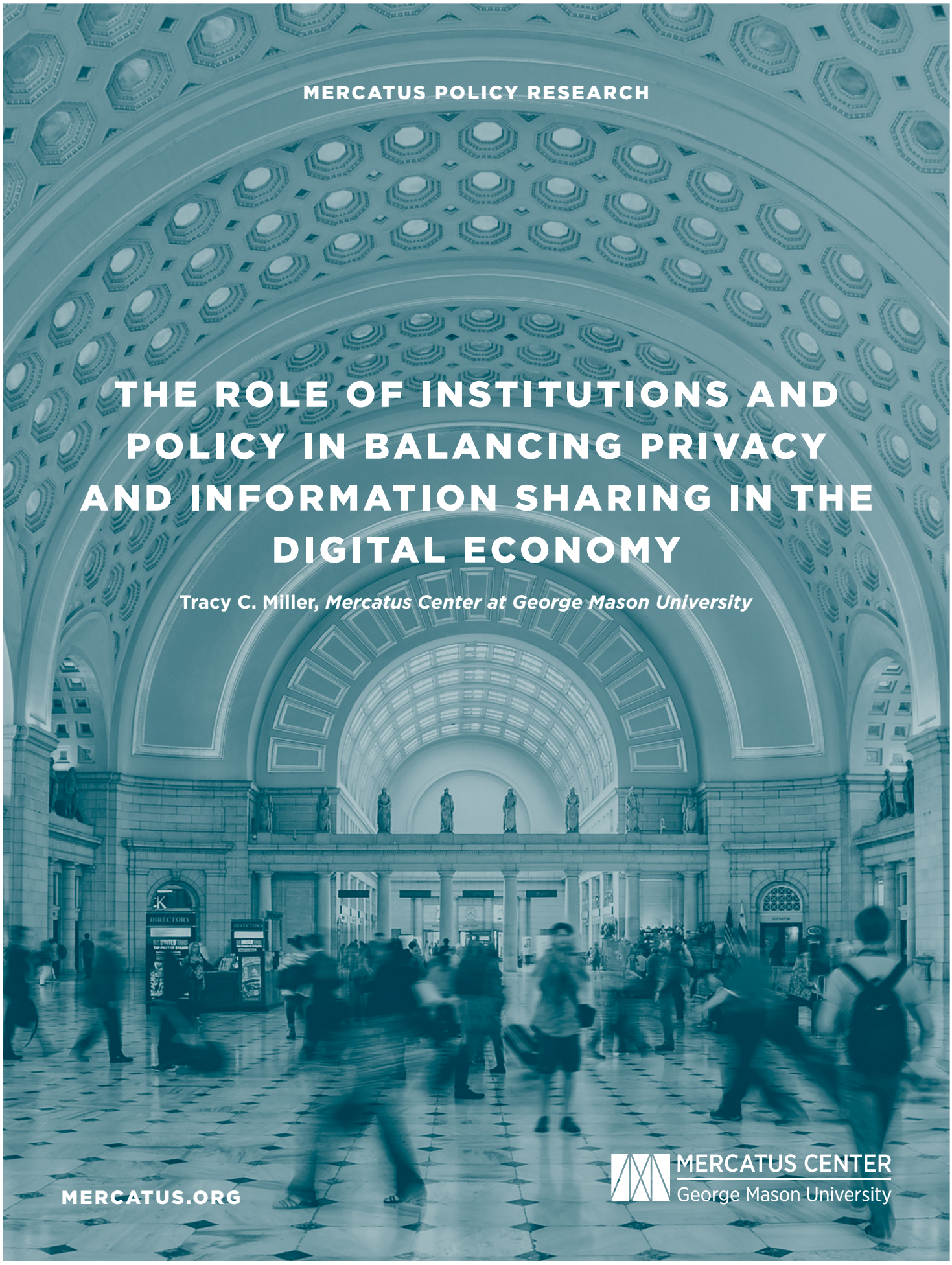

MERCATUS POLICY RESEARCH

THE ROLE OF INSTITUTIONS AND POLICY IN BALANCING PRIVACY AND INFORMATION SHARING IN THE DIGITAL ECONOMY

Tracy C. Miller, *Mercatus Center at George Mason University*

MERCATUS.ORG

MERCATUS CENTER
George Mason University

Tracy C. Miller. "The Role of Institutions and Policy in Balancing Privacy and Information Sharing in the Digital Economy." Mercatus Policy Research, Mercatus Center at George Mason University, Arlington, VA, October 2022.

ABSTRACT

Today's online economy relies on exchanges of data for services. Online service providers collect personal data to earn revenue from targeted advertising. Many users of online services are concerned that their data might be used in ways contrary to their interests, interfering with their privacy. This research focuses on online data collection, processing, disclosure, and use by private companies, and it considers both costs and benefits. Privacy policy in the United States places too much emphasis on notice and consent, which raises transaction costs without doing enough to protect online users from the risks associated with disclosing personal data online. More stringent privacy regulation similar to the European Union's General Data Protection Regulation would impose substantial costs on firms, making it harder for small firms to compete against dominant platforms, such as Google and Facebook. This paper argues for permissive privacy policy that does not discourage collection and processing of personal information for online advertising. A better approach is continued case-by-case FTC regulation combined with expanded legal liability of data controllers for data practices that subject a user to specific and significant harm or risk of harm. This approach could be combined with fiduciary responsibilities for firms that collect large amounts of personal information.

JEL codes: H1, H7, K2, K4, L1, M3, O3.

Keywords: Privacy, competition, fiduciary, class action, liability, Federal Trade Commission, common law, negligence, privacy norms, notice and consent, self-regulation, behavioral advertising

Policy toward online privacy is an important and contentious issue. Many people are concerned about the loss of control over their data and the possibility that information about them is used in ways that are harmful to their interests. In response to concerns about privacy and data security, several states have passed comprehensive data protection laws, and others are considering doing so. These laws emphasize giving consumers more control over what online service providers may do with their personal data. Stricter privacy regulation, however, could reduce the incentives of digital platform companies to provide the enormous variety of information and online services they now provide free of charge.

Many online services are provided in exchange for data collected about users of those services (data subjects). Such pay-with-data arrangements are problematic in several respects. The cost to the data subject of disclosing personal information online is highly uncertain. The data subject gains a tangible benefit in exchange for an uncertain future cost. Users of online services have little choice but to disclose substantial amounts of personal information to participate fully in social and economic life. In light of the problems with pay-with-data arrangements, what changes in policy can better protect the privacy interests of consumers of online services while maintaining competition and incentives for innovation in this market?

Some privacy proponents advocate stricter privacy regulation and point to the European Union's General Data Protection Regulation (GDPR) as an example. But the kind of rules that are most prominent in the GDPR and some state privacy regulations raise the transaction costs of collecting, processing, and using online data. As a result, they have the potential to discourage some information flows that are mutually beneficial. A more productive alternative

to designing privacy regulation that restricts the flow of information is to enact regulation that ensures that information flows appropriately.[1]

This research paper starts by considering the nature of privacy problems, beginning with a discussion of the privacy paradox. It then discusses ethical considerations in privacy policy. Next it discusses how market participants and governments seek to overcome problems and conflicts related to privacy. Specifically, it discusses general principles that guide policy toward privacy, including principles related to the role of privacy self-management. Following that is a discussion of how US privacy policy is governed. Next is a discussion of how to promote better data protection practices, which considers the role of self-regulation, legislation, Federal Trade Commission (FTC) regulation, and evolution of the common law in response to changes in technology and its effects on privacy. This paper argues for policy that relies less on notice and consent, expands privacy torts via court decisions, and continues but limits the role of the FTC in regulating privacy. Such policy should be supplemented with legislation that prohibits data practices that subject a user to specific and significant harm or risk of harm. Congress or state legislatures should consider imposing fiduciary obligations on online service providers that deal extensively with personal data.

UNDERSTANDING PRIVACY PROBLEMS

A variety of problems are often discussed under the rubric of privacy. These include concerns about the collection and use of personal data by digital platforms, personal information made public by the media, data breaches that may lead to identity theft, aggregation of data to profile people for marketing and other purposes, and surveillance by government authorities. This research focuses largely on the collection and use of data by private companies, including the ways that data may be sold and aggregated.

The Privacy Paradox

People reveal data about themselves online in a variety of ways, such as searching for information, buying and selling products online, choosing friends, posting information, responding to others' posts on social media, and sending emails. In each case, they voluntarily choose to engage with online platforms.

1. This important principle is discussed in Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), 2.

People's choices about disclosing personal information online seem to contrast with the desire to protect their privacy that they reveal in surveys, giving rise to the notion that there is a privacy paradox. Concern about a paradox is based on the results of numerous studies showing a discrepancy between users' preferences and their actual behavior.[2]

Because most people regularly trade their data for online services, their choices presumably reflect how they weigh the expected costs or risks of lost privacy resulting from information collected about them against the expected benefits of the services they receive in exchange. Critics of privacy regulation use this presumption to argue that regulation that might limit such exchanges "overvalues privacy."[3] James Cooper, director of the Program on Economics and Privacy at the Antonin Scalia Law School, argues that the FTC should curtail its privacy regulation in light of people's revealed preferences.[4]

Others, however, argue that more privacy regulation is needed, because in making decisions that result in disclosing their personal data, consumers often make choices that are not consistent with their interests. Daniel Solove argues that people have biases that often result in irrational decisions and that misunderstanding, lack of knowledge, and behavioral manipulation also play an important role in contributing to many consumers' making less-than-optimal decisions about privacy.[5] He also argues that giving people more information and better options for managing their own privacy will not be very effective in countering "distorting influences" on their behavior.[6]

The privacy paradox is the apparent discrepancy between people's statements about the value of privacy and the little value they ascribe to it in their online behavior. But there are several possible explanations for this. One is that although people place a high value on privacy in general, they place a much lower value on the perceived loss of privacy from particular transactions in which they engage. Of greatest concern are those explanations that argue that, with existing institutions and policies, many consumers are unable to make a tradeoff that is consistent with their preferences between privacy and the other goods and services they obtain online in exchange for it.

---

2. For a literature review, see Susanne Barth and Menno D. T. de Jong, "The Privacy Paradox," *Telematics and Informatics* 34, no. 7 (2017): 1038–58.
3. Daniel J. Solove, "The Myth of the Privacy Paradox," *George Washington Law Review* 89, no. 1 (2021): 33.
4. James C. Cooper, *Lessons from Antitrust: The Path to a More Coherent Privacy Policy* (Washington, DC: US Chamber of Commerce Foundation, 2017).
5. Solove, "The Myth of the Privacy Paradox," 15–16.
6. Solove, "The Myth of the Privacy Paradox," 42.

One argument is that people do not do enough to protect their privacy because of asymmetric information about the privacy risks associated with individual decisions, often resulting in their underestimating those risks. A more encompassing argument is that people's decisions are affected by systematic psychological deviations from rationality.[7] The ways that people deviate from rationality include lack of self-control, optimism bias, and a tendency to underinsure against risks, among others.

The view that people make decisions that systematically deviate from rationality gives rise to proposals for soft paternalistic policies to help people make better decisions. Many proponents of this view argue for tools such as nudges to alter behavior. Nudges are interventions "that alter [] people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[8] Nudging people to disclose more or less online data can be accomplished with information, presentation, or the choice of defaults (usually opt-in or opt-out).[9] But even if one accepts the proposition that behavior deviates from rationality, the question still remains, who decides whether people should be nudged in the direction of more or less information disclosure?

Based on experimental evidence, Kirsten Martin contends that "consumers are not acting paradoxically when going online."[10] The case for the existence of a paradox rests on the assumption that consumers, if they decide to disclose information, are relinquishing privacy.[11] She argues that instead consumers continue to expect privacy after they disclose information online. She demonstrates that many consumers view privacy as a core value and expect firms to respect privacy norms in terms of how they collect, distribute, and use information collected in a particular context.[12] She shows that consumers are less likely to engage with firms that violate privacy norms by using the data they collect in certain ways. Even if there is not a paradox, questions remain about whether changes in policy

7. Daniel Kahneman and Amos Tversky, eds., *Choices, Values and Frames* (New York: Cambridge University Press, 2000), cited in Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality: A Survey," in *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, ed. Katherine J. Strandburg and Daniela Stan Raicu (New York: Springer, 2006).
8. Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New York: Penguin Books, 2009), 6.
9. Athina Ioannou et al., "Privacy Nudges for Disclosure of Personal Information: A Systematic Literature Review and Meta-analysis," *PLoS ONE* 16, no. 8 (2021): e0256822.
10. Kirsten Martin, "Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms," *Business Ethics Quarterly* 30, no. 1 (2020): 66.
11. Martin, "Breaking the Privacy Paradox," 69.
12. Martin, "Breaking the Privacy Paradox," 70.

could more effectively motivate firms to use the data they collect in ways that do not violate consumers' privacy expectations.

