts: "For example, including the welfare gains from Facebook would have added between 0.05 and 0.11 percentage points to GDP-B growth per year in the US."[69]

In a literature review of the economics of privacy, Acquisti et al. concluded that:

> Extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: **the optimal balancing of privacy and disclosure is very much context-dependent, and it changes from scenario to scenario**.[70]

Moreover, what we think of as privacy is actually an umbrella covering many related concepts, each with their own separate complicating factors.[71] As some economists have aptly pointed out:

> If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing.[72]

With this in mind, digital privacy regulations can have important intended and unintended consequences that could significantly harm consumer welfare in the long

---

[67] *Id.*

[68] Erik Brynjolfsson et al., *GDP-B: Accounting for the Value of New and Free Goods in the Digital Economy*, NBER Working Paper No. 25695 (2019).

[69] *Id.*

[70] Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 52(2) J. Econ. 48 Literature (2016) (emphasis added).

[71] Acquisti, et al., *supra* note 22, at 443.

[72] *Id.* at 462.

run. These include misunderstanding consumer preferences, requiring excessive data protection, mandating business models, imposing compliance costs that potentially exceed to benefits of those regulations, crowding out superior privacy offerings stemming from the private sector, and protecting some companies' market power.

A. Opt-in versus opt-out

One significant deviation from current US privacy law that would be highly problematic would be switching of the default presumption concerning data use from "opt-out" to "opt-in" for an expanded class of data.

A core problem is that "'[o]pt-in' provides no greater privacy protection than 'opt-out' but imposes significantly higher costs with dramatically different legal and economic implications."[73] In staunching the flow of data, opt-in regimes impose both direct and indirect costs on the economy and on consumers,[74] reducing the value of certain products and services not only to the individual who does not opt-in, but to the broader network as a whole. Not surprisingly, these effects fall disproportionately on the relatively poor and the less technology-literate.[75]

Furthermore, empirical research shows that opt-in privacy rules reduce competition by deterring new entry. Thus, the seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition: "[R]ather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive.... [I]n some cases where entry had been profitable without regulation, [some firms] will choose not to enter."[76]

---

[73] Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* at 1, *available at* http://bit.ly/2lvZ9uz. *See also* Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155 (Apr. 2010), *available at* http://bit.ly/2lvKy2s.

[74] *Id.* at 5 ("[T]he 'opt-out' system sets the default rule to 'free information flow' and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an 'opt-in' system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.") (emphasis in original).

[75] *See, e.g.,* Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REPORT 31, 38 (2002); *Opt-in Dystopias*, *supra* note 73, at § 5.1.

[76] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 48-49 (2015) (emphasis added).

For these reasons, when data usage is consistent with "the context of the transaction or the company's relationship with the consumer," regardless of the sensitivity of the data involved, the Commission does not generally require even choice, let alone affirmative consent, before a company collects or uses consumer data.[77] Survey data confirms the Commission in this approach. A 2014 survey by the Pew Research Center, which found a wide range of sensitivities for different kinds of information, with social security numbers being the most sensitive and basic purchasing habits being the least sensitive.[78] The report went on to note that "there are a variety of circumstances under which many Americans would share personal information or permit surveillance in return for getting something of perceived value."[79]

For those data uses that do fall outside the context of the transaction, the Commission requires "affirmative express consent" (opt-in consent) *only* for uses of particularly sensitive data.[80] This is the correct approach as it recognizes that, given the proper context, a large amount of socially beneficial uses of data are possible under an opt-out regime.

By contrast, an opt-in requirement effectively implies a determination that unauthorized data uses are presumptively harmful. But the mere fact that a consumer's information may be used in ways that the user doesn't expect or understand does not mean that such use is harmful to consumers individually or in the aggregate. Whether such uses are desirable, or on net are beneficial or harmful to consumers, is enormously context- and person-specific. But it does seem to be the case that presumptively deterring these transactions does *not* benefit consumers:

> "Opt-in" is frequently portrayed as giving consumers greater privacy protection than "opt-out." In fact, the opposite is true. **"Opt-in" provides no greater privacy protection than "opt-out" but imposes significantly higher costs with dramatically different legal and economic implications**.[81]

Similarly:

---

[77] FTC Privacy Report at 48.

[78] Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CENTER, Jan. 14, 2016 *available at* https://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[79] *Id.*

[80] *Id.* at 60.

[81] *See* Cate & Staten, *Protecting Privacy in the New Millennium: supra* note 73, at 1.

