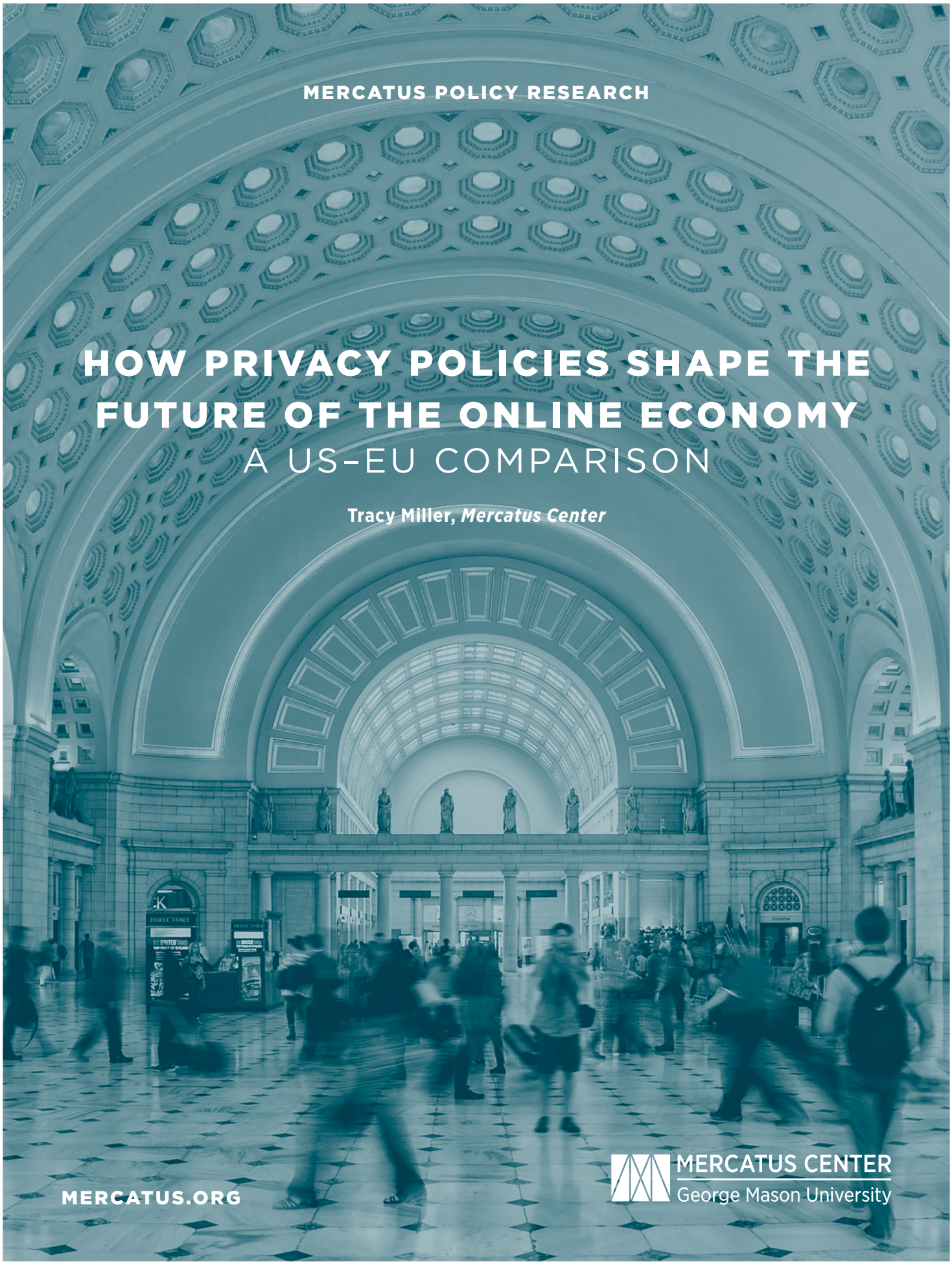

MERCATUS POLICY RESEARCH

HOW PRIVACY POLICIES SHAPE THE FUTURE OF THE ONLINE ECONOMY

A US–EU COMPARISON

Tracy Miller, ***Mercatus Center***

MERCATUS.ORG

MERCATUS CENTER
George Mason University

Tracy Miller. "How Privacy Policies Shape the Future of the Online Economy: A US–EU Comparison." Mercatus Working Paper, Mercatus Center at George Mason University, April 2025.