The Nature of Privacy Problems

Taking steps to protect privacy is costly. Because of the large number of online interactions they engage in, most consumers are unwilling to take the time to carefully read and understand what firms may do with their data. Firms do not negotiate with users about what will be done with their data; they offer contracts of adhesion, which are usually take-it-or-leave-it deals. If users desire a service offered by a platform, they disclose whatever information the website requests without giving much thought to the consequences.

Consumers who decide whether to provide their data to a firm on the basis of its privacy policy may find that the firm changes that policy without providing adequate notice or seeking their consent. Once they have developed an ongoing relationship of sharing their data with an online service provider, it may be very costly for them to switch to a different one.

Much of data that are collected online are intended for use in online behavioral advertising, where the ads users see depend on advertisers' inferring users' interests from data collected about them. Behavioral targeting has some advantages in that the ads served to each user are more likely to be for products that individuals value. Nevertheless, some consumers consider themselves to be more vulnerable and demonstrate reluctance to click on personalized ads if their data were collected covertly.[13]

A major problem with online data collection is that data subjects cannot be certain how their data will be used in the future. Uses that data subjects do not expect and would not have agreed to if asked often involve substantial risk. The most serious risk may be from data breaches where parties gain unauthorized access to sensitive data that they can use to steal people's identities or otherwise harm such people. There is also a risk that data collected may be sold to third parties who are intent on stalking or harming data subjects. Less risk is involved when the entity that collects the data has implicit or explicit permission of the data subject to use the data for legitimate commercial purposes. But there is still a question of whether the intentions of the firm that collects or processes the data are consistent with the expectations of the data subject. And there is also the

13. Elizabeth Aguirre et al., "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing* 91, no. 1 (2015): 34–49.

possibility that the entity that collects or acquires the data will use the data for a purpose that it had not planned on when it first collected the data.

In some cases, online businesses may use data they have accumulated from various sources to price discriminate or otherwise gain a bargaining advantage in transactions with data subjects. The data could also be used to restrict opportunities for data subjects, such as in decisions to grant credit or provide insurance.

The amount of risk of information being misused by parties who acquire it legitimately is questionable. For example, some kinds of price discrimination may be facilitated by the information firms have collected from online profiles, but in many cases, charging different prices to different consumers benefits some consumers and may not be morally objectionable. Online discrimination is likely to be based largely on "less problematic criteria like purchasing patterns, social affiliations, criminal histories, insolvency records, and Internet browsing behavior" rather than on questionable criteria such as race, gender and age.[14] Firms providing credit and insurance are legally authorized to collect certain kinds of data, but problems arise if the data subject is not aware of what additional data those firms may have collected from online sources and if they use those data in a way that is not considered legitimate for making a particular decision.

The largest cost for those who are anxious about privacy may be the uncertainty concerning how their data will be used. This uncertainty is exacerbated by the role of third parties such as data brokers, who process and disseminate data but have no direct connections to the data subjects. Legislation that makes it easier for data subjects to get information about how their data will be used or assurance that there are enforceable limits to what firms will do with the data will benefit at least a large subset of the population.

Privacy as an Ethical Issue

Privacy is, fundamentally, an ethical issue. Respecting privacy involves being constrained by "the implicit privacy norms about what, why, and to whom information is shared within specific relationships."[15] Technology that disregards entrenched norms threatens to disrupt "the very fabric of social life."[16] According to this view, society should seek "a world in which [its] expectations about

14. Lior Strahilevitz, "Reputation Nation: Law in an Era of Ubiquitous Personal Information," *Northwestern University Law Review* 102, no. 4 (2008): 1676.
15. Kirsten Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics* 137, no. 3 (2016): 551.
16. Nissenbaum, *Privacy in Context*, 3.

the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones."[17]

But in pluralistic society, not everyone's expectation can be met. Martin suggests viewing privacy norms as "mutually beneficial and sustainable agreements within a community" about sharing information.[18] She explores a social contract view of privacy, which suggests that information exchanges within communities should be governed by "communities' locally negotiated norms."[19]

Technology has made possible aggregation and analysis of data in ways that have significantly altered entrenched information flows by altering who receives data, the principles that govern data transmission, and the kind of information that flows from one party to another.[20] Some of these changes may violate existing norms. The question then becomes how to respond to violations of norms.

As people become informed about data collection and processing, one response is public outcries against those ventures that many people find offensive. An example of this is illustrated by what happened in response to a joint venture by Lotus Development Corporation and Equifax, Inc., to create a database, the Lotus Marketplace: Households, that would contain information about households that could be used by marketers and mail-order companies.[21] The database would have used public records along with inferences to compile information about 120 million individuals that includes name, address, type of dwelling, marital status, gender, age, estimated household income, lifestyle, and purchasing propensity. This venture provoked substantial public opposition and was canceled before the database was compiled.[22]

The public reaction to the Lotus Marketplace: Households database illustrates that the public did not recognize a simple dichotomy between public and private information as the basis for whether information sharing is acceptable. Even though all the information that would have been used was compiled or inferred from public sources, a large number of people recognized the venture as a violation of a norm. Digital technology has radically altered the way information can be accessed, so many people who could be affected by its disclosure

17. Nissenbaum, 231.
18. Martin, "Understanding Privacy Online," 553.
19. Martin, 554.
20. Nissenbaum, *Privacy in Context*, 204.
21. Laura J. Gurak, *Persuasion on Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* (New Haven, CT: Yale University Press, 1997).
22. Gurak, *Persuasion on Privacy in Cyberspace*.

view combining different kinds of information, which is available from different public sources, as a violation of privacy. In recent cases, courts have not shown a similarly nuanced view that even though individual pieces of information are public, using technology to combine and distribute them as profiles of people may not be appropriate.

Even if certain innovative practices do not violate any existing law, those that violate norms can provoke popular opposition that is strong enough to motivate companies to change their plans. But business and government interests in accumulating and using personal information often prevail in the face of public opposition.[23]

The question is, when does violation of privacy norms justify government using its coercive power to prohibit or penalize certain kinds of collection, processing, or dissemination of personal information? One answer is that when public opposition is insufficient to motivate companies to change their practices, a response through law and public policy may be called for, particularly if "violations are widespread and systematic" and motivated by self-interest and if the parties "perpetrating the violations are overwhelmingly more powerful or wealthy."[24] Another view argues that government should not intervene except in cases where data are used to harm someone or are collected, processed, used, or disseminated in violation of the terms of a contract.

When firms violate consumer expectations in their privacy practices, consumers may adjust their expectations if they become convinced that the benefits outweigh the costs of the ways firms are using the data.[25] For those consumers who view the benefits as less than the costs, opting out of doing business with those firms may be an adequate solution.

Any attempts to limit information collection involve tradeoffs. To the extent that regulations limit how firms can use and collect data to earn revenue, the result may be higher prices or lower quality of goods and services available online. In addition to trading access to low- or zero-priced goods and services for reduced risks to privacy, privacy regulation that requires an opt out or opt in may raise transaction costs to firms of attracting consumers and to consumers of accessing websites and associated goods and services.

23. Nissenbaum, *Privacy in Context*, 8.
24. Nissenbaum, 237.
25. When popular opposition to certain practices subsides, does it subside because expectations have changed or because opponents have become demoralized?

HOW LAW HAS RESPONDED TO PRIVACY PROBLEMS

The collection and use of data for commercial purposes involves an exchange relationship between consumers and firms that collect their data. If consumers and data controllers were to enter into complete contracts, the "parties would specify the entitlements and duties associated with all possible contingencies" concerning the collection, processing, use and storage of personal information.[26] But real-world contracts are incomplete, so disputes ultimately arise that courts and government officials must address. Even when contracts are well-specified, with detailed privacy terms spelled out, the cost of reading those contracts and giving meaningful assent likely exceeds the benefits for many consumers.

As noted earlier, online platforms rely largely on contracts of adhesion, which are presented by sellers "in a take-it-or-leave-it form" and contain standard clauses.[27] Some consumers who agree to such a contract might not have read and understood its terms. The contract may contain important clauses those consumers would not have consented to if they had known those clauses were included in it. Governments should and often do intervene by law to invalidate unfair clauses that have not been negotiated in such contracts.[28] But US legislation has provided only "weak protection against unfair clauses."[29]

Privacy regulation in the United States emphasizes privacy self-management—i.e., users' making decisions about disclosing data in light of information provided by online service providers about their privacy policies. The FTC, which plays an important role in regulating privacy, recommends that businesses collecting user information abide by fair information practice principles (FIPPs), particularly providing notice of their privacy policies to consumers who then may choose whether to engage with those firms. In a number of cases, the FTC has initiated enforcement actions against firms for providing insufficient notice of their practices that affect data privacy.

The problem with privacy self-management is that most people deal with hundreds of firms that collect and use their data for various purposes. Some of the firms that collect and process personal data, such as data brokers, may be unknown to users because they do not directly interact with users. Once data

---

26. Richard R. W. Brooks, "Observability and Verifiability: Informing the Information Fiduciary" (unpublished manuscript, October 9, 2015), PDF file, 17, https://www.law.uchicago.edu/files/file/brooks_observability_verifiability.pdf.
27. Elena D'Agostino, "The Unconscionability Doctrine in a Law and Economics Perspective," in *Contracts of Adhesion between Law and Economics: Rethinking the Unconscionability Doctrine* (Heidelberg: Springer, 2015), 2.
28. D'Agostino, "The Unconscionability Doctrine," 5.
29. D'Agostino, "The Unconscionability Doctrine," 57.

have been collected, it is hard to predict how they might be used at some point in the future. And the data aggregation process means that the relationship between information collected about consumers as part of individual transactions and the profile that is constructed is often different than what consumers might expect. Most consumers are not willing to spend the time to adequately assess the privacy risks that they may face as a result of deciding to interact with an online service provider. These risks are "often vague, abstract, and uncertain" and thus hard to compare with the easily identifiable benefits of sharing personal data.[30] The similarities of different companies' privacy policies means that consumers usually do not have the option of choosing among policies that are more or less protective of their privacy.[31] The value of differences in the price or quality of products and services offered by competing firms often exceeds the value to consumers of any differences in their privacy policies.

A different approach than privacy self-management may be more effective in limiting the risks consumers face when they interact with online service providers. One approach is to rely on rules that specify what online firms can and cannot do with data they collect about users. This could include regulating the transfer of data to third parties and requiring that firms process and use data only in ways consistent with their stated purpose of collecting such data.[32] The GDPR includes a number of ex ante rules, which restrict what firms can do with data, but firms may be able to circumvent many of them by obtaining consent from consumers. If government enforces rules with no room for consumers and firms to negotiate exceptions, those rules may discourage mutually beneficial or innovative information exchanges. In the United States, if government were to implement strict restrictions on data collection and use, businesses may respond by taking legal action using the First Amendment to defend their freedom to use the data they collect.[33] The First Amendment limits what the federal government can do because laws that restrict data collection would be a prior restraint on speech. The European Union does not have such a strong constraint on government action to protect privacy.