> [T]he opt-out regime produces better welfare results than the anonymity regime, which in its turn is better than the opt-in regime. Therefore, from a social welfare point of view, it matters whether opt out or opt in is adopted as the privacy standard.[82]

And, of course, an opt-in regime is indeed more expensive than an opt-out regime.[83] As Fred Cate and Michael Staten detail, the costs can fall widely on both consumers and providers, can be significant, and can deter valuable information exchange:

> [C]onsider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. In obtaining permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that an "opt-in" system was significantly more expensive to administer, costing almost $30 per customer contacted. To gain permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls than in an "opt-out" system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.[84]

As this example suggests, the crucial problem with an opt-in regime is that it staunches the flow of data, imposing both direct and indirect costs on the economy and on consumers:

> An "opt-out" system presumes that consumers **do want** the convenience, range of services, and lower costs that a free flow of personal information facilitates, and then allows people who are particularly concerned about privacy to block the use of their information. Put another way, the "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.

---

[82] Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis Of Privacy Policies*, *available at* https://www.econstor.eu/bitstream/10419/25876/1/521168813.PDF.

[83] *See* Cate & Staten, *supra* note 73; Lundblad & Masiello, *Opt-in Dystopias*, *supra* note 73.

[84] *See* Cate & Staten, *supra* note at 73, at 5.

> In other words, an "opt-in" system sets the default rule to "no information flow," thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information.
>
> Consequently, an "opt-in" system for giving consumers control over information usage **is always more expensive than an "opt-out" system**.[85]

Finally, empirical research shows that opt-in privacy rules deter competition by deterring new entry. The seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition:

> [M]ost privacy regulation requires firms to obtain one-time individual consumer consent to use consumer data (rather than the consent requests increasing with the amount of data used). Therefore, privacy regulation imposes transaction costs whose effects… will fall disproportionately on smaller firms. Consequently, rather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive.
>
> * * *
>
> [In] competition between a generalist firm offering products that appeal to a variety of consumer needs and a specialist firm offering a product that serves fewer consumer needs,… privacy regulation can preclude profitable entry by the specialist firm. Under regulation, the extra costs required to obtain consent mean that in some cases where entry had been profitable without regulation, the specialist firm will choose not to enter. The generalist firm then captures the whole market. This implies that privacy regulation can increase the advantage enjoyed by a large generalist firm. This deprives consumers of the higher-quality niche product offered by a specialist firm, which represents a loss that must be balanced against any gain to consumers due to the increased privacy.[86]

B. Mandating transparency and fairness

While it may be true that many consumers are ill-informed,[87] it is not clear that a GDPR-style government-imposed mandate on companies to process information

---

[85] *Id.* (emphasis in original).

[86] Campbell, Goldfarb & Tucker, *supra* note 76, at 48-49.

[87] But, see, *supra*, notes 22-44 and accompanying text.

"lawfully, fairly and in a transparent manner"[88] will do anything to make consumers better informed. First, if a company is not behaving lawfully, then it is unclear that a government regulation will do anything to stop such unlawful behavior. Second, fairness is a highly subjective term open to interpretation—and abuse. Third, and perhaps most important, government mandates for "transparent" information processing are often counter-productive.[89] Consider the example of mandatory disclosures of information on packaged food, which have resulted in an over-abundance of information, leading to a decline in the use of such labels by consumers—and leading to further attempts to provide more useful and useable information on the part of food companies and governments, many of them also unhelpful.[90] Likewise, consider the mandatory disclosure requirements for financial transactions, which have led to an explosion of form-filling but done little to improve consumer decision-making and may have undermined it, due to the great length of many such disclosures and resultant information processing fatigue.[91]

Further complicating matters, consumers' preference for privacy, and similarly the benefits they derive from sharing information or from less protective uses of their information by firms, vary throughout the population.[92] The relationship between privacy and quality is purely subjective:

> Saying that a publisher's decision to collect and analyze additional data reduces the quality of its service is akin to saying that a restaurant's decision to replace corn with green beans on its menu lowers the quality of

---

[88] GDPR at Article 5 (1).

[89] *See generally*, Geoffrey A. Manne, *The Hydraulic Theory of Disclosure Regulation and Other Costs of Disclosure*, 58 ALA. L. REV. 473 (2007).

[90] J. E. Todd & J. N. Variyam, *The Decline in Consumer Use of Food Labels, 1995-2006*, Economic Research Report Nr. 63 (2006), *available at* http://www.ers.usda.gov; J. N. Variyam & J. Cawley, *Nutrition Labels and Obesity*, NBER Working Paper No. W11956 (2006); B. Wansink & P. Chandon, *Can "Low-Fat" Nutrition Labels Lead to Obesity?*, J. Marketing Res., 43: 605-17 (2006); B. Wansink, S. T. Sonka, & C. M. Hasler, *Front-label Health Claims: When Less is More*, 29 Food Policy 656-67 (2004).

[91] Angela A. Hung et. al., EFFECTIVE DISCLOSURE IN FINANCIAL DECISIONMAKING (RAND Corp., 2015) *available at* https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1270/RAND_RR1270.pdf.