Abstract

This paper examines the impact of privacy policies on the future of the online economy, with a comparative analysis of the United States and the European Union. As online services increasingly rely on personal data to drive advertising revenues, privacy regulations have evolved to address concerns over data security and consumer rights. This paper explores the tradeoffs involved in privacy regulation, including its effects on market concentration, innovation, and transaction costs. While stricter privacy laws, like the European Union's General Data Protection Regulation (GDPR), have provided individuals with greater control over their data, they have also imposed significant compliance costs, disproportionately affecting smaller firms and threatening advertising-based business models. The United States, lacking comprehensive federal privacy legislation, has adopted a more sectoral and enforcement-based approach, with the Federal Trade Commission (FTC) playing a key role. State-level regulations, particularly in California, are beginning to mirror aspects of the GDPR, raising questions about the future direction of US privacy policy. So far, privacy regulation in the European Union and the United States has not fundamentally altered the business model governing the online economy, but as regulation continues to evolve, it may have more of an impact on business models, consumer choices, and competitive dynamics, with ongoing tensions between consumer protection and economic innovation.

JEL codes: H77, K15, K23, K24, K41, M3, O38

Keywords: privacy policy, online economy, personal data, behavioral advertising, real-time bidding, competition, class action, Federal Trade Commission, regulation, litigation, standing, private right of action, notice and consent, transactions costs, innovation, European Union, GDPR

Personal data play a critical role in the online economy, providing information that enables firms to better target their advertising, which is the most important source of revenue for many online service providers. As the online economy has grown, so have concerns about privacy and data security. Over the years, governments have enacted privacy laws and increased restrictions on the collection, storage, use, and sharing of personal data online.

Regulating data collection, processing, and storage to protect privacy and data security involves important tradeoffs. Such regulation involves a mix of requirements for data controllers and enforced rights of data subjects, including rules about consent that firms must obtain to collect, store, share, and process data. Government policy determining how and how much to regulate firms' interactions with users concerning their personal information affects the ease with which agents may exchange data for online goods and services and the distribution of benefits and costs from that exchange.

The business model that drives much of the online economy involves firms providing goods and services to users in exchange for their personal data so the firms can earn revenue from targeting advertising to users. Privacy regulation, by limiting the amount and kinds of data that firms may collect and imposing costly requirements on them in their activities as data controllers, reduces the net revenue that those firms can earn in exchange for the services they provide. Thus, privacy regulations limit the opportunity to fund consumer services through advertising revenue.

In light of recent policy trends and political pressure for more privacy regulation, what will the future of privacy regulation look like, and what will be the consequences for the online economy? The United States can learn from what has already happened in the European Union, because privacy regulation there is stricter than in the United States.

In this paper, I argue that the future regulation of data collection and its effects on the online economy are still unclear, though certain observable trends

in policy and outcomes may continue for the foreseeable future. Firms are under pressure to be more transparent about their data collection and processing practices and to give data subjects more choices concerning whether and how their data will be collected and used. Where firm data collection is limited more by centralized regulation, innovation is reduced, transaction costs are rising, and market concentration seems to be increasing. Although the trend is toward more restriction of data collection, which makes it more difficult to target advertising to individuals, many firms, especially those with large platforms, have found ways to adjust to the regulations and continue to prosper. Existing privacy regulations have given data subjects more control over whether their data are collected and processed by specific online service providers. However, so far these regulations have done little to limit how these data are used or to help consenting consumers understand the associated privacy risks. Where data protection policy is stricter, it has tended to disproportionately harm small firms while giving a competitive advantage to large platforms without significantly restricting their ability to collect and monetize data.