An alternative approach that may be more flexible than ex ante rules would be to hold firms liable for using data in a way that harms data subjects. Unlike leg-

30. Solove, "The Myth of the Privacy Paradox," 44.
31. John A. Rothchild, "Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)," *Cleveland State Law Review* 66, no. 3 (2018): 559–648.
32. Solove, "The Myth of the Privacy Paradox," 49.
33. Jack M. Balkin, "Information Fiduciaries and the First Amendment," *UC Davis Law Review* 49, no. 4 (2016): 1183–239.

islation spelling out how firms may collect, process, and distribute data, liability rules focus on whether firms protect data enough to avoid harmful consequences for data subjects. To be effective, liability rules may need to be accompanied with a recognition that certain kinds of firms that collect, process, or use large amounts of personal information have fiduciary obligations toward data subjects. By definition, a fiduciary has a duty of care and a duty of loyalty toward its clients.[34] Imposing fiduciary obligations is one way to protect freedom of speech while also applying general principles to protect the interests of data subjects.[35]

Restrictions on how firms may use data and liability rules emphasize that privacy problems arise from what firms do with data after they collect such data. If, after consumers consent to allow firms to collect personal data, those firms are not accountable in some way for what they do with the data, then they are more likely to use the data in a way that harms data subjects. Exchanging data for online services leaves data subjects vulnerable to uses of their personal information that can harm their interests after the data have been transferred.[36] Without additional rules or liability, firms that acquire data may have insufficient incentives to consider the interests of data subjects in deciding what to do with the data collected about them.

One important question is whether the law should prohibit or restrict surreptitiously collecting data. Technology has made it easier to profitably use such data and combine them with other data about a person. Roger Ford refers to the example of using cell phones to track shoppers' location in shopping malls without their permission, which is an example of what he calls a "unilateral invasion of privacy."[37] To counter this, the law, including FTC regulation, has largely focused on requiring data controllers to notify consumers about how they collect data and to obtain consumers' consent.

Some proponents of stricter privacy regulation argue that policy toward private-sector invasions of privacy may overemphasize self-management. Even if every firm that collects data from users of personal computers and mobile devices is required to inform data subjects and seek their consent, it may be too costly for data subjects to understand the possible consequences resulting from the use of their data and to make good decisions about allowing their data to be

34. Richard Whitt, "Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era," *Santa Clara High Tech Law Journal* 36, no. 1 (2019): 75–131. Whitt notes that in most cases, for information fiduciaries to carry out their duty of care, they must also maintain confidentiality of users' information.
35. Balkin, "Information Fiduciaries and the First Amendment."
36. Ignacio Cofone, "Beyond Data Ownership," *Cardozo Law Review* 43, no. 2 (2021): 501–72.
37. Roger Ford, "Unilateral Invasions of Privacy," *Notre Dame Law Review* 91, no. 3 (2016): 1077.

collected and used in each specific situation. For this reason, a better approach may be to change the incentives of the outside entities who make decisions about collecting, disseminating, and using those data.[38] If particular kinds of decisions by outside entities were to not give enough weight to the benefits to the data subject of restricting information flows, then government could raise the costs of collecting, disseminating, or using data by those entities. Government could accomplish this by imposing disclosure or opt-in requirements, taxing certain kinds of information flows, and banning others.[39]

The GDPR and privacy legislation in several states raise the cost of collecting and processing sensitive personal data by imposing opt-in requirements. Sensitive data usually include racial or ethnic origin, religious beliefs, mental or physical health, sexual orientation, immigration status, and biometric data.[40] The GDPR also includes political opinions and union membership as sensitive data.

Another important type of privacy problem that may warrant ex ante rules is where one party has disproportionate power and may use it to take advantage of another. Outside of the realm of public discourse, where the First Amendment treats everyone as equally competent, the law specially protects those who are vulnerable.[41] This is why advertising, which is not considered public discourse, is regulated so that firms are compelled to disclose certain kinds of information and are prohibited from misleading consumers in advertisements. Where data subjects are vulnerable, stricter privacy regulation may be warranted. This is part of the rationale for the Children's Online Privacy Protection Act (COPPA). Whether the law should treat adults as vulnerable is questionable.

HOW IS US PRIVACY POLICY GOVERNED?

The Role of Market Forces and Self-Regulation

In the United States, especially in the early years of this century, powerful political resistance limited the enactment of information privacy law, especially law directed at practices of the private sector.[42] Instead of reflecting government

38. Ford, "Unilateral Invasions of Privacy."
39. Ford, "Unilateral Invasions of Privacy," 1109.
40. "Privacy Law Comparison," WireWheel, accessed September 28, 2022, https://wirewheel.io/resource/privacy-law-comparison/.
41. Free speech rules apply to public discourse in a way that they do not to other kinds of communication. See Robert C. Post, *Democracy, Expertise and Academic Freedom: A First Amendment Jurisprudence for the Modern State* (New Haven, CT: Yale University Press, 2012), 15.
42. Colin J. Bennett and Charles D. Raab, "Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective," *Regulation and Governance* 14, no. 3 (2020): 453.

regulation and enforcement, privacy policies and practices largely reflected firm decisions about collecting, using, and disseminating data in response to market competition and industry self-regulation.

How firms collect, process, and use information depends partly on the computer code that governs online interaction. An important question is how the software and hardware that make cyberspace what it is regulate cyberspace as it is.[43] Computer code (the architecture of cyberspace) imposes limits on how governments can regulate interaction on the internet. Government regulation can alter the architecture of the internet, but the existing architecture constrains the government's ability to enforce regulation of data collection and the kind of regulation that will be most effective. Self-regulation can influence firm- and industry-level decisions about code with impacts on firm privacy practices. Competition can also play a role as dominant firms, such as Apple, make decisions that can influence the architecture of cyberspace and affect how easily other online firms can collect data from consumers who use complementary services, such as operating systems, that the dominant firms provide.[44]

Although privacy proponents have argued that internet users who desire more privacy often lack options, Apple's introduction of App Tracking Transparency (ATT) and mandatory Privacy Nutrition Labels as part of iOS 14 illustrate how entrepreneurs respond with new options if enough consumers value greater privacy protection than is being provided by the firms with which they currently do business. Apple has recently sought to communicate to iPhone and iPad users various updates and settings on its devices designed to protect the privacy of email, transaction history, location data, contact lists, and browsing history.[45] Apple's ATT framework includes a mandatory opt-in system for enabling tracking on iOS, and its Privacy Nutrition Labels require app developers to self-declare the kinds of data they collect and for what purposes.[46]

If enough consumers value privacy, entrepreneurs are likely to develop better approaches to help consumers achieve their privacy preferences at an affordable cost. Even if most consumers do not read privacy policies, those policies are spelled out in enough detail that users who care about privacy can find

43. Lawrence Lessig, *Code: And other laws of Cyberspace* (New York: Basic Books, 1999), 6.
44. For an example of this, see Garrett Sloane, "What Apple's iPhone Update Means for the Ad Industry," *Advertising Age* 92, no. 13 (2021): 1–2.
45. "Apple Shows It Takes Privacy Seriously with Campaign Focused on Online Safety," *B&T Magazine*, May 18, 2022.
46. Konrad Kollnig et al., "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels," in *2022 5th ACM Conference on Fairness, Accountability, and Transparency* (New York: Association for Computing Machinery, 2022), 508–20.

all the information they require.[47] This, in turn, gives firms incentives to satisfy the preferences of those who place a high value on privacy.

Network effects may increase the influence of highly informed consumers who care about privacy. Because network effects can go in both directions (contributing to rapid growth or rapid decline in the number who use a given platform), online platforms may realize the importance of not offending users.[48]

In dealing with online service providers that offer less privacy than they desire, users have self-help options. These include managing cookies and using do-not-track functions of browsers. Several services provided by third-parties (ad blockers, virtual private networks [VPNs], or incognito browsing) limit data that can be collected, but they do so at a "cost to underlying product functionality."[49] Competition can motivate entrepreneurs to develop lower-cost ways to satisfy users' privacy preferences. For example, one way to reduce transaction costs of enabling consumers to achieve a desired level of privacy is to provide consumers with a user-selected universal opt-out mechanism that automates the process of deciding whether to share data with a website.[50] In 2018, a group of entrepreneurs applied for a patent for a universal data privacy control management system.[51]

Evidence is mixed on whether doing more to protect privacy helps firms much in competing with their rivals to attract users. But firms can gain some advantages by being transparent about their data collection practices. One experimental study finds that when privacy information is prominently displayed "consumers tend to purchase from online retailers who better protect their privacy."[52]

If people oppose surreptitious collection and use of their personal data, they can choose to respond more favorably to online behavioral advertising presented on websites of firms that are more transparent about the firms' data collection practices. The way consumers respond to personalized ads could give them important leverage over the data collection process. Some research demonstrates that consumers who receive personalized advertising based on data

47. Geoffrey A. Manne, Kristian Stout, and Dirk Auer, *Comments on Developing the Administration's Approach to Consumer Privacy* (Portland, OR: International Center for Law and Economics, 2018).
48. Manne, Stout, and Auer, *Comments on Developing the Administration's Approach*.
49. Manne, Stout, and Auer, 9.
50. Keir Lamont, "Five Burning Questions (and Zero Predictions) for the US State Privacy Landscape in 2022," *Future of Privacy Forum* (blog), January 26, 2022.
51. "Universal Data Privacy Control Management System," Justia Patents, May 1, 2018, https://patents.justia.com/patent/20190342336.
52. Janice Y. Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254–68.

collected covertly perceive themselves to be more vulnerable and are less likely to click-through to the website of the product or service advertised.[53]

In addition to competing to provide better privacy protection, firms may cooperate with each other and self-regulate. Self-regulation is defined as principles or standard practices that are agreed on at the industry or firm level. They include "codes of practice, privacy seals and standards, and data protection impact assessment."[54] An important advantage of self-regulation is that online firms control and design their software and hardware and can make those decisions with a view toward providing some level of privacy to their users. By contrast, omnibus regulation is clumsy and can quickly become obsolete in the rapidly changing world of online commerce.[55]

Outside the United States, there is limited emphasis on the role of self-regulation or market competition for promoting privacy. With the European Union leading the way, many countries have enacted strict information privacy laws, which have produced a "pervasive legal compliance culture within global companies."[56] Because of these laws, the current privacy regime can better be described as one of coregulation. Tools that once served a self-regulatory purpose now serve to augment and implement legal rules.[57] Multinational groups of companies have adopted binding corporate rules to "codify internal rules for the transfer of personal data within a group" in order to conform to data protection legislation of countries in which they do business.[58]

The Role of the FTC

In contrast to the approach to privacy in the European Union and elsewhere, privacy policy in the United States has been described as fragmented. Rather than a unified framework, different kinds of privacy rules and regulations have been applied to different sectors of the economy, such as healthcare, finance, commerce, communications, and law enforcement.[59] Federal regulation has codified some general rules as part of COPPA, which apply to all kinds of personal information about children, but no similar general federal legislation has been enacted pertaining to the privacy of adults' online information.

53. Aguirre et al., "Unraveling the Personalization Paradox."
54. Bennett and Raab, "Revisiting the Governance of Privacy," 454.
55. Bennett and Raab.
56. Bennett and Raab, 453.
57. Bennet and Raab, 454.
58. Bennet and Raab, 454.
59. Nissenbaum, *Privacy in Context*, 238.

The sectoral approach to privacy has some important advantages over the omnibus approach of privacy law in the European Union. It allows for deriving appropriate context-relative rights that vary from one sector to the next.

The FTC has come to play an important role in regulating privacy in the United States in sectors where federal legislation has been enacted and in the rest of the economy as well. In 1999, the FTC recommended that Congress enact legislation that would require firms to develop privacy practices for the web sites they operate and that these practices be based on the following FIPPs:[60]

- Notice: Disclose how consumer information will be used.
- Choice: Offer consumers "choices as to how their personal identifying information" will be used.[61]
- Access: Offer consumers reasonable access to the information collected about them, including an opportunity to correct inaccuracies or delete information.
- Security: Take reasonable steps to protect the security of information collected from consumers.

Congress has not enacted legislation to implement the FIPPs. Instead, the FTC has gradually increased its involvement in privacy regulation under section 5 of the Federal Trade Commission Act, which gives the FTC the authority to take actions against firms who engage in unfair and deceptive practices. The FTC is "the broadest and most influential regulatory force on information privacy in the United States."[62] Besides enforcing statutes that affect privacy, such as COPPA and the Fair Credit Reporting Act, the FTC is responsible for regulating privacy that is not covered by specific statutes. Such regulation affects the collection and management of most kinds of data by merchants or online platforms.

Daniel Solove and Woodrow Hartzog argue that the FTC takes a common-law approach to regulating privacy.[63] Rather than defining which practices are permissible and which are not in advance, they respond on a case-by-case basis to alleged violations of privacy.