[92] *See, e.g.*, Kai-Lung Hui & I.P.L. Png, *The Economics of Privacy*, in HANDBOOKS IN INFORMATION SYSTEMS, VOL. 1, ECONOMICS AND INFORMATIONAL SYSTEMS 489 (Andrew B. Whinston & Terrence Hendershott, eds., 2006) (noting that "the key policy issue is not whether individuals value privacy. It is obvious that people value privacy. What is not known is how much people value privacy and the extent to which it varies").

> its food. These statements will likely be true for some, but are false for others. There is no right answer.[93]

This makes it problematic to adopt policies aimed at mandating increased privacy protections because, for many people, these policies will harm them, even as the very same policies will benefit others. The upshot is that it is unclear what fairness entails for data processors, and thus what it means to comply with such a requirement. This introduces significant discretion on the part of enforcers into the system. Whether their sense of fairness better comports with overall social preferences is perhaps even less likely.

C. Compliance opportunity costs

The enactment of privacy regulations will often involve substantial costs for firms. Compliance with legal requirements that go beyond optimal protection measures and may entail inefficient direct costs, and the costs of government reporting, erroneous enforcement, and vexatious litigation can be substantial. In general, at least some of these costs will be passed on to consumers, either in the form of higher prices, lower quality, or less innovation, and these costs can offset or wipe out any possible gains from greater privacy protections.

In addition to these direct and indirect costs, privacy regulations may also entail substantial opportunity costs. These costs include the redirection of firms' engineers, lost business opportunities, and forgone investments.[94]

It has been estimated that American S&P 500 companies and UK FTSE 350 companies spent a combined total of $9 billion to comply with the GDPR in the year running up to its entry into force alone, for example.[95] Microsoft alone estimated that it had 1,600 engineers working on GDPR-related compliance projects.[96] During a

---

[93] Cooper, *Privacy and Antitrust supra* note 18, at 1138.

[94] For a catalogue of the compliance costs and unintended/unforeseen consequences of the GDPR, for example, see Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, TRUTH ON THE MARKET (May 24, 2019), *available at* https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/.

[95] Oliver Smith, *The GDPR Racket: Who's Making Money From This $ 9 bn Business Shakedown*, FORBES, May 2, 2018, *available at* https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#33232d9834a2

[96] Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of their Own Data*, MICROSOFT, May 21, 2018 *available at* https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

recent Senate hearing, Keith Enright, Google's chief privacy officer, estimated that the company spent "hundreds of years of human time" to comply with the new privacy rules.[97]

According to the International Association of Privacy Professionals, the Global Fortune 500 will spend an estimated $7.8 billion in compliance costs for GDPR.[98] For large US firms, total compliance costs are estimated to reach $150 billion.[99] As a result of the law, an estimated 75,000 "data protection officers" will be hired for compliance.[100]

And these figures do not include the significant costs incurred by smaller firms, firms that originate from other countries, and the expenses that businesses will have to incur in the future to stay in compliance with the GDPR.

But the costs do not stop there. The adoption of the GDPR has not magically conjured up an army of engineers to ensure compliance with its provisions. Instead, there is a vast opportunity cost involved, as many engineers have been forced to spend significant amounts of their time working on these issues.[101] This is time that could otherwise be put to more productive uses, such as better managing supply chains, improving existing products and user experiences, and developing new and innovative goods. It is impossible to put a precise number on this cost, though its potential breadth is significant (the GDPR has no *de minimis* carve outs, which means that even tiny companies must ensure they comply with its provisions).[102]

It is also important to account for the effects of privacy regulation on firms' ability to adopt efficient business practices or to engage in data-based innovation. Data

---

[97] Ashley Rodriguez, *Google Says it Spent "Hundreds of Years of Human Time" Complying With Europe's Privacy Rules*, QUARTZ, Sept. 26, 2018 available at https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/.

[98] *Global 500 Companies to Spend $7.8B on GDPR Compliance*, IAPP, Nov. 20, 2017 *available at* https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/.

[99] Daniel Castro and Michael Mclaughlin, *Why the GDPR Will Make Your Online Experience Worse*, FORTUNE, May 23, 2018 *available at* http://fortune.com/2018/05/23/gdpr-compliant-privacy-facebook-google-analytics-policy-deadline/.

[100] Rita Heimes and Sam Pfeifle, *Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide*, IAPP, Nov. 9, 2016 *available at* https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

[101] *See* Stapp, *GDPR After One Year*, *supra* note 94.

[102] *See* GDPR Art. 2. *See also* Stapp, *GDPR After One Year*, *supra* note 94

(information) regulation (as opposed to other types of regulation) is particularly likely to affect institutional structure. As Luis Garicano notes:

> Organizations exist, to a large extent, to solve coordination problems in the presence of specialization. As Hayek pointed out, each individual is able to acquire knowledge about a narrow range of problems. Coordinating this disparate knowledge, deciding who learns what, and matching the problems confronted with those who can solve them are some of the most prominent issues with which economic organization must deal.[103]

Regulations that affect how firms can collect, store, use and disseminate information may thus have significant effect on firm governance and organization.