US Privacy Policy: The Role of Legislation, the FTC, and the Courts

The US government regulates privacy in different ways for different sectors of the economy. The United States has long had federal privacy laws that apply to educational, financial, and health data and to data about children 13 and younger, but no federal statutes have been enacted to regulate privacy in other sectors. As the internet has grown and more information is exchanged online, the FTC has assumed an important role in regulating privacy and data security. A growing number of states, led by California, have enacted comprehensive privacy laws governing how firms must handle personal data they collect, store, use, and share with others. The courts have also been involved, adjudicating cases involving privacy and data security.

FTC privacy and data security policy

Several different federal agencies have been involved in privacy regulation. The FTC plays a leading role in privacy enforcement. It enforces the Gramm-Leach-Bliley Act, which covers financial data, the Fair Credit Reporting Act (FCRA), and the Children's Online Privacy Protection Act. But other agencies are also involved. The Department of Health and Human Services enforces the Health

Insurance Privacy and Accountability Act (HIPAA), and the Department of Education enforces the Family Educational Records Privacy Act (FERPA).

Besides enforcing selected federal privacy statutes, the FTC also enforces commercial privacy and data security in situations where no legislation applies. Rather than enacting ex ante rules specifying what firms must do, the FTC takes a case-by-case approach. The agency has brought hundreds of cases involving the privacy and security of consumer data.[1]

FTC enforcement of privacy is based on its authority under section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices."[2] The FTC statute finds a practice unfair if it "causes or is 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."[3]

Until recently, the FTC's approach to general privacy problems was largely to direct enforcement actions at deceptive acts and practices. The FTC and state attorneys general filed legal claims against companies that violated their stated privacy policies.[4] In complaints prior to 2014, the FTC required each company that allegedly violated its own privacy policies and statements about privacy settings to develop a comprehensive privacy program.[5] They also required companies to obtain explicit user consent to apply new privacy policies to previously collected data. More recently, the FTC has expanded its privacy and data security enforcement to place greater emphasis on unfairness. Between 2014 and 2018, many FTC complaints involved companies failing to notify consumers about the information they were collecting or failing to obtain consent before collecting it.[6]

Enforcement action typically results in negotiated agreements between the FTC and the targeted company. These consent decrees commonly involve adoption of a 20-year privacy compliance program that the FTC monitors.[7] The FTC usually does not impose fines for a first offense, but once a company is under a consent decree, the FTC can impose substantial fines for failure to adhere to

1. Daniel J. Gilman and Liad Wagman, "The Law and Economics of Privacy," *UCLA Journal of Law and Technology* 29, no. 2 (Spring 2024): 58.
2. 15 U.S.C. § 45.
3. 15 U.S.C. § 45 (n).
4. Federal Trade Commission, *Privacy and Data Security Update: 2019, December 2019, 2*.
5. Patricia Bailin, "Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices" (Westin Research Center Study, International Association of Privacy Professionals, Portsmouth, NH, 2014), 2.
6. Müge Fazlioglu, "What FTC Enforcement Actions Teach Us About the Makings of Reasonable Privacy and Data Security Practices: A Follow-up Study" (International Association of Privacy Professionals, Portsmouth, NH, June 11, 2018), 2.
7. William McGeveran, "Friending the Privacy Regulators," *Arizona Law Review* 58 (2016): 989.

its conditions, and the fines can be proportional to the number of users of the company's services.[8]

Scholars and advocates criticize US privacy policy for not protecting privacy adequately due to an "existing patchwork of privacy statutes" that are weak, incomplete, and fractured.[9] But despite Congress's failure to pass national privacy legislation, since the 1990s corporate America has expanded its efforts to protect consumer privacy. Large firms devote considerable resources to privacy protection, with thousands employing a chief privacy officer (CPO).[10]