Early on, the FTC's approach to regulating privacy was limited largely to thin jurisprudence, holding firms to contract-like promises.[64] The FTC encour-

60. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May 2000.
61. Federal Trade Commission, *Privacy Online*, 36.
62. Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114, no. 3 (2014): 583.
63. Solove and Hartzog, "The FTC and the New Common Law of Privacy."
64. Solove and Hartzog.

aged self-regulation, and its enforcement focused on firms that violated privacy-related promises to consumers.[65] After many companies chose to write vague privacy policies, the FTC shifted toward enforcing consumer expectations.[66]

Gradually the commission came to play a growing role in policing unfair—rather than just deceptive—behavior.[67] For the FTC to consider an act or practice unfair, the act or practice must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[68] Emotional impact and other subjective kinds of harm are generally not sufficient to consider a practice unfair.[69]

On the basis of the cases it has heard, the FTC has acknowledged certain kinds of practices as being unfair, including the following:[70]

- Imposing retroactive policy changes that apply to data collected in the past without obtaining the consent of data subjects
- Providing the means and instrumentalities to invade others' privacy
- Transferring data to unseemly businesses
- Unfairly designing a product such that it can mislead or manipulate users into sharing information they would prefer not to share

Much of the FTC's impact on privacy policy has been through its privacy reports. Those reports guide the FTC's "policy-making initiatives, legislative support and enforcement acts."[71] The FTC "regularly borrows norms developed from the self-regulatory systems of industries" and incorporates protections from sectoral laws, such as healthcare privacy statutes, into its theories and settlements applied to other sectors of the economy.[72]

The FTC acts in response to unfair and deceptive practices that cannot easily be remedied by common law, contract law, or market forces.[73] The FTC has

65. Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge: Cambridge University Press, 2016), 146.
66. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 145.
67. Hoofnagle, 146.
68. 15 U.S.C. § 45(n) (2016).
69. "FTC Policy Statement on Unfairness," Federal Trade Commission, December 17, 1980, https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.
70. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 160–62.
71. James C. Cooper and Joshua D. Wright, "The Missing Role of Economics in FTC Privacy Policy," in *The Cambridge Handbook of Consumer Privacy*, ed. Evan Selinger, Jules Polonetsky, and Omer Tene (Cambridge: Cambridge University Press, 2017), 465–88.
72. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 146.
73. Hoofnagle, 344.

investigation, enforcement, and litigation authority.[74] The FTC initiates investigations in response to complaints of consumers or competitors, popular press news articles, and "observations of staff attorneys as they interact with companies."[75]

Respondents in FTC proceedings almost always negotiate consent agreements with the agency rather than contest the agency's allegations.[76] With a few exceptions, a commission order becomes final if it is not "stayed by the Commission or by a reviewing court."[77] After issuing a cease and desist order, the commission must seek the help of a court "to obtain civil penalties or consumer redress for violations of its orders."[78] Civil penalties may be applied only if the commission shows that the violator had "'actual knowledge that such act or practice is unfair or deceptive and is unlawful' under Section 5(a)(1) of the FTC Act."[79]

First-time offenses involving unfair or deceptive practices typically do not result in civil penalties.[80] Even without civil penalties, FTC actions can have an enormous public relations cost, given that FTC enforcement targets are frequently featured on the front page of the *Wall Street Journal*.[81]

Over time, general standards have gradually become more specific and rule-like. The FTC has incorporated qualitative judgments based on norms and best practices. It has also developed more substantive baseline standards for privacy based on industry norms and consumer expectations and has held companies liable for violating the privacy policies of partners and for furnishing partners with "the means to commit unfair or deceptive acts or practices."[82]

FTC privacy regulation may work better in a context where firms self-regulate, even when the self-regulatory regime is weak.[83] These regimes can function as standards, and the FTC can enforce those standards using the legal theory of deception. Self-regulation recognizes the ability of market participants to discover and codify norms and takes that responsibility away from the agency, reducing its workload.

---

74. Solove and Hartzog, "The FTC and the New Common Law of Privacy."
75. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 103.
76. Hoofnagle, 159.
77. "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," Federal Trade Commission, May 2021, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
78. "A Brief Overview."
79. "A Brief Overview."
80. Rohit Chopra and Samuel A. A. Levine, "The Case for Resurrecting the FTC Act's Penalty Offense Authority," *University of Pennsylvania Law Review* 170, no. 1 (2021): 71–123.
81. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 166.
82. Solove and Hartzog, "The FTC and the New Common Law of Privacy," 663.
83. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 181.

The Role of State Attorneys General

FTC privacy regulation interacts with state privacy laws and practices as carried out largely by state attorneys general. Attorneys general have the power to enforce state and some federal laws.[84] State attorneys general have often been stricter than the FTC in regulating privacy, even though most states have not enacted omnibus privacy laws. A good illustration of this is what firms are allowed to do with consumer data in bankruptcy cases.

One early case that involved an attempt of a firm to sell its customer data as part of a bankruptcy settlement involved Toysmart. Toysmart's privacy policy included a promise that it would never sell its customers' personal information to a third party. Nevertheless, when it encountered severe financial problems that led to bankruptcy, the company solicited bids for its customer databases.[85] The FTC filed a complaint in the US District Court for the District of Massachusetts to prevent Toysmart from selling its customer information.[86] The FTC subsequently reached a settlement that would have permitted Toysmart to sell its customer data as part of a package that includes the entire website, but only to a buyer doing business in a related market who agrees to abide by Toysmart's privacy policy.[87] But several state attorneys general objected to the settlement in bankruptcy court, arguing that the proposed sale of customer data was an unfair and deceptive business practice that violated state laws.[88] As a result, Toysmart did not sell its customer lists.

In some subsequent bankruptcy cases, state attorneys general have permitted the sale of customer data, with customers being able to opt out or, in one case, opt in to allowing the buyer to use their data.[89] In 2005, Congress passed the Bankruptcy Abuse Prevention and Consumer Protection Act (the BAPCPA), which included provisions to better protect consumer privacy interests.[90]

---

84. Bilyana Petkova, "The Safeguards of Privacy Federalism," *Lewis and Clark Law Review* 20, no. 2 (2016): 645.
85. Federal Trade Commission, "FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations," press release, July 21, 2000, https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding.
86. Federal Trade Commission, "FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors," press release, July 10, 2000, https://www.ftc.gov/news-events/press-releases/2000/07/ftc-sues-failed-website-toysmartcom-deceptively-offering-sale.
87. Federal Trade Commission, "FTC Announces Settlement with Bankrupt Website, Toysmart.com."
88. Laura N. Coordes, "Unmasking the Consumer Privacy Ombudsman," *Montana Law Review* 82, no. 1 (2021): 17.
89. Coordes, "Unmasking the Consumer Privacy Ombudsman."
90. The BAPCPA amended the bankruptcy code to make it harder for consumers to file for bankruptcy, but the act also spells out rules for the sale of consumer data in corporate bankruptcy fil-

The Role of Courts and the Common Law

Just as they played a limited role in regulating product safety and false advertising laws, courts have arguably not done enough to protect privacy. Proponents of FTC regulation argue that common-law tort theories have not effectively addressed dangerous products or false advertising. Likewise, some contend that privacy problems are "too subtle to fit into common law rights of action."[91]

One possible reason for the alleged failure of the common law in protecting privacy is the requirement of intent for a claim under a privacy tort to succeed. The FTC originally became involved in privacy enforcement partly in response to concerns about the failure of common-law fraud remedies because it is so difficult for a plaintiff to prove intent to deceive against a tortfeasor.[92] Unlike a judge using common law, Congress did not require the FTC to prove intent to deceive in cases involving fraud.[93] The FTC stepped in to correct this alleged failure of the courts to adequately address privacy problems, initially focusing on deceptive practices involving data collection, processing, and use. Ideally, deception could be addressed by bringing civil actions under the common law for making false statements.

Enforcement of privacy laws and policy by the FTC and other government agencies or by state attorneys general is constrained by limited resources of state and federal government agencies. To fill gaps in enforcement, legislators have often included statutory private rights of action. An important advantage of private rights of action is that lawyers have an incentive to represent plaintiffs' interests well while also assessing the likelihood that their case has merit. Unlike government lawyers and bureaucrats, private lawyers are rewarded for their performance, particularly if they are paid on a contingency fee basis.

Those who oppose a private right of action are concerned that there will be too many lawsuits that impose excessive costs on firms. But courts, with limited resources, have ways of rationing access. Federal courts often dismiss privacy claims owing to failure of plaintiffs to show cognizable harm, even when the statute does not require showing harm.[94] Courts do not recognize privacy and data security harms that "are too speculative and hypothetical" or "too based

---

ings. See Daniel Brian Tan, "Maximizing the Value of Privacy through Judicial Discretion," *Emory Bankruptcy Development Journal* 34, no. 2 (2018): 681–722.

91. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 344.

92. Hoofnagle, 119–120.

93. Hoofnagle, 120.

94. Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," *Boston University Law Review* 102, no. 3 (2022): 793–863.

on subjective fears and anxieties," requiring instead that plaintiffs demonstrate tangible injuries.[95] Courts have mandated proof of harm for statutes that do not require it and "even for statutes that include statutory damages."[96] They have excluded many kinds of harm such as emotional injury and unmet expectations.[97]

It should not be a surprise that courts have set a high bar to limit the number of privacy cases that plaintiffs win. Courts of necessity must answer the question of when and how privacy regulation should be enforced in a way that is consistent with achieving important social goals.[98]

Privacy cases are challenging for courts and government agencies to deal with because they often involve risk of future harms, and the harms are often small and caused by many actors.[99] Sometimes organizations cause a small harm to each of a large number of people. Class action lawsuits are a way to account for a large number of people experiencing small harms. One problem is that class action lawsuits may overdeter certain kind of violations, such as those subject to statutory damages that exceed actual damages.[100] Because a lawsuit can involve substantial discovery costs, which are disproportionately borne by commercial defendants, plaintiffs may have too much incentive to bring questionable cases.[101] But these problems with class action suits can be overcome with appropriate reforms.

Privacy Policy and Economic Analysis

Disclosing information online involves risks as well as benefits, so an important question is how policy should account for the risk involved. The precautionary principle, which emphasizes controlling or limiting the development of new ideas or technologies on the basis of possible harms they might cause, plays an important role in EU privacy policy but much less so in the United States. An alternative to the precautionary principle is permissionless innovation.[102] Much US regulation during the 1960s and 1970s was guided by the precautionary principle, but since 1980, permissionless innovation has played a decisive role in US

95. Danielle Keats Citron, "The Privacy Policymaking of State Attorneys General," *Notre Dame Law Review* 92, no. 2 (2016): 798–99.
96. Citron and Solove, "Privacy Harms," 800.
97. Citron and Solove, 800.
98. Citron and Solove, 794.
99. Citron and Solove, 812.
100. Brian T. Fitzpatrick, "The Conservative Class Action," in *The Conservative Case for Class Actions* (Chicago: University of Chicago Press, 2020), 114–130.
101. Fitzpatrick, "The Conservative Class Action."
102. Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2016).

policy toward information technology. A permissionless innovation approach views the risks of innovation as worth bearing if the possible benefits are large enough relative to the costs. During the past 30 years, consumer protection policy in the United States has relied much more on cost-benefit considerations than policy in Europe.[103] The FTC Bureau of Economics (BE) has played an important role in privacy policy decisions, contributing to the importance of cost-benefit considerations.

Precaution may be appropriate when the threat of harm is highly probable, tangible, immediate, irreversible, or catastrophic.[104] Technologies that raise questions about morally significant issues, such as what it means to be human, may also warrant precautionary regulation.[105] But most privacy problems arise in situations where harm is improbable, remote, and correctible and does not involve violation of fundamental moral principles.

Precautionary thinking is more likely to be a problem when it guides public policy and results in regulations "mandated and enforced by government officials."[106] By contrast, precautionary steps may be the appropriate response of families, businesses, and other organizations to some new technologies. Private entities will make decisions in light of their individual perceptions of benefits and costs.

Many internet users have decided that the benefits of having their data collected more than compensate them for the associated risks. Some consumers can now afford goods and services in exchange for data that they might not have been able to afford if they had to pay monetary prices instead. Access to the internet, which is now widely available and inexpensive, expands consumption opportunities for all consumers, but particularly those with limited incomes.