This dynamic could manifest itself as companies simply choosing to collect and use less data, but it could mean a lot of other things as well. It could affect corporate organization (e.g., deterring vertical integration or creating "data firewalls" between different divisions of a company), encourage limits on the geographic scope of data collection or operation,[104] affect the mechanisms for determining executive compensation, or (further) encourage jurisdictional considerations to dictate incorporation and principal place of business decisions. While choosing second-best options is rational from the perspective of regulated parties, it is nevertheless costly to society, both in terms of the firm's efficient operation relative to its operation in a viable alternative regulatory regime and to consumer welfare generally.

To take just one example, privacy regulations could arguably make it harder for companies to price discriminate in those instances where the practice would be welfare-enhancing. The most obvious example is that of insurance markets.[105] At the extreme, protecting users' privacy may prevent firms from obtaining information relevant to the setting of insurance premiums and compensation amounts. To the extent that this prevents insurers from better aligning premiums and risk, it impedes the role of premiums in accurately signaling risk and encouraging risk reduction. Moreover, to the extent that insurance companies would find it difficult or impossible to use subscribers' smartphone or GPS data and the like in assessing risk, it would

---

[103] Luis Garicano, *Hierarchies and the Organization of Knowledge in Production*, 108 J. POL. ECON. 874, 874 (2000).

[104] For example, at least 1,129 US news sites are unavailable in the EU due to GDPR. *See Websites Not Available in the European Union after GDPR*, DATA.VERIFIEDJOSEPH *available at* https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr (last visited May 30, 2019).

[105] Acquisti, et al., *supra* note 31, at 470.

increase these firms' administrative costs and may preclude them from offering lower premiums.

At the same time, mandating opt-in consent before firms may use data in novel ways will, at the margins, deter experimentation and innovation by all firms. It will impede the ability of firms to offer innovative product improvements, but also even to monetize their current products and services through the use of consumer data. The end result may be higher direct prices for consumers as well as fewer quality improvements over time.

D. Crowding out

Another unintended consequence of mandating certain modes of privacy protection is that regulation may preempt private entities from offering differentiated or even superior protection on their own.

This pitfall is notably illustrated by Blockchain technology's rocky relationship with Europe's GDPR. Blockchain is the fruit of efforts by some of the most privacy-conscious individuals on the planet. At its core, blockchain technology usually implies partial or even total anonymity. While the most successful distributed ledgers, such as Bitcoin and Ethereum, are not fully anonymous (the ledger of completed transactions is public, though the contents of each transaction is private),[106] other projects such as Monero and Zcash offer total privacy to their users.[107] Details aside, the distributed ledger industry is, in no small part, a reaction to fears about privacy and centralization in mainstream web services.[108]

Given this, one could be forgiven for thinking that blockchain technology would obviously comply with the requirements set out in the GDPR. But nothing could be further from the truth. In fact, the GDPR could potentially present a significant stumbling block to the wider adoption of distributed ledger technology.[109] Indeed,

---

[106] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-peer Electronic Cash System*, at 6 (2008), at https://bitcoin.org/bitcoin.pdf ("The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.").

[107] *See* Griffin Knight, *Monero vs. Zcash and the Race to Anonymity,* MEDIUM, Feb. 28, 2018, https://medium.com/coinmonks/monero-vs-zcash-and-the-race-to-anonymity-4322b0a9bd90.

[108] *See, e.g.,* Vitalik Buterin, *Privacy on the Blockchain*, ETHEREUM BLOG, Jan. 15, 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

[109] *See* Michèle Finck, *Blockchains and Data Protection in the European Union*, 4 EUR. DATA PROT. L. REV. 17, 33 (2018).

some of the GDPR's requirements, such as the right to erasure and amendment, are virtually incompatible with the immutable nature of the blockchain ledger.[110]

The fact that blockchain might not comply with the GDPR is a clear case of what Nassim Taleb calls "Wittgenstein's ruler." He observes that

> [u]nless you have confidence in the ruler's reliability, if you use a ruler to measure a table you may also be using the table to measure the ruler. The less you trust the ruler's reliability, the more information you are getting about the ruler and the less about the table.[111]

In the case at hand, the fact that blockchain technology does not comply with the strenuous requirements of the GDPR says more about the regulation's rigidity and its inability to adapt to new technology (even though it has only just entered into force) than it does about blockchain's lack of privacy protection.

Privacy regulation may also crowd out self-help products. These technologies and companies enable consumers to withhold data, send signals they are low-value purchasers, and exert more granular control over data. High profile examples of these technologies include ad blockers and VPNs. By potentially negating the need (or the perceived demand) for these products, regulation may effectively drive these firms out of business—firms whose specialized research and development may potentially yield relatively more optimal degrees of protection.

All of this has important downsides. In effect, regulation will shift the burden and decision-making regarding privacy protection from consumers, notably by using third-party products, onto online platforms operating under strict constraints. This may lead to both inadequate privacy protection and protection provided at a higher cost.