The FTC has played a significant role in the evolution of US privacy policy by providing a forum for the expansion of privacy discourse.[11] The commission's creative use of its enforcement powers, combined with market forces that rewarded improved privacy protection, has moved the privacy discourse away from an emphasis on procedures to facilitate users' informational self-determination.[12] In response, firms have adopted dynamic, forward-looking practices based on an understanding of privacy defined by consumer expectations.[13] Kenneth Bamberger and Deirdre Mulligan, in their research on corporate privacy policies, interviewed CPOs. One of them stated that the objective of their company's privacy policy was to do the right thing to maintain a trusted relationship with employees, clients, and other constituencies.[14]

The government could take an adversarial approach to enforcing regulation, or it could take a more responsive approach. Although the FTC Act presupposes that the agency will do most of its work through adversarial enforcement, many of its actions can be described as responsive.[15] Responsive regulation differs from other strategies of market governance both in what triggers regulators to respond and in what the response will be.[16] Responsive regulation opens the door for a wide variety of regulatory approaches, with the best strategy depending on history, context, and regulatory culture.[17]

---

8 Adjustment of Civil Monetary Penalty Amounts, 16 C.F.R. 1.98 (2025); McGeveran, "Friending the Privacy Regulators," 999.

9. Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Books and on the Ground," *Stanford Law Review* 63, no. 2 (2011): 249.

10. Bamberger and Mulligan, "Privacy on the Books," 251.

11. Bamberger and Mulligan, 279.

12. Bamberger and Mulligan, 279.

13. Bamberger and Mulligan, 269

14. Bamberger and Mulligan, 271.

15. McGeveran, "Friending the Regulators," 997–998.

16. Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University Press, 1992), 4.

17. Ayres and Braithwaite, *Responsive Regulation*, 5.

Firms are more likely to comply when an agency uses a responsive regulatory approach if the agency operates according to an enforcement pyramid.[18] At the base of the pyramid, where most regulatory action occurs, the agency uses dialogue and persuasion to motivate firms to pursue industry best practices to protect the privacy and security of user data. When dialogue and persuasion fall short, the next level of enforcement involves formal methods such as a warning letter, a rebuke, or an announcement of an investigation.[19] At the top of the enforcement pyramid, the agency imposes civil penalties or, in the most severe cases, some kind of criminal penalty. A company's business license may also be suspended or revoked.[20]

McGeveran emphasizes the role of graduated penalties in FTC policy.[21] Although firms often incur no penalty for violating privacy on a first offense, on subsequent offenses, firms "end up paying many times what it would have cost to comply in the first place."[22]

Responsive regulation works most effectively when regulated parties are otherwise motivated to comply with the law, which is often the case with privacy and data security policy.[23] It helps if there is broad public support for the regulator's approach to the law.[24] Companies and their investors know that pursuing privacy and data security enhances brand value, customer trust, and profitability.[25] Corporate privacy officials understand privacy and data protection obligations in terms of risk management and meeting consumer expectations.[26]

The FTC has employed responsive regulatory tools such as publicity, research, best-practice guidance, and deliberative, participatory processes that solicited input from privacy advocates and businesses. Its activities boosted self-regulatory efforts, increased the transparency of corporate privacy practices, and empowered privacy advocates.[27]

---

18. Ayres and Braithwaite, 19–36.
19. Ayres and Braithwaite, 35–36.
20. Ayres and Braithwaite, 36.
21. McGeveran, "Friending the Regulators," 1000.
22. Federal Trade Commission, "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," news release, August 9, 2012, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
23. McGeveran, "Friending the Regulators," 985.
24. Christine Parker, "The 'Compliance' Trap: The Moral Message in Responsive Regulatory Enforcement," *Law and Society Review* 40, no. 3 (2006): 611.
25. McGeveran, "Friending the Regulators," 986.
26. Bamberger and Mulligan, "Privacy on the Books," 270–272.
27. Bamberger and Mulligan, 287–288.