Sometimes regulators do not carefully compare the benefits with the costs of policies they implement. The advantages of cost-benefit analysis can be seen in some recent cases where the FTC appears to have overreached by penalizing behavior for which little tangible harm could be identified compared with possible benefits. In particular, critics point out that it is not the responsibility of government to penalize firms for behaving in a way that consumers may consider objectionable, such as engaging in practices that consumers consider

103. David Vogel, "The Law and Politics of Risk Assessment," in *The Politics of Precaution: Regulating Health, Safety, and Environmental Risks in Europe and the United States* (Princeton, NJ: Princeton University Press, 2012), 252–78.
104. Thierer, *Permissionless Innovation*, 34.
105. Thierer, 36–37.
106. Thierer, 36.

to be "creepy," if the practices play an important role in a mutually beneficial exchange.[107] An example of overreach is the FTCs complaint against DesignerWare. In alleging that DesignerWare violated section 5 of the Federal Trade Commission Act, the commission focused on the company's use of software to disable computers remotely, capture keystrokes and screenshots, take photographs with the computer's camera, and log any WiFi hotspots the computer detects.[108] Although use of the computer's camera is an actionable injury, it is hard to justify the agency's consent order, which entirely prohibited using monitoring software, given that the purpose of the software is to collect for or recover a computer from a renter who is behind in payments.

Although critics argue on the basis of cases like the one just described that economic analysis has not played a sufficient role in FTC privacy policy,[109] the FTC'S hesitancy to impose restrictions on data collection, processing, and use shows that the agency at least implicitly compares benefits to costs. The BE is concerned that giving too much weight to information privacy rights will discourage innovation and "starve the market of information."[110] Chris Jay Hoofnagle argues that BE economists have had a laissez-faire bias and that their research has not paid sufficient attention to behavioral economics or liberal and centrist works on consumer protection.[111]

As an FTC Commissioner, Maureen Ohlhausen urged the FTC in privacy cases to ask whether a company's collection or use of data, communication of information, or lack of disclosure actually harmed consumers.[112] Hoofnagle argues that the harms-based approach lacks rigor and "omits other kinds of injuries, such as affronts to dignity and violation of consumer expectations."[113] Although a credible case could be made for treating affronts to dignity as privacy violations, consumer expectations, which often reflect subjective preferences rather than well-defined principles, are questionable as the basis for a privacy standard. When perceived harm depends on consumer preferences, such harm is

107. J. Howard Beales III and Timothy J. Murris, "FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?," *George Washington Law Review* 83, no. 6 (2015): 2223.
108. Beales and Murris, "FTC Consumer Protection at 100."
109. Cooper and Wright, "The Missing Role of Economics in FTC Privacy Policy."
110. Chris Jay Hoofnagle, "The Federal Trade Commission's Inner Privacy Struggle" in *The Cambridge Handbook of Consumer Privacy*, ed. Evan Selinger, Jules Polonetsky, and Omer Tene (Cambridge: Cambridge University Press, 2018), 168.
111. Hoofnagle, "The Federal Trade Commission's Inner Privacy Struggle," 171, 173.
112. Lynn Stanton, "Ohlhausen 'Concerned' FCC Order Will 'Fragment' Privacy Oversight," *Cybersecurity Policy Report*, June 22, 2015, https://www.proquest.com/trade-journals/ohlhausen-concerned-fcc-order-will-fragment/docview/1692807245/se-2?accountid=14541.
113. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 344.

best avoided by consumers' choosing a service provider that better satisfies their preferences. Where satisfying consumer expectations is at issue, the FTC can and should act against firms that violate express promises or unilaterally change their privacy policy without obtaining consumer consent.[114]

The First Amendment limits the willingness and ability of courts in the United States to act against affronts to dignity, such as speech that seems intended to inflict emotional distress at a private family funeral.[115] This is particularly the case if the offending speech involves "a matter of public concern."[116] By contrast, EU privacy policy often prioritizes dignity, reputation, and personal honor over free expression.

REFORMING US PRIVACY POLICY

The Problem with Emphasis on Notice and Consent

As already discussed, notice and consent plays a major role in regulation of privacy in the United States and other countries. There are several reasons procedural regulation based on notice and consent plays such a major role in privacy policy: it is consistent with a free-market approach to privacy,[117] and it is easy to implement and enforce.

But the emphasis on privacy self-management is problematic in several ways. Notice and consent offers "all-or-nothing decisions" involving privacy policies that are too difficult for many people to understand.[118] Making informed decisions about privacy for each of the parties to whom users disclose information is very time consuming, especially in light of users' limited knowledge about what parties might do with that information or how it might be aggregated with other information that has already been collected about users.

One issue with notice and consent is whether the law should mandate that consumers must opt in to having their data collected or whether being able to opt out is sufficient. Those who think that consumers underestimate or under-

114. Beales and Murris, "FTC Consumer Protection at 100," 2218.
115. Snyder v. Phelps, 562 U.S. 443 (2011). The Court held that the members of Westboro Baptist Church, when picketing a funeral, were speaking on a matter of public concern on public land and were entitled to protection under the First Amendment.
116. Ronald J. Krotoszynski Jr., "The United States: The Polysemy of Privacy: An Analysis of the Many Faces and Facets to Privacy in the Contemporary United States," in *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (New York: Oxford University Press, 2016), 36.
117. Daniel Susser, "Notice after Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't," *Journal of Information Policy* 9 (2019): 148–73.
118. Susser, "Notice after Notice-and-Consent," 157.

value the risks associated with sharing their data might argue for opting in as the default. If one can be confident that consumers know and act in ways consistent with their own preferences, then transaction costs may be the decisive factor. An "'opt-out' default rule means that consumers who do not think decisionmaking costs are worthwhile do not need to bear those costs."[119] Some experiments have found that, among consumers who are more concerned about privacy, there is not much difference in decisions to share or not share data, regardless of whether the default is opt-in or opt-out; but those to whom privacy does not matter are much more likely to stick with the default.[120] When opt-in is the default, firms may incur high costs to try to persuade more consumers to opt-in, so an opt-out default may be preferable, except in the case of children, who may not be mature enough to make good decisions. Mandating opt-in "in situations where no clearly defined, significant harm is threatened may violate the First Amendment," as has been demonstrated in Supreme Court cases.[121]

Whether the default is opt-in or opt-out can make a large difference in how many choose to share their data, at least in experimental research, which shows sticky defaults. But in actual practice, this issue may not make a large difference, given that firms can find ways to influence whether consumers stick with the default. Experience has shown that defaults do not work well when firms have "a strong interest in whether the consumer sticks with or opts out of the default" and "the ability to shape the presentation of the default and the process for opting out."[122] This is illustrated by the failure of defaults to have much impact on consumers' decisions to allow financial institutions to share their data with third parties or to opt out of the default not to be charged fees for bank overdrafts.[123]

If more privacy protection is the goal, substantive regulation is likely to be more effective than policy that emphasizes consent. But in light of the benefits of information exchange, substantive rules should be limited to "hard bound-

119. Beales and Murris, "FTC Consumer Protection at 100," 2207n276.
120. Yee-Lin Lai and Kai-Lung Hui, "Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns," in *SIGMIS CPR '06: Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research: Forty Four Years of Computer Personnel Research: Achievements, Challenges & the Future*, ed. Kate Kaiser and Terry Ryan (New York: Association for Computing Machinery, 2006), 253–63.
121. Fred Cate and Michael Staten, "Protecting Privacy in the New Millennium: The Fallacy of Opt-In" (unpublished manuscript, 2001), https://www.semanticscholar.org/paper/Protecting-Privacy-in-the-New-Millennium%3A-THE-OF-Cate-Staten/2f775d82ef0abd3a740da55c91391f625c23147b.
122. Lauren E. Willis, "Why Not Privacy by Default?," *Berkeley Technology Law Journal* 29, no. 1 (2014): 109.
123. Willis, "Why Not Privacy by Default?," 96–107.

aries that block particularly troublesome practices" and combined with softer default rules that can be bargained around.[124] Default rules make more sense for privacy harms that are largely a matter of the personal preferences of a subset of the population.

With greater reliance on substantive rules than on consent to protect consumers from egregious violations of their privacy, notice would still play an important role by providing basic situational awareness.[125] This situational awareness could enable those who value privacy more highly than most people to take additional steps to protect their data, such as withholding certain information, engaging in obfuscation, or using privacy enhancing technologies.[126] In situations where third parties, such as data brokers, make decisions about processing and disseminating data, notice could help reduce consumers' ignorance and uncertainty about what data are contained in their profiles and how they are used.

Requiring firms to provide notice of what they do with user information plays at least two other important roles: it "can empower third parties that advocate on behalf of users,"[127] and it can encourage better corporate behavior, given that the process of learning how data are shared within an organization and with third parties can give firms a reason to revise their practices in light of social norms.[128]

Because notice and consent has played such an important role in privacy policy in the past, reform of US privacy policy that is politically feasible is likely to include a continuing role for notice and consent. The challenge is to overcome the tension between informing people about "how their data [are] used and shared" and enabling "regulators, policymakers and experts" to assess an organization's practices and whether it is keeping its promises that are part of its notices.[129] This could be better accomplished if online firms were required to provide two separate statements: a transparency notice that provides the details regulators need to know and an individual notice that is short and simple enough for nonexpert users to comprehend and digest.[130]

---

124. Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126, no. 7 (2013): 1903.
125. Susser, "Notice after Notice-and-Consent."
126. Susser, 165. For a discussion of the role of obfuscation, see Finn Brunton and Helen Nissenbaum, "Political and Ethical Perspectives on Data Obfuscation," in *Privacy, Due Process and the Computational Turn*, ed. Mireille Hildebrandt and Katja de Vries (New York: Routledge, 2013), 25.
127. Susser, "Notice after Notice-and-Consent," 166.
128. Susser, 166–67.
129. Daniel J. Solove and Paul M. Schwartz, "ALI Data Privacy: Overview and Black Letter Text," *UCLA Law Review* 68, no. 5 (2022): 1270.
130. Solove and Schwartz, "ALI Data Privacy," 1270.

One substantive rule that could be combined with notice and consent would be a rule requiring a data controller to provide heightened notice for "any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject."[131] The American Law Institute advocates such an approach to privacy regulation along with requiring clear and affirmative (opt-in) consent in situations where heightened notice is required.[132]

The Role and Limitations of Self-regulation

Early in the internet era, the FTC and others envisioned a major role for self-regulation to govern privacy policy in the United States. Some aspects of self-regulation have fallen far short of expectations, whereas others show promise for contributing to better policy in the future.