Unlike government intervention, which can misread potential demand for a given set of protections, self-help technologies act as revealed preferences. Their success or failure conveys valuable information about the type and quantity of privacy protection that is actually important to users. In turn, firms can monitor the success of these products and incorporate valuable privacy features into their own offerings. Arguably this is what has happened with browsers incorporating ad blockers, for example.

---

[110] *Id.*

[111] *See* N.N. TALEB, FOOLED BY RANDOMNESS: THE HIDDEN ROLE OF CHANCE IN LIFE AND IN THE MARKETS 224 (Random House Publishing Group 2008).

To make matters worse, by imposing command and control obligations on firms, regulation ignores the possibility that they might not be the least cost avoiders. In other words, it is plausibly more efficient for society to encourage users to withhold their personal information than to force firms to put in place costly measures designed to protect it. By legally preventing firms and consumers from reallocating the rights that exist between them, the strictest privacy regulations may ultimately harm consumers and firms alike.

E. Entrenching incumbent firms

Finally, the adoption of privacy regulation may also have a significant effect on competition. Not only do these regulations potentially favor large incumbents over innovative startup companies, they may also induce firms to make costly choices regarding the business models that will prevail in affected sectors.

For a start, numerous economists have pointed out the privacy regulation tends to entrench established incumbents. For instance, Campbell, Goldfarb and Tucker show that "a potential risk in privacy regulation is the entrenchment of the existing incumbent firms and a consequent reduction in the incentives to invest in quality. These incentives are stronger when firms have little consumer-facing price flexibility, as is the case in online media."[112] Indeed, "privacy regulation can shield a large, general incumbent from potential competition because regulation raises the threshold quality and scope for profitable entry by a challenger.... This is more likely for relatively strong incumbents: the stronger the incumbent, the better the marginal entrant must be."[113] This applies with even more force when privacy regulations rely on opt-in consent, because users are less likely to test the products of new entrants.[114]

Another potential issue is that privacy regulations may lead firms to adopt differentiated business models (or advocate for regulations supporting them) not for their intrinsic value but for their ability to reduce their own costs relative to other firms, and to increase those of their rivals. Apple CEO, Tim Cook, appeared to evidence this dynamic in his reaction to the introduction of the GDPR. Cook publicly came out in favor of this type of regulation, calling for the United States to adopt similar

---

[112] *See* James Campbell, Avi Goldfarb & Catherine Tucker, *supra* note 76, at 68.

[113] *Id.*

[114] *Id.* at 49. *See also*, Jan Bouckaert & Hans Degryse, *Default Options and Social Welfare: Opt in Versus Opt Out*, 169 J. INSTITUTIONAL AND THEORETICAL ECON. JITE 468-489 (2013).

provisions.[115] Unsurprisingly, he forgot to mention that Apple's business model is far less reliant on personal data than those of its rivals, such as Google and Facebook, because it is not in the business of targeted advertising.[116] Apple thus stands to lose far less from the adoption of privacy regulations than its close rivals.

This last issue would not be much of an issue if all consumers unambiguously preferred Apple's business proposition to that of its rivals, but this simply is not the case. Take smartphones, for instance. Whereas Apple offers the most high-end smartphones with more privacy protection (less exposure to targeted advertising), Google has differentiated itself by producing an OS that relies on targeted search engine advertising to generate profits (the Android OS).[117] This type of differentiation is potentially valuable for consumers. Privacy-conscious users can pay extra money to obtain the most secure device, while targeted advertising on the Android OS decreases the direct cost of devices for more price-sensitive consumers. By arbitrarily preferencing a particular business model via privacy regulation, legislators may ultimately deprive consumers of valuable choices.

An ex ante requirement of a particular privacy model may, in fact, do much to discourage competition. Developing successful online platforms entails significant fixed costs; no magic switch exists to suddenly bring into existence a particular version of a software platform. Development of successful platforms entails hundreds or thousands of hours of engineering time—and mandating a platform that consumers don't seem to prefer means devoting that time to developing what the market has demonstrated to be an inferior product. Thus, the returns to such development will necessarily be less than the returns to development of the primary, ad-supported product possible under an opt-out default presumption, and, consequently, the ad-supported product will be forced to itself subsidize the legally-mandated paid version of the product.

For large, established platforms this cost can be (more or less) easily absorbed (depending, of course, on the underlying technology of the platform). But for startups such a regulatory obligation would amount to a significant entry barrier. In particular, the ability to gain critical mass for its service would be significantly reduced as its

---

[115] *See* Russell Brandom, "Tim Cook wants a federal privacy law—but so do Facebook and Google", THE VERGE, Oct. 24, 2018, available at https://www.theverge.com/2018/10/24/18018686/tim-cook-apple-privacy-law-facebook-google-gdpr.

[116] *See, e.g.*, Mehreen Khan, "Apple and Facebook call for EU-style privacy laws in US", THE FINANCIAL TIMES, Oct. 24, 2018, available at https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713.