Corporate privacy leaders have framed privacy as a way to promote trust and burnish corporate reputations.[28] In spite of an emphasis on privacy by corporate leadership, however, Ari Waldman suggests that many people's experiences with websites and privacy notices are inconsistent with a trust-based, forward-looking vision of privacy.[29] This is because many engineers do not design technology products and services with privacy in mind. Unlike CPOs, the engineers who design products and the lawyers who draft privacy notices have a narrower understanding of privacy that is limited to notice or synonymous with data security.[30]

To convince engineers to take privacy obligations seriously often requires "strong, disruptive regulatory interventions."[31] If the risk of enforcement is low, engineers might not have enough incentive to implement more privacy-friendly product design.[32] Structural limitations built into corporate organizations may prevent the robust privacy norms held by CPOs from influencing product designers.[33]

In the United States, the FTC's approach has emphasized balancing privacy rights with the benefits associated with the free flow of information. "Legislators and regulators were relatively quick to join a conversation about addressing privacy risks to advance electronic commerce."[34]

The FTC has proposed privacy rulemaking that could lead to stricter regulation. In its August 2022 Advanced Notice of Proposed Rulemaking (ANPR), the FTC announced that it was considering imposing privacy regulations that "contravene revealed consumer preferences."[35] In contrast to the restraint the commission has exercised in its past regulatory actions, the ANPR contemplates sweeping regulations with major economic and political implications that likely exceed the FTC's authority.[36]

Several times, the FTC has overreached by imposing regulations that go beyond its congressional mandate, but Congress and the courts have acted to rein it in. On one occasion, Congress threatened to defund the agency. In addition, the US Supreme Court has recently demonstrated a greater willingness

28. Bamberger and Mulligan, 280.
29. Ari Ezra Waldman, "Designing Without Privacy," *Houston Law Review* 55, no. 3 (2018): 659–727.
30. Waldman, "Designing Without Privacy," 703.
31. Waldman, 706.
32. Waldman, 705.
33. Waldman, 712.
34. Bamberger and Mulligan, "Privacy on the Books," 282.
35. Geoffrey A. Manne, Daniel J. Gilman, and Kristian Stout, "FTC Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security," *ICLE Comments,* FTC Docket No. 2002-0053 (November 2022): Executive Summary, 3**.**
36. Manne et al., "FTC Advance Notice," Executive Summary, 7–8.

to enforce constitutional limits on an agency's authority, as illustrated by its jurisprudence concerning the "major questions doctrine" and its 2024 decision to overturn the longstanding Chevron doctrine.[37] The limited budget allocations provided to the FTC by Congress will also curtail what it can do compared to what is entailed by data regulations of the scope consistent with its recent ANPR about privacy and data security.[38]

Although Congress has attempted to enact comprehensive privacy statutes, it has failed repeatedly because of the divisive issues and complex tradeoffs involved. Existing statutes, such as the FCRA, demonstrate the way Congress recognizes tradeoffs in privacy rules. The FCRA emphasizes accuracy and fairness of credit reporting for purposes such as the efficient operation of the banking system, insurance underwriting, and better employment decisions.[39] It has specific provisions intended to achieve numerous policy goals that include but are not limited to privacy.[40]

State privacy policy

Although Congress has been unable to enact omnibus privacy legislation, a growing number of states have done so. California led the way by enacting legislation that is stricter than in most other states, resembling in some ways the European Union's GDPR.

The California Consumer Privacy Act (CCPA) requires online service providers to provide consumers with explicit notice before selling their data to third parties.[41] The data controller must also provide them with the option to opt out of having their data sold. The link enabling them to do so must be clear and easy to find and use.[42]

The California Privacy Rights Act (CPRA), which supplements the CCPA, also gives consumers the right to direct a business that collects sensitive personal information to limit its use of that information to what is necessary to perform a service or provide goods.[43] Along with the right to know what personal data

37. Manne et al., Executive Summary, 8.
38. Manne et al., 27.
39. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2011).
40. Manne et al., "FTC Advance Notice," 25.
41. Morgan Carter, "The Optimal Opt-in Option: Protecting Vulnerable Consumers in the Expanding Privacy Landscape," *Columbia Law Review* 124, no. 2 (March 2024): 442.
42. Carter, "The Optimal Opt-in," 442.
43. Preston Bukaty, *The California Privacy Rights Act (CRPA): An Implementation and Compliance Guide (Ely, UK: IT Governance Publishing, Ltd., 2021), 59.*

are being collected, shared, and used and the right to request that firms delete data collected about them, the CPRA gives consumers a right to data portability: firms must respond to a verified consumer request by providing the consumer's personal data that it has collected "in a readily usable format that allows the consumer to transmit this information from one entity to another without hindrance."[44]