One aspect of self-regulation that looked potentially promising in the past was seal-of-approval programs, administered by a seal-granting authority, such as True Ultimate Standards Everywhere (TRUSTe) or BBBOnLine. Such programs enable firms to send a signal to consumers regarding whether the firm intends to protect "privacy post-contractually."[133] If the seal of approval provides a meaningful signal about whether a firm intends to protect privacy, then it may be more efficient than mandatory standards, particularly "for cases in which few consumers are sensitive to privacy and when their potential loss is small."[134]

Although a number of firms have received a seal of approval from TRUSTe, it has a questionable record in terms of promoting effective privacy policy. In a case that was settled in 2014, the FTC obtained a consent order prohibiting TRUSTe from misrepresenting "the steps it takes to evaluate, review or recertify a company's privacy practices" and "the frequency with which it evaluates, certifies, reviews, or recertifies a company's privacy practices."[135] The basic problem is that TRUSTe made little effort to detect when firms were violating its standards and required little or nothing of firms that were the subject of the numerous

131. Paul M. Schwartz and Daniel J. Solove, *Principles of the Law: Data Privacy* (Philadelphia, PA: American Law Institute, 2020), cited in Solove and Schwartz, "ALI Data Privacy," 1271n92.
132. Schwartz and Solove, *Principles of the Law*, cited in Solove and Schwartz, "ALI Data Privacy," 1273n106.
133. Zhulei Tan, Yu Jeffrey Hu, and Michael D. Smith, "Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems* 24, no. 4 (2008): 153–73.
134. Zhulei, Hu, and Smith, "Gaining Trust through Online Privacy Protection," 169.
135. Evan Brown, "TRUSTe Agrees to Alter Certification Practices, Pay $200,000," *Journal of Internet Law* 18, no. 7 (2015): 30–31.

complaints it received from users of certified web sites.[136] One study finds that sites certified by TRUSTe, were "more than twice as likely to be untrustworthy as uncertified sites."[137] TRUSTe is the best-known privacy certification authority. Benjamin Edelman's research finds that BBBOnLine, another authority, imposed stricter requirements so that sites it certified were more likely to be trustworthy than those it did not.[138]

Privacy self-regulation is also reflected in the growing employment of privacy professionals in large companies. To some extent, the growing employment of privacy professionals is in response to FTC privacy policy and state data breach notification laws, but the role these professionals play is about more than compliance. Social and technological changes have been "fueling privacy consciousness," which has been associated with growing media interest in privacy.[139] Between 1995 and 2010, there was a dramatic change from corporate managers devoting little time or attention to privacy to corporate structures that include direct leadership, often by C-level executives managing large staffs of privacy professionals.[140]

Many firms now employ chief privacy officers (CPOs). Corporate privacy leaders reflect a shift in views about privacy, defining privacy "as more than 'informational self-determination,'"[141] instead emphasizing a "substantive notion of privacy rooted in *consumer expectations*."[142] Firms are embedding privacy in "decisions about product design and market entry" as part of a "risk-assessment process."[143] They view privacy policy as more than compliance with laws and regulations. Instead, companies are embracing a "dynamic, forward-looking outlook towards privacy" that would enable them to maintain a trusted relationship with employees, clients, and other stakeholders.[144]

Continuing Role for the FTC

As discussed, the FTC has played an important role in regulating privacy in the United States and has accounted for benefits and costs in its decisions.

136. Benjamin Edelman, "Adverse Selection in Online 'Trust' Certifications and Search Results," *Electronic Commerce Research and Applications* 10, no. 1 (2011): 205–12.
137. Edelman, "Adverse Selection," 205.
138. Edelman, 205.
139. Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on Books and on the Ground," *Stanford Law Review* 63, no. 2 (2011): 276, 277.
140. Bamberger and Mulligan, "Privacy on Books," 260.
141. Bamberger and Mulligan, 251.
142. Bamberger and Mulligan, 251.
143. Bamberger and Mulligan, 252.
144. Bamberger and Mulligan, 271.

Its flexibility is a strength that could enable it to play an important role in the future. Its continued effectiveness may depend on whether the tradition of civil discourse to achieve policy consensus can be upheld in light of pressures toward greater partisanship.

Nevertheless, the FTC faces incentives that may interfere with its effective regulation of privacy.

It has an incentive to engage in enforcement actions to justify its role, regardless of whether each action is warranted. At the same time, its lawyers may not have a sufficient incentive to pursue the most egregious violations, and it does not have the power to impose the kind of penalties that might deter such violations.

Courts and the Common Law

As privacy problems grow, some legal theorists foresee a greater role for courts in adjudicating privacy cases. A persuasive case can be made for allowing privacy law to develop via common-law courts. In a common-law court system, there is a tendency for "the set of all legal rules to become dominated by rules" that achieve efficient "allocative effects."[145] To remain efficient, the common law "must change as conditions change."[146] It does so because parties are more likely to litigate rather than settle out of court when the legal rules relevant to a dispute are inefficient. Because inefficient rules give rise to more litigation, they will tend to be overturned and replaced by efficient rules, which will tend to persist.[147] This evolutionary pressure leading to efficiency does not come from the behavior of judges; it comes from the behavior of litigants.[148]

Although the FTC's approach to privacy and information security resembles common-law rulemaking, it differs in fundamental ways.[149] Unlike judges in court cases, the FTC is not an independent adjudicator; it is a party to the enforcement actions it brings. The FTC chooses to bring cases "that are most likely to advance its policy goals."[150] Thus, there is nothing about the process by which the FTC chooses the mix of cases to be adjudicated that favors the

145. George Priest, "The Common Law Process and the Selection of Efficient Rules," *Journal of Legal Studies* 6, no. 1 (1977): 65.
146. Paul Rubin, "Why Is the Common Law Efficient?," *Journal of Legal Studies* 6, no. 1 (1977): 51.
147. Priest, "The Common Law Process," 75.
148. Rubin, "Why Is the Common Law Efficient?," 61.
149. Justin Hurwitz, "Data Security and the FTC's Uncommon Law," *Iowa Law Review* 101, no. 3 (2016): 980.
150. Hurwitz, "Data Security," 984.

persistence of efficient rules and the overturning of those that are inefficient, as happens with common-law court cases.

There is widespread perception that courts have not done enough to uphold privacy. The process by which inefficient rules are replaced with efficient rules via court decisions can be slow. Judges' decisions do not always lead to more efficient rules, but over time, if judges are more likely than not to judge a particular case correctly, the continuing refinement and incremental development will lead to better laws.

The common law develops gradually in response to changes in the environment. Thus, it may take time for courts to recognize privacy rights in online interactions that are consistent with rights they have recognized offline. One example is the right to implied confidentiality. Courts have acknowledged a right to implied confidentiality in certain offline interactions, but in only a few cases have courts recognized a right to implied confidentiality in similar kinds of online interactions, and all those cases have involved commercial disputes.[151] Because it is an informal norm, courts may be able to uphold this right more effectively than may legislation.

In offline contexts, courts have developed general rules for enforcing confidentiality when there is no explicit contractual agreement. Courts have considerable discretion in determining whether an implied expectation of confidentiality is reasonable in any given circumstance.[152] Courts decide such cases based on context (customs, timing, purpose of disclosure, and relationship between parties), the nature of the information disclosed, who the sender is, who the receiver is, who the information subject is, and the terms of disclosure that may have been discussed or understood by the parties.[153] Similar criteria could be applied to evaluate whether someone has violated expectations of confidentiality in online interactions.

In privacy litigation, it has been common for courts to make a simple distinction between whether information is considered public or private, with no protection granted to data subjects against anyone collecting, disseminating, or using public information about them. According to Helen Nissenbaum, the "private/public dichotomy" does not provide a good foundation for a normative conception of privacy, because digital technologies have altered the terms under which "others have access to us and to information about us" in what were tra-

151. Woodrow Hartzog, "Reviving Implied Confidentiality," *Indiana Law Journal* 89, no. 2 (2014): 763–806.
152. Hartzog, "Reviving Implied Confidentiality," 774.
153. Hartzog, 777–802.

ditionally considered public and private domains.[154] In the past, ordinary people could generally expect not to be noticed or known in public arenas, other than perhaps settings where most people know each other. Before the internet age, even if several people noticed a person in public places at different times, it was unlikely for anyone to be able to combine disparate observations from unrelated observers into a profile that accurately describes the person. But now a variety of technologies such as radio frequency devices, video surveillance cameras, and facial recognition technology make it possible to track the location or compile a detailed profile of an individual for a relatively low cost.

In some situations, courts have eventually altered their understanding of privacy in response to changing technology. This alteration is illustrated in the Supreme Court's decision in *Katz v. United States* to overturn a prior decision (*Olmstead v. United States*) in which the court had ruled that wiretapping was not an unreasonable search and thus did not violate the Fourth Amendment.[155] In deciding that wiretapping did indeed violate the Fourth Amendment, the Court concluded that, given the role of telecommunications in modern life, the First Amendment purpose of protecting free speech and the Fourth Amendment purpose of protecting privacy required treating electronic eavesdropping on telephone conversations as a search, even though it did not involve physical trespass.[156]

Courts can play an important role in defining what constitutes cognizable harm in privacy cases. Privacy proponents are concerned that courts have too often taken an overly narrow approach toward harm, finding injury only for harms that look like harms that courts have recognized in the past. Recently, in at least some cases, courts seem to be taking a nexus approach, recognizing a new privacy interest where several traditional privacy concerns overlap.[157] One example of this is in *Heglund v. Atkin County*, involving an alleged violation of the Driver's Privacy Protection Act, in which the court granted standing because "a[n] individual's control of information concerning her person . . . was a cognizable interest at common law."[158] This approach allows the courts to identify injuries similar to those they have long been competent in adjudicating

154. Nissenbaum, *Privacy in Context*, 119.
155. Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967).
156. Laurence H. Tribe, "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier" (address, First Conference on Computers, Freedom, and Privacy, Burlingame, CA, March 26, 1991), 15, 20–21.
157. Matthew S. DeLuca, "The Hunt for Privacy Harms after Spokeo," *Fordham Law Review* 86, no. 5 (2018): 2469.
158. Heglund v. Aitkin County, 871 F. 3d, 572, 577 (8th Cir. 2017). The plaintiffs alleged that their information in Minnesota's driver's license database had been accessed by police officers hundreds of times over a 10-year period.

without "hampering Congress's power to respond to new forms of harm."[159] In doing this, the courts are seeking to preserve the balance between constitutionally protected rights and the flexibility to protect privacy in the face of changing technology through legislation.

Actual and Proposed Legislation

Many proposals for privacy legislation are modeled after the GDPR. Legislation that has been considered by the US government and enacted by a few state governments includes some provisions similar to provisions of the GDPR that may have harmful consequences. The GDPR requires that any data collection and processing must comply with the principles of "lawfulness, fairness and transparency," "purpose limitation," "data minimization," "accuracy," "storage limitation," "integrity and confidentiality," and "accountability."[160]

The GDPR considers data collection to be lawful if the data subject has given consent or there is some other valid reason for collecting the data to serve the interests of the data subject, the public interest, or legitimate interests pursued by the data controller or by a third party. The legitimate interests of the data controller are constrained by questions of whether the processing is "disproportionate, intrusive and unfair."[161]

The GDPR principle of lawfulness in most cases requires consent, which must be freely given, specific, informed, an unambiguous indication of wishes, auditable, easy to withdraw, and explicit.[162] The consent must be given by a "clear affirmative act."[163] This implies that the data subject has read and understood what data will be collected, how they will be processed, and whether they will be processed by a third party. The GDPR is clear that requesting a data subject to agree to terms and conditions via a check box is insufficient.[164] The GDPR standards of consent are high, and it is hard to imagine that they will be fully enforced. In response to those standards, many websites use consent management platforms (CMPs), but research shows that most CMP designs do not sat-

159. DeLuca, "The Hunt for Privacy Harms," 2470.
160. General Data Protection Regulation, art. 5 (2016), cited in Damien Geradin, Theano Karanikoti, and Dimitrios Katsis, "GDPR Myopia: How a Well-Intended Regulation Ended Up Favouring Large Online Platforms—the Case of Ad Tech," *European Competition Journal* 17, no. 1 (2021): 47–92.
161. Geradin, Karanikoti, and Katsis, "GDPR Myopia," 56n22.
162. Stephen Breen, Karim Quazzone, and Preeti Patel, "GDPR: Is Your Consent Valid?," *Business Information Review* 37, no. 1 (2020): 19–24.
163. Breen, Quazzone, and Patel, "GDPR: Is Your Consent Valid?"
164. Rothchild, "Against Notice and Choice," 596–97.

isfy the minimum requirements for specific and informed consent required by the GDPR.[165]

The GDPR approach to privacy goes beyond self-management. The European Union recognizes privacy in its Charter of Fundamental Rights of the European Union, which states that "everyone has the right to the protection of personal data."[166] The goal of EU data law is to "protect individuals from risks to personhood caused by the processing of personal data."[167] The law seeks to protect individuals who do not want their information disclosed, even if the information is not sensitive and its use would not cause adverse consequences for them.