[117] *See* Dirk Auer, *Appropriability and the European Commission's Android Investigation*, 23 COLUM. J. EUR. L. 658 (2017).

upfront fixed costs will explode, and its users will be spread across multiple services. The net result will be less entry (especially by smaller firms) and less-effective competition:

> [A] specialist that fills a smaller niche and offers a smaller quality premium over the equivalent function of the generalist is more likely to earn lower revenue after entry in the case with regulation than in the case without.... Intuitively, absent regulation, entrants offer a targeted product after entry, and if the content of the firm's product offering has broad enough appeal, this generates enough revenue to allow them to profitably enter. With regulation... [s]maller entrants and entrants that offer a smaller quality premium in their niche are more likely to offer an untargeted product in equilibrium after entry. Since an untargeted product generates less revenue, this means that, all else equal, the marginally profitable entrant must be larger than before to overcome the fixed cost of entry....[118]

The pro-incumbent bias of GDPR has been evident since it went into effect. GDPR has been particularly good for large incumbents in ad-supported markets, for example, because they operate first-party ad networks, which means they have a direct relationship with end-users and can quickly obtain the opt-in consents required by GDPR. During the first year of GDPR, smaller adtech vendors suffered the largest decreases in website reach while Facebook only saw a minor decline, and Google increased its reach.[119]

GDPR is also decreasing both the number and size of venture capital investments in EU startups. According to Jia et al.:

> Specifically, our findings suggest a $3.38 million decrease in the aggregate dollars raised by EU ventures per state per crude industry category per week, a 17.6% reduction in the number of weekly venture deals, and a 39.6% decrease in the amount raised in an average deal following the rollout of GDPR … We use our results to provide a back-of-the-envelope calculation of a range of

---

[118] Campbell, Goldfarb & Tucker, *supra* note 76.

[119] *See* Björn Greif, *Study: Google is the biggest beneficiary of the GDPR*, CLIQZ, Oct. 10, 2018 *available at* https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

> job losses that may be incurred by these ventures, which we estimate to be between 3,604 to 29,819 jobs.[120]

And a survey by Merrill Corp reported that "55 percent of respondents said they had worked on deals that fell apart because of concerns about a target company's data protection policies and compliance with GDPR."[121] A separate study by PricewaterhouseCoopers LLP found that "fewer than half of international companies worth $100 million or more said they are fully prepared to comply with GDPR."[122] And many small and medium-sized businesses have left the EU market or shut down entirely due to GDPR.[123]

---

[120] Jian Jia, Ginger Zhe Jin, and Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. w25248 (2018).

[121] *GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey*, Merrill Corporation, Nov. 13, 2018 *available at* https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html.

[122] *The Journey to Digital Trust*, PWC (2018) *available at* https://www.pwc.co.uk/cyber-security/pdf/pwc-digital-trust-insights-survey.pdf.

[123] Below is a non-exhaustive selection of some of the firms that have either shutdown entirely or have withdrawn from the EU drawn from Stapp, *GDPR After One Year*, *supra* note 94:

- CoinTouch, Peer-to-peer cryptocurrency exchange, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/
- Drawbridge, Cross-device identity service, https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/
- FamilyTreeDNA (Mitosearch and Ysearch), Free and public genetic tools, https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna/
- Gravity Interactive (Ragnarok Online and Dragon Saga), Video game developer, http://blog.warpportal.com/?p=10892
- Hitman: Absolution, Video game developed by IO Interactive, https://www.ioi.dk/hitman-absolution-service-message/
- Klout, Social reputation service by Lithium, https://www.relevance.com/lithium-ends-klout-gdpr/
- Loadout, Video game developed by Edge of Reality, https://www.gamesindustry.biz/articles/2018-05-09-gdpr-spells-closure-for-free-to-play-shooter-loadout
- Monal, XMPP chat app, https://monal.im/blog/gdpr-removing-monal-from-the-eu/
- MotoSport, Powersports retailer, https://static-content.motosport.com/GDPR/index.html
- Parity, Know-your-customer service for initial coin offerings (ICOs), https://www.parity.io/picops-discontinued-may-24th-2018/
- Payver, Dashcam app, https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04
- Pottery Barn, Housewares retailer, https://www.apnews.com/6b2b86fd88d147179aac7e7582942c15
- Seznam, Social network for students, https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html
- Steel Root, Cybersecurity and IT services, https://twitter.com/steel_root/status/992740684250648576
- StreetLend, Tool sharing platform for neighbors, http://web.archive.org/web/20190423095016/https:/www.streetlend.com/

These foregone benefits must be accounted for in assessing the full implications of more invasive privacy regimes. Imposing broad, general regulations regarding business models and privacy practices is a surefire way to curtail innovation and reduce overall competition. This inevitably will lead to a handful of large firms that are able to dominate a space as network effects will reinforce their success, and a lack of differentiation along privacy and advertising dimensions will discourage or outright forbid experimentation with novel business models.