Another important provision of the CPRA, which may impact the business model of exchanging services for data, is the "right to no retaliation."[45] Organizations cannot discriminate against a California resident who exercises the right to opt out of data selling. But the organization can charge different prices or provide different levels of service to those who opt out, provided the difference is "reasonably related to the value provided to the business by the consumer's data."[46] Firms that offer financial incentives to those who opt in to having their data collected must provide notice to consumers that they do so and include a "good faith estimate of the value of the consumer data that form the basis for offering the financial incentive."[47] If this rule is enforced in a heavy-handed way, with the state requiring detailed reporting from the firm about how it values the data it collects, it could significantly raise costs and limit the mutually beneficial exchange of personal data for goods and services.[48]

The variation in privacy policies between different states can raise compliance costs for online firms that do business in multiple states. A federal privacy law could reduce these costs, especially if the federal law could preempt existing state laws. But disagreement over which parts of state laws would be preempted is one of the obstacles that has made it so difficult to craft a federal privacy law that can make it through Congress.

Even with the somewhat stricter regulatory regime of California and a few other states, in the United States, informational privacy is "treated both legally and socially as more of a consumer preference . . . than a fundamental right."[49] The European Union, by contrast, treats privacy as a fundamental right.

---

44. California Privacy Rights Act, Cal. Civ. Code § 1798.130(a)(2)(A).
45. Bukaty, *California Privacy Rights Act*, 64.
46. California Privacy Rights Act, Cal. Civ. Code § 1798.125(a)(2).
47. Jeewon Kim Serrato, "How Much Is Your Data Worth? CCPA's Data Valuation Requirement Explored," *San Diego Law Review* 59, no. 4 (2022): 621.
48. It appears that firms have found ways to limit the costs of satisfying this requirement by providing general statements about the value of the data they collect that do not include numerical estimates. See examples at https://www.termsfeed.com/blog/ccpa-notice-financial-incentive/#What_Must_A_Ccpa_Cpra_Compliant_Notice_Of_Financial_Incentive_Include.
49. Manne et al., "FTC Advance Notice," 3.

Private enforcement of privacy and data security: The role of litigation

Because of the limited funding of the FTC, it only has the capacity to enforce privacy and data security in select high-profile cases, bringing an average of fewer than 20 complaints per year over the last five years.[50] In some situations, those who experience harm from data breaches or infringement of their privacy have the option of private enforcement via the courts. But under some sectoral data protection laws, such as FERPA and HIPAA, individuals cannot bring private lawsuits against firms for violating the statute.[51]

Privacy and data breach class action litigation has increased in recent years.[52] It has been hard to win privacy or data security cases because of the need to demonstrate standing to sue. For a class action to proceed, at least one class representative must have standing to pursue their own claims individually.[53] Article III of the US Constitution limits the jurisdiction of the federal courts to hearing "cases" and "controversies" so that the courts "do not intrude upon the powers" given to other branches of government.[54] To be granted Article III standing, the class representative must have experienced harm that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[55]

In data security cases, courts do not seem to have taken very seriously the probable risks associated with data breaches. Those bringing a case against a firm that experienced a data breach have often not been granted standing if they do so before any member of the class affected has experienced clear harm, such as identity theft. If they wait too long, however, courts may rule that any harm that occurred could be blamed on some other breach that happened later.