The European Union also seeks to promote the free flow of information, recognizing the right to access information, freedom of expression, and journalistic freedoms. In cases where there are conflicts, EU courts must decide how to balance privacy rights and other interests. Regulators apply a least-means test whereby the benefits of information flows must be obtained at the least constitutional cost.[168] Thus, EU regulation places a higher weight on the privacy interests of the data subject than does US law, which gives more weight to the utilitarian benefits of information exchange. Under the GDPR, a "data controller must have a legal basis to collect data," whereas in the United States, data "collection is permitted unless it has been specifically prohibited."[169]

GDPR restrictions on the collection and processing of data could severely hinder some activities, such as behavioral advertising. The GDPR has safeguards to permit the collection and processing of information for the "legitimate interests pursued by the controller or by a third party."[170] This clause could be taken to allow publishers to collect data for behavioral advertising, but other provisions of the GDPR raise considerable uncertainty about when collecting such data could be viewed as "disproportionate, intrusive and unfair" and thus prohibited.[171]

---

165. Midas Nouwens et al., "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence," in *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 2020), 194–207.
166. 2012 O.J. (L C 326) 02, tit. 1, art. 8.
167. Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal* 106, no. 1 (2017): 127.
168. Schwartz and Peifer, "Transatlantic Data Privacy Law."
169. Lindsey Barrett, "Confiding in Con Men: US Privacy Law, the GDPR, and Information Fiduciaries," *Seattle University Law Review* 42, no. 3 (2019): 1083.
170. General Data Protection Regulation, art. 6, § 1 (2016), cited in Geradin, Karanikoti, and Katsis, "GDPR Myopia."
171. Geradin, Karanikoti, and Katsis, "GDPR Myopia," 56n22.

The purpose limitation, storage limitation, and data minimization requirements of the GDPR limit many beneficial uses of data. The benefits of being able to use data for purposes not foreseen at the time they are collected are in some cases enormous. Techniques of data analytics, such as machine learning and artificial intelligence, make it possible to derive all kinds of valuable new insights from old data. "Since analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, it becomes difficult to define ex ante the purposes of data processing."[172]

GDPR regulation raises the transaction costs of collecting and processing information. Data subjects must be given the right to withdraw consent for collecting and using their data at any time. Data subjects also have a right of data portability. Data controllers are required to conduct Data Protection Impact Assessments and have a data protection officer.

A major problem with the GDPR approach to privacy regulation is how it favors large, incumbent companies, such as Google and Facebook. It does so by imposing a variety of costs on companies that collect and process data. Many of these requirements include high fixed costs that result in economies of scale. The cost of complying may be millions of dollars, even for a small company, threatening its survival.

Besides economies of scale, large companies have other advantages over small ones in complying with the GDPR. Large platforms provide many services that users consider to be essential, so users are more likely to opt into data collection by those platforms. Established firms that have existing relationships with users are more likely to be able to persuade them to opt into data collection.[173] For large platforms with walled gardens to which users login, such as Android or Facebook, users need to consent only once to use the platforms repeatedly, whereas outside those walled gardens consent must be obtained for every website visit.

The GDPR makes it more difficult for firms to sell information to third parties than to use the information themselves.[174] This creates barriers to innovation,

---

172. Alessandro Mantelero and Giuseppe Vaciago, "Data Protection in a Big Data Society: Ideas for a Future Regulation," *Digital Investigation* 15 (2015): 104–9, cited in Mark MacCarthy, "In Defense of Big Data Analytics," in *The Cambridge Handbook of Consumer Privacy*, ed. Evan Selinger, Jules Polonetsky, and Omer Tene (Cambridge: Cambridge University Press, 2018), 57.

173. Willis describes all the ways that a firm can influence its users to permit the firm to collect their data by making effective use of incentives, regardless of the default. Willis, "Why Not Privacy by Default?"

174. The GDPR requires the data controller at the time the personal data are obtained to inform the data subject of any recipients or categories off recipients. GDPR art. 13, § 1I (2016), cited in Geradin, Karanikoti, and Katsis, "GDPR Myopia."

particularly from smaller startup firms that may be able find new ways to process data.[175] By limiting options of third parties who might compete with them, this provision also favors large, incumbent, vertically integrated firms.

Mandating certain modes of privacy protection, as does the GDPR, may interfere with private firms' attempts to offer other forms of privacy protection that may be superior, such as blockchain technology. Blockchain technology implies "partial or even total anonymity," and the GDPR may discourage the wider adoption of it because of requirements such as the right to erasure and amendment of data.[176] Government regulation "may also crowd out self-help products," such as ad blockers and VPNs.[177] Unlike government intervention, competition among self-help technologies favors firms that cost-effectively provide the privacy protection that users desire.[178]

States have recently enacted legislation to protect privacy. The California Consumer Privacy Act (CCPA) was enacted in 2018, Virginia and Colorado passed similar laws in 2021, and Utah and Connecticut enacted privacy laws in the first half of 2022. Each of these laws requires businesses of a certain size or larger to disclose the personal information they collect in response to consumer requests. Businesses must also accede to a consumer's requests not to sell that consumer's personal information and must delete the information on request.[179] The laws prohibit companies from discriminating against consumers by charging a different price or providing a different quality of goods or services to those who do not let the business use or sell their personal information.[180] They may offer promotions, discounts, and other financial incentives in exchange for personal information, but only if the incentive offered is reasonably related to the value of the information. The CCPA also applies to data brokers and requires data brokers to register with the state.[181]

---

175. Beales and Muris, "FTC Consumer Protection at 100."
176. Manne, Stout, and Auer, *Comments on Developing the Administration's Approach*, 23–24.
177. Manne, Stout, and Auer, 24.
178. Manne, Stout, and Auer, 24.
179. Taylor Kay Lively, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, March 31, 2022, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
180. The Utah law is the most lenient in that it allows data controllers to offer "a different price, rate, level, quality, or selection of a good or service to a consumer" if the consumer opted out of targeted advertising or if the offer relates to the consumer's voluntary participation in a bona fide loyalty program. Taylor Kay Lively, "Utah Becomes Fourth US State to Enact Comprehensive Consumer Privacy Legislation," *Privacy Advisor*, International Association of Privacy Professionals, March 25, 2022, https://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/.
181. "California Consumer Privacy Act," California Office of the Attorney General, accessed September 30, 2022, https://oag.ca.gov/privacy/ccpa.

Although the requirement of the CCPA and other state privacy laws that data controllers not discriminate against those who opt out of data collection seems reasonable on its face, depending on how it is enforced it could create significant risks for companies that do not provide the same free services to everyone who wants to use their site, regardless of whether those users allow the company to collect and use their information. It assumes that a government agency can come up with a fair and objective formula for determining whether the incentives companies provide to users are reasonably related to the value of the information users disclose.

The disclosure and opt-out requirements of the state privacy laws and the GDPR do not apply to deidentified information.[182] Thus, mutually beneficial exchanges of online services for data will continue to be permitted as long as the identities of data subjects are not attached to the data.

The Case for State or Federal Omnibus Privacy Legislation

The number of states with privacy legislation is growing. As of July 2022, five states have passed omnibus privacy legislation, and many other states are considering doing so. Relying on state legislation to protect privacy has advantages and disadvantages. As laboratories of democracy, states can experiment with different kinds of privacy legislation. Ideally, as the effects of different approaches become evident, states would seek to imitate the legislation of those states whose legislation contributes to the most desirable outcome.

The more that privacy policies vary from state to state, the more costly it will be for a firm doing business online to comply with each state's policy for collecting data from users. One estimate is that if all 50 states were to pass privacy legislation, the total cost to firms from legislation passed by states in which they are not headquartered would be between $98 billion and $112 billion per year.[183]

When laws differ between states, firms tend to adopt policies that conform to the most stringent state law.[184] If most firms adjust their practices to conform to the most stringent state law, then the most stringent state laws may become the de facto privacy policy for the nation as a whole.

---

182. The GDPR exempts "anonymous" data, which are roughly equivalent to data that are deidentified. See also "Privacy Law Comparison."
183. Daniel Castro, Luke Dascoli, and Gilliam Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Washington, DC: Information Technology and Innovation Foundation, 2022).
184. Petkova, "The Safeguards of Privacy Federalism," 645.

Concern that some states, such as California, have enacted laws that are too stringent and will have major nationwide effects has influenced efforts to pass national legislation that would preempt state laws. Because state laws are only beginning to take effect, it is not entirely clear how the policies of states that set the bar high will spill over to states with less stringent laws. Whether national legislation would be better than allowing each state to set its own policy depends partly on what kind of legislation is considered by the federal government.

Whether enacted by the state governments or federal government, privacy legislation should balance the benefits of information sharing with the costs of data being used in a way that is harmful or undesired by the data subject, and it should do so while minimizing transaction costs. The Uniform Law Commission (ULC) has created a model privacy law that attempts to balance benefits and costs by defining three categories of data practices: compatible data practices, incompatible data practices, and prohibited data practices.

A firm does not need the user's consent for a compatible data practice. By definition, such a practice is expected or clearly beneficial to the user.[185] The ULC considers the use of data for targeted advertising to be a compatible data practice.[186] But in the model privacy law, the data controller must disclose the compatible data practices it engages in routinely.

To engage in incompatible data practices, the firm must have the consent of the user. If the data are not sensitive, the data controller must provide notice of the practice, and the user must be given the opportunity to withhold consent.[187] To process sensitive data, a controller must obtain from the data subject "express consent in a signed record."[188]

A data practice would be prohibited by the model privacy law if it were likely to subject a user to specific and significant harm or risk of harm, whether financial, physical, reputational, or psychological.[189] Also prohibited would be incompatible data practices without the consent of the data subject.

In comparison with the ULC model privacy law, recently proposed privacy legislation, such as the American Data Privacy and Protection Act, places too much emphasis on notice and consent by, for example, requiring separate opt-in consent for each new product or service that is developed or calibrated using

185. Uniform Law Commission, *Uniform Personal Data Protection Act*, 2021, 9.
186. Uniform Law Commission, *Uniform Personal Data Protection Act*, 11.
187. Uniform Law Commission, 12
188. Uniform Law Commission, 12.
189. Uniform Law Commission, 12–13.

personal data.[190] In addition, several state laws and proposed federal laws raise obstacles to firms collecting data and using them for online behavioral advertising in exchange for providing online services.

Most proposed federal legislation contains many provisions similar to those in the GDPR and might do more to reduce competition and discourage innovation than it achieves in terms of enhanced privacy. By requiring opt-in consent in many situations, such proposed legislation would raise transaction costs and make it especially hard for small firms to enter the market and compete against firms that already have a large user base.

Fiduciary Responsibilities

Two bills proposed in 2021 would impose fiduciary responsibilities on digital platform firms "to do no harm" to those disclosing information to them.[191] As discussed earlier, this is a promising approach for enhancing privacy. Existing law imposes fiduciary obligations on physicians, some financial advisors, and lawyers. Professionals are legally obligated to act in the best interests of those with whom they have a fiduciary relationship. Neil Richards argues that "bookstores, search engines, ISPs, cloud storage services, providers of physical and streamed data, and websites and social networks when they deal in our intellectual data" should be treated as information fiduciaries.[192] Fiduciary relationships protect vulnerable consumers who often have very little information about the online service providers that have accumulated lots of information about them. As data subjects, those who use online services cannot do much to monitor the operations of firms who collect their personal data or prevent the firms from acting against their interests.[193]

The relationships between people and online platforms are very different than the standard arms-length relationships common to many traditional markets. The former are ongoing and of high frequency and occur "within an interactive environment" that is "completely constructed for the individual" and responsive to the individual.[194] This makes users of platforms especially vulnerable.

---

190. Alden Abbott and Satya Marar, "Unintended Consequences: The High Cost of Data Privacy Laws," *National Interest*, July 19, 2022.
191. These two bills, introduced in 2021, use the term "duty of loyalty," which is equivalent to fiduciary responsibility. Müge Fazlioglu, "Distilling the Essence of the American Data Protection Act Discussion Draft," *Privacy Tracker*, International Association of Privacy Professionals, June 6, 2022.
192. Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (New York: Oxford University Press, 2015), 168.
193. Balkin, "Information Fiduciaries and the First Amendment," 1222.
194. Woodrow Hartzog and Neil Richards, "The Surprising Virtues of Data Loyalty," *Emory Law Journal* 71, no. 5 (2022): 996.

Digital service providers try to convince users that they are trustworthy. But something more, like being legally designated as information fiduciaries, may be needed to hold them accountable. Because it is very difficult to know what happens to the data that these firms collect about users, market competition may not be enough to motivate them to take the steps necessary to secure the data they collect and protect users' privacy interests.