IV. Liability for algorithmic decision-making

Seeking to punish firms for "harming" consumers by focusing on the opacity of the algorithms used in commission of the alleged harm is a fraught exercise. Moreover, in addition to some algorithms being designed in a way not amenable to reverse engineering in order to detect the exact source of bias in the code, many, if not most, viable algorithms are proprietary.[124] Thus, even where regulatory interventions into the operation of an algorithm were possible, such interventions could run afoul of the legal protections afforded to private property.

To overcome these problems, some researchers are attempting to develop means of testing the bias of algorithms using proxies and educated guesses.[125] Yet, even assuming we can reliably detect algorithmic biases in such a way, two problems complicate the regulation of bias in algorithms. First, probing the "state of mind" of algorithms to determine the *why* of a particular algorithmic output holds a computer program to a higher standard than we hold even morally culpable humans. Second, focusing on the operation of the algorithms shifts the focus away from the practically relevant level of legal analysis: we should care about the existence of harms and the deterrence

---

- Super Monday Night Combat (SMNC), Video game developed by Uber Entertainment, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr
- Tunngle, Video game VPN, https://www.bbc.com/news/technology-44239126
- Unroll.me, Inbox management app, https://techcrunch.com/2018/05/05/unroll-me-to-close-to-eu-users-saying-it-cant-comply-with-gdpr/
- Verve, Mobile programmatic advertising, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr
- Williams-Sonoma, Housewares retailer, https://apnews.com/3b6945f9f5794d87bb5c78bb093f724a

[124] Sarah Tan et al., Distill-and-Compare: Auditing Black-Box Models Using Transparent Model Distillation, ARXIV (2018).

[125] *See*, e.g., *Id.*; *See also* Kartik Hosanagar and Vivian Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire*, HARVARD BUSINESS REVIEW (Jul. 23, 2018), *available at https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire*

of those harms, not the particular means by which an algorithm reached a harmful end.

F. Liability and black box processes

Calls for "algorithmic transparency"[126] to reduce bias in decision-making quickly run into an obvious issue: the human brain is just as much of a "black box," from a legal perspective, as are opaque computer programs. We frequently know just as little about the choices that humans make as we do about those made by computer algorithms, particularly when they are powered by machine learning or other artificial intelligence techniques.[127]

This raises an important question: Why should we apply a double standard to artificial intelligence when human intelligence is also biased and non-transparent? Vijay Pande, a partner at venture capital firm Andreessen Horowitz aptly frames the problem with an example from the healthcare industry:

> Let's take the example of a human doctor making a diagnosis. Afterward, a patient might ask that doctor how she made that diagnosis, and she would probably share some of the data she used to draw her conclusion. But could she really explain how and why she made that decision, what specific data from what studies she drew on, what observations from her training or mentors influenced her, what tacit knowledge she gleaned from her own and her colleagues' shared experiences and how all of this combined into that precise insight? Sure, she'd probably give a few indicators about what pointed her in a certain direction—but there would also be an element of guessing, of following hunches. And even if there weren't, we still wouldn't know that there weren't other factors involved of which she wasn't even consciously aware.[128]

Programs designed to draw inferences through machine learning or other statistical or computational methods use what we can think of as "hunches" about large sets of data. Those programs might get the result wrong, and some

---

[126] *Algorithmic Transparency: End Secret Profiling*, EPIC, https://epic.org/algorithmic-transparency/ (last visited May 30, 2019).

[127] See Hosanagar and Jair, *supra,* note 125.

[128] Vijay Pande, *Artificial Intelligence's 'Black Box' Is Nothing to Fear*, NY TIMES, Jan. 25, 2018.

harm might arise. But the problem is no different than a human being who draws mistaken hunches based on his own experience.

G. Focus on algorithmic accountability instead of algorithmic transparency

To the extent that cognizable harms arise out of the behavior of opaque algorithms, careful application of liability principles—without resort to probing the state of "mind" of the algorithm—coupled with incentives to develop appropriate insurance and other private risk mitigation strategies would likely give rise to an optimal regulatory environment.

A regulation requiring algorithmic transparency would be challenging to apply in practice. For example, it's not as simple as banning the use of certain data as an input:

> Sometimes we are interested in detecting bias on features intentionally excluded from the black-box model. For example, a credit risk scoring model is probably not allowed to use race as an input. **Unfortunately, not using race does not prevent the model from learning to be biased**. Racial bias in a data set is likely to be in the outcomes—the labels used for learning; not using race as an input feature does not remove the bias from the labels.[129]

Thus, even if the algorithm is constrained from directly using certain categories of data, the results may still reflect the use of correlated proxies for those prohibited categories. Indeed, not including the prohibited category can make it more difficult to identify the source of the bias. However, no matter the algorithm used, we can always observe the *outputs* of the process, assess any harms produced, and assign liability based on observed outcomes that we deem to be illegal.[130]

Thus, a better alternative to mandating algorithmic transparency (were it even possible) is to pursue "algorithmic accountability."[131] Although these two concepts have occasionally been conflated, they are not synonymous. As Joshua New and Daniel Castro of the Center for Data Innovation note, algorithmic accountability is "the

---

[129] Tan et al., *supra* note 124 at 6 (emphasis added).

[130] Although controversial, this approach may end up mirroring the 'disparate impact' analysis the Supreme Court sometimes employs in civil rights analysis. *See, e.g.,* Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Communities Project, Inc., 135 S. Ct. 2507, 2518 (2015) (Disparate impact can be used when assessing claims under the Fair Housing Act). A full discussion of this potential is beyond the scope of this Comment, but deserves careful consideration.

[131] Curt Levey and Ryan Hagemann, *Algorithms with Minds of Their Own*, WALL ST. J., Nov. 12, 2017.

principle that an algorithmic system should employ a variety of controls to ensure the operator (i.e., the party responsible for deploying the algorithm) can verify it acts in accordance with its intentions, as well as identify and rectify harmful outcomes."[132] Whereas algorithmic transparency focuses disclosure requirements, algorithmic accountability focuses on what truly matters: harmful outcomes.

If a liability regime is properly designed, the developers and their customers will necessarily adjust the operation of algorithms to reach more socially optimal outcomes.

Indeed, this approach would be consistent with jurisprudence in other areas of our legal system. Certain crimes, for example, do not hinge on a scienter, or "state of mind" requirement. In many states, the crime of statutory rape, for example, is complete when one of sufficient age has sexual congress with one of insufficient age, regardless of what either party thought or intended.[133]

Focusing on algorithmic accountability as opposed to algorithmic transparency is analogous. Inquiring into the *why* of an algorithm's decisions probes either the intent of the computer or the intent of the programmer using the algorithm's behavior as a proxy. But it is essentially irrelevant what an algorithm "thought" at any one point: we only care that the harm it caused could have been avoided, and if it was not avoided that the law can make injured parties whole.

And this highlights a critical point: in order to assign liability, particular harms need to be identified. It is not enough to merely point to the existence of individualized marketing, risk scoring, or differential pricing and declare the outputs of an algorithm to be improper. Many such practices have benefits as well as costs. Differential pricing, for example, can be beneficial when it is used to facilitate the development of a market by bringing in consumers who would otherwise have been priced out of the market.[134] Individualized marketing can be illegally discriminatory,[135] but it can also be broadly beneficial when it helps to connect firms to consumers who are genuinely interested in their goods and services. Conduct ought to be challenged based on its actual effects, and the theories of harm employed must be sufficiently specified

---

[132] Joshua New and Daniel Castro, *How Policymakers Can Foster Algorithmic Accountability*, Center for Data Innovation (2018), pp. 1-2, *available at* http://www2.datainnovation.org/2018-algorithmicaccountability.pdf.

[133] *See, e.g.*, Model Penal Code § 213.1 (1)(c)(i).

[134] See note 104 and accompanying text.

[135] *See, e.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2008).

such that firms can reasonable determine when their conduct—and not merely the abstract design of their algorithms—runs afoul of the law.

Once harms are well-defined, a more tailored liability regime can then be developed. It may make sense to focus liability on the operators of algorithms—as opposed to developers—since they are "least cost avoiders."[136] This is largely an empirical question, however, dependent on the party with the greatest degree of control over the operation of algorithms, as well as the party best positioned to recover its own losses through contractual protections. For example, an algorithmic operator may indeed be the best party to assume liability for harms that arise out of algorithmic bias (as opposed to a developer), because they most easily control the deployment of the algorithms and are most likely to be able to guarantee contractual indemnification from the developers. Moreover, having control over both deployment as well as contractual protections, they are the party that may have the easiest time completing an insurance underwriting process that helps pool the risk of algorithmic harms across a large number of similarly situated firms.[137]

V. Conclusion

Given the complications confronting privacy regulation, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Commission has historically taken, and which has, generally, yielded a stable, evenly administered regime: case-by-case examination of actual privacy harms and a minimalist approach to ex ante, proscriptive or prescriptive regulations, coupled with narrow legislation targeted at unambiguously problematic uses of personal information. For all its imperfections, following this approach will allow authorities to balance flexibility and protection, without stumbling into the unintended and harmful consequences that would surely arise from a more restrictive regulatory approach.

---

[136] New and Castro, *supra* note 132.

[137] Note, we are not offering this as a conclusion because, again, this is an empirical question. Instead, this discussion is meant to underscore the paucity of proposals that aim to attach liability based on the internal mechanisms of an algorithm, as opposed to its impact on the world, and the parties best able to handle that impact. For a similar discussion of tailoring a liability regime to encourage optimal cybersecurity protections and damage recovery, see generally, Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 5 (2017).