If firms were to be treated as information fiduciaries, they would have the freedom to "monetize some uses of personal data" but not to use the data in unexpected ways that harm consumers or violate an important social norm.[195] Ariel Dobkin suggests that information fiduciaries should abide by the following four principles:[196]

- Anti-manipulation of the user
- Nondiscrimination
- Limited third-party sharing
- Adherence to the company's own privacy policy

The federal government could pass legislation requiring certain kinds of online service providers to uphold each of these principles, where a violation would be defined as disregarding users' reasonable expectations or violating users' trust.[197] The statute would need to define the covered entities and the general duty, but it would not need to specify detailed rules. Courts could do so "as cases arise by determining what a 'reasonable user' should expect."[198] Insetad of being spelled out in detail by legislation, rules could be left to develop via common-law courts cases as courts apply the four principles to resolve specific disputes in the current environment.

If an online service provider is considered an information fiduciary, then its speech can be restricted in ways consistent with fulfilling its fiduciary responsibilities. A firm acts as an information fiduciary if it presents itself to the public as respecting privacy, if it takes active steps to induce trust, and if its assurances of trust are consistent with social norms.[199] This implies a narrow definition of

195. Balkin, "Information Fiduciaries and the First Amendment," 1227.
196. Ariel Dobkin, "Information Fiduciaries in Practice: Data Privacy and User Expectations," *Berkeley Technology Law Jorunal* 33, no. 1 (2018): 1–52.
197. Dobkin, "Information Fiduciaries in Practice."
198. Dobkin, "Information Fiduciaries in Practice," 49.
199. Balkin, "Information Fiduciaries and the First Amendment," 1222–24.

information fiduciaries that could apply to cloud service providers, email providers, and internet service providers, but not to online retailers.[200]

Jane Bambauer argues that fiduciary relationships should be exceptional and should not apply to garden-variety internet firms because "the law may better serve consumers by encouraging skepticism rather than trust" in such firms.[201] Some skeptics question the feasibility of applying the concept of information fiduciary to firms such as Facebook, Google, and Uber.[202] These firms have a fiduciary obligation to earn profit for their stockholders, and they do so not by serving the interests of the users from whom they collect data but of their clients who pay for their services, such as online advertisers.

Even without fiduciary obligations, the common law regarding negligence can be used to hold firms liable to failing to "exercise reasonable care not to subject others to an unreasonable risk of harm."[203] This principle was applied by the court in *Remsburg vs. Docusearch*, a case concerning an information broker that sold a social security number and workplace address to an individual who used the information to locate and murder a woman.

Private Right of Action

If the federal government or state governments enact privacy legislation that is not too strict, a persuasive case can be made that it should include a private right of action. As noted earlier, this approach will enhance enforcement, given the limited resources of the FTC and state attorneys general. Private rights of action, however, have been an obstacle to getting legislation passed at the federal level, given that many firms have opposed them owing to concern about the high costs that firms may need to bear if privacy cases proliferate.[204] To avoid the risks of overenforcement, governments need to have rules constraining how courts treat privacy cases.

Because online privacy disputes often involve a large number of people who suffer the same kind of harm, a good way to resolve them may be class action law-

200. Jane Bambauer, "The Relationship between Speech and Conduct," *UC Davis Law Review* 49, no. 5 (2016): 1953.
201. Bambauer, "The Relationship between Speech and Conduct," 1952.
202. Lina M. Khan and David E. Pozen, "A Skeptical View of Information Fiduciaries," *Harvard Law Review* 133, no. 2 (2019): 497–541.
203. Remsburg v. Docusearch, No. 2002-255 (N.H. Feb. 18, 2003).
204. Cameron F. Kerry and John B. Morris, "In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition," *TechTank* (blog), Brookings Institution, July 7, 2020.

suits. Class actions work well when many people experience small losses. They are also affordable for class members because there is usually no upfront cost.

In practice, however, the situations where harms to privacy can be resolved by class action lawsuits may not be very common. Class actions are suitable for data security breaches, but it is much more difficult to identify concrete harms to an identifiable class from most kinds of privacy violations. In Canada, class actions have been brought frequently for cases involving health information and data security but less frequently for other types of claims, such as those involving "the collection of personal information without consent, unauthorized sale of personal information to data aggregators, or defamatory or other reputational harms related to the use of personal information."[205] Canadian courts have often been unwilling to certify these kinds of class actions, and US courts have demonstrated a similar unwillingness to consider such cases.

If privacy legislation is enacted that includes a private right of action, one way to make such a provision more politically palatable is to require a standard of "knowing or reckless disregard for the privacy or security of individuals" to find a defendant to have violated a statute.[206] As noted earlier, to avoid overenforcement of privacy via class actions, courts should award only actual damages in such cases. Brian Fitzpatrick suggests other reforms to class actions such as requiring plaintiffs to bear some of the costs of discovery so that defendants do not have too much incentive to settle cases, especially those that are of questionable merit.[207]

COMPARING THE LEGISLATIVE, COMMON-LAW, AND FTC APPROACHES TO REGULATING PRIVACY

FTC regulation is most effective if it is used in combination with self-regulation to promote best practices by firms that collect, process, or use online data. As an agency, the FTC is nimble enough to react to changes in technology and to discover and uphold contextual norms for privacy. The FTC has a comparative advantage in taking an economic approach and considering the costs and benefits of certain privacy practices. To the extent that the FTC focuses on unfair practices, FTC cases include a heavy dose of cost-benefit analysis.[208] Even if it

205. John J. A. Lenz, "Privacy Class Actions' Unfulfilled Promise," in *Class Actions in Privacy Law*, ed. Igancio N. Cofone (New York: Routledge, 2021), 57.
206. Kerry and Morris, "In Privacy Legislation."
207. Fitzpatrick, "The Conservative Class Action," 117–21.
208. Hoofnagle, "The Federal Trade Commission's Inner Privacy Struggle."

has not done enough to compare benefits to costs, the FTC arguably has made some efforts to limit its regulation in order to allow continued mutually beneficial information exchanges.

Legislation is costly to enact, and legislators are slow to agree about the best way to respond to new problems. Legislation often results in costly unintended consequences, particularly if it places too many restrictions on what firms can do in order to support a right to privacy. The political process may result in legislation that favors the interests of large, incumbent firms, who favor rules that increase rivals' costs. Nevertheless, legislation may respond effectively to new problems by clearly spelling out rights and responsibilities of the different parties to a transaction if those rights and responsibilities are consistent with widely accepted ethical norms.

Legislation may be an effective way to impose fiduciary responsibilities on digital platforms that store and process large amounts of consumer data. But mandating fiduciary responsibilities, especially loyalty toward end users, may be inconsistent with the business models of some online platforms that collect "personal data in order to serve targeted ads."[209] This "creates a perpetual conflict of interest" between the companies and their end users.[210]

Even without imposing fiduciary duties on data collectors, "courts can employ fiduciary concepts to define the common law duties" of data collectors.[211] The Pennsylvania Supreme court established in *Dittman v. UPMC* that an employer has a common law duty to "exercise reasonable care to protect" employees from harm resulting from a breach of the data it collected from them.[212] Since fiduciary law recognizes a "mandatory core" that cannot be overridden by agreement, it can protect data subjects from exploitative clauses that might otherwise be included in contracts of adhesion.[213]

The idea of imposing fiduciary duties, particularly loyalty, "could supply a political lodestar for privacy reform more generally."[214] Emphasis on duties of loyalty could counterbalance First Amendment objections to restricting certain kinds of data collection, processing, or use.

---

209. Whitt, "Old School Goes Online," 96.
210. Jack M. Balkin, "Fixing Social Media's Grand Bargain" (Aegis Series Paper No. 1814, Hoover Institution, Stanford, CA, October 15, 2018), 12.
211. Daniel M. Filler, David M. Haendler, and Jordan L. Fischer, "Negligence at the Breach: Information Fiduciaries and the Duty of Care for Data," *Connecticut Law Review* 54, no. 1 (2022): 135.
212. Dittman v. UPMC, 196 A.3d 1047 (Pa. 2018), cited in Filler, Haendler, and Fischer, "Negligence at the Breach."
213. Filler, Haendler, and Fischer, "Negligence at the Breach," 143.
214. Hartzog and Richards, "The Surprising Virtues of Data Loyalty," 1007.

The US government has been unsuccessful in enacting comprehensive privacy legislation. Such legislation is hampered by low levels of trust in the federal government.[215] Americans also distrust corporations and are concerned that federal legislative proposals will be heavily influenced by corporate lobbying. But well-designed federal legislation would have advantages over 50 different state omnibus privacy laws. Even if federal legislation would not do much to preempt existing state laws, it could reduce costs if it were passed before most states have enacted their own omnibus laws.

Courts are often slow in responding to changing conditions and, as a result, leave some privacy problems uncorrected. Nevertheless, there are advantages of relying on common-law remedies that arise from court decisions. One is that courts can respond better to disputes involving informal norms than legislatures or regulatory agencies. Another is that court decisions tend to be part of an evolutionary process that results in the set of all rules being dominated by those rules that lead to efficient outcomes. Courts also have a comparative advantage in cases involving liability or negligence, which can play an important role in compensating people for privacy-related harms and harms from data breaches. Courts can also play an important role in limiting the applicability of statutes so they do not violate constitutionally protected rights, such as freedom of speech.

CONCLUSION

Privacy policy in the United States can be improved in several ways. Existing policy puts too much emphasis on privacy self-management. The transaction costs of the existing regime of notice and consent are too high. Although consent plays an important role in enabling consumers to exercise their preferences to limit the personal information they share in particular contexts, it cannot protect consumers from what firms might do with data the firms have already collected. Consent also adds unnecessary costs in transactions where firms use data in a way that data subjects expect or benefit from. Liability—possibly combined with fiduciary responsibilities—is a better way to preserve the freedom of firms to use data for innovative purposes while being accountable to data subjects who agree to disclose personal data to them. Regulation to hold firms liable for harmful uses of data can and should be supplemented with policies that encourage the development of

215. Jeeyun (Sophia) Baik, "Data Privacy and Political Distrust: Corporate 'Pro Liars,' 'Gridlocked Congress,' and the Twitter Issue Public around the US Privacy Legislation," *Information, Communication & Society* 25, no. 9 (2020): 1211–28.

technological solutions that can help consumers make and enforce decisions about ways to limit the data that are collected about them and how the data are used.

Heavy handed regulation like the GDPR is likely to interfere with the continued growth and application of data analytics, which has been enormously beneficial for consumers and businesses in many sectors of the US economy and offers the potential for continued growth in productivity and innovation. Nevertheless, the United States could benefit from coherent national privacy legislation, if that legislation does not significantly hinder the exchange of data for online services. The FTC plays an important role and should continue to do so, but targeted federal legislation could reduce uncertainty and compliance costs and prevent states from creating a costly "thicket of conflicting laws."[216]

Information processing is an important part of today's economy, and as opportunities to collect and process data grow in the future, welfare can be further enhanced by allowing firms to continue collecting and processing data with appropriate safeguards. Rules that place rigid limits on how existing data can be used and shared with third parties or how long they can be stored may do more harm than good. The challenge is to reduce the risks associated with data collection, processing, and dissemination. A promising approach toward reducing risks to data subjects would be to impose the obligations of information fiduciaries on selected online firms that make extensive use of personal data, but as discussed earlier, important obstacles may make that difficult to achieve. Alternatively, a robust regime that combines FTC regulation and common-law court cases to hold firms liable for privacy harms caused by their data collection, storage, dissemination, and processing may provide adequate privacy protection while interfering little with the continued growth and development of the information economy.

216. Alan McQuinn and Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law* (Washington, DC: information Technology and Innovation Foundation, 2019).

ABOUT THE AUTHOR

Tracy Miller is a senior policy research editor at the Mercatus Center at George Mason University. Previously, he was associate professor of economics and fellow for the center for Vision and Values at Grove City College. His research interests include antitrust policy, environmental policy, health economics, and transportation policy. He has published articles on agricultural policy, antitrust policy, environmental policy, international trade, and transportation policy. He received his PhD in economics from the University of Chicago. He also holds an MS in agricultural economics from Michigan State University and BS in forestry from Virginia Polytechnic Institute and State University.

ABOUT THE MERCATUS CENTER AT GEORGE MASON UNIVERSITY

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

As a university-based research center, the Mercatus Center trains students, conducts research of consequence, and persuasively communicates economic ideas to solve society's most pressing problems and advance knowledge about how markets work to improve people's lives.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Since 1980, the Mercatus Center has been a part of George Mason University, located on the Arlington and Fairfax campuses.