In spite of widespread concern that with private rights of action, defendant firms will incur excessive and unnecessary legal costs, in reality plaintiffs usually lose data security cases, with many dismissed for lack of standing. A few federal and state laws provide private rights of action against companies that collect or

50. "Cases Tagged with Privacy and Security," Federal Trade Commission, accessed on February 26, 2025, https://www.ftc.gov/enforcement/cases-proceedings/terms/1420?page=2.
51. McGeveran, "Friending the Regulators," 979.
52. Nabil Shaikh, "Surveillance Class Actions: Reconstructing a Federal Data Privacy Right of Action," *University of Pennsylvania Law Review* 172, no. 3/4 (2024): 868–869.
53. Shaikh, "Surveillance Class Actions," 893.
54. Lee J. Plave and John W. Edson, "First Steps in Data Privacy Cases: Article III Standing," *Franchise Law Journal* 37, no. 4 (Spring 2018): 489.
55. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013), quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).

retain personal information without proper authorization, but such laws have not resulted in courts granting much relief to plaintiffs when companies violate the letter of the law. In a number of cases, such as Gubala v. Time Warner Cable, Inc., courts have denied standing, distinguishing a technical violation of the law—in this case holding data for too long—from a violation that includes allegations of harm sufficient to be considered concrete.[56] Plaintiffs have lost several cases where courts found only a technical violation of the law.

Examples exist of effective private enforcement of privacy, though limited to narrow aspects of it. Congress enacted the Video Privacy Protection Act of 1988 (VPAA), which authorizes consumers to sue when a video tape service provider discloses personal information.[57] Although the statute refers to video tapes, consumers have used it in cases involving more modern forms of video consumption, such as streamed video feeds.[58] The VPAA has successfully protected privacy of video consumers for more than 30 years.[59]

Hybrid enforcement regimes involving a mix of agency action and private litigation have also been effective in US privacy law. Federal statutes that have hybrid enforcement regimes include the Telephone Consumer Protection Act, the FCRA, and the Driver Privacy Protection Act.[60] Regulatory agency action and private lawsuits related to these laws have resulted in concrete outcomes, including limiting abusive telemarketing practices, restricting abuse of consumer credit files, and preventing others from collecting sensitive information from drivers' records.[61]

With private rights of action, every wrong under a statute is a potential subject of litigation. This gives companies an incentive to comply in every interaction with every consumer.[62] In some situations, "the courts are the only place a person can turn to obtain redress and protection."[63] The threat of a private suit

56. Congressional Research Service, *Enforcing Federal Privacy Law: Constitutional Limitations on Private Rights of Action*, updated May 31, 2019, 3–4.
57. Lauren Henry Scholz, "Private Rights of Action in Privacy Law," *William and Mary Law Review* 63, no. 5 (2022): 1651.
58. Scholz, "Private Rights of Action," 1651–1652.
59. See "The Video Privacy Protection Act as a Model Intellectual Privacy Statute," *Harvard Law Review* 131, no. 6 (2018): 1766, 1768–1769; Ann Stehling, "From Blockbuster to Mobile Apps—Video Privacy Protection Act of 1988 Continues to Protect the Digital Citizen," *SMU Law Review* 70, no. 1 (2017): 205, 210; "Video Privacy Protection Act," Electronic Privacy Information Center, accessed February 26, 2025, https://archive.epic.org/privacy/vppa/.
60. Scholz, "Private Rights of Action," 1655–1656.
61. Scholz, 1656.
62. Scholz, 1657.
63. Alexandra Lahav, *In Praise of Litigation* (New York: Oxford University Press, 2017), 29.

may be more of a deterrent, because private litigants are more likely to collect damages than a regulatory agency.[64]

Litigation is "one part of the broader political conversation, a way to reveal critical information, sharpen reasoned arguments, and apply the language of law to divisive problems."[65] Information revealed during discovery can motivate firms to change their practices and provide insights to regulators about corporate practices and patterns of wrongdoing, which can contribute to regulatory action and reform.[66]

The application of Article III standing to privacy cases is evolving over time. The recent Supreme Court decision in TransUnion LLC v. Ramirez would seem to make it more difficult for plaintiffs to be granted standing in privacy and data security cases.[67] The case arose under the FCRA, which says that consumers can sue credit reporting agencies for reporting inaccurate information about them. The court did not grant standing to plaintiffs who did not suffer concrete harm, even though the inaccurate information in their credit reports exposed them to risk of future harm.[68] But in several circuit court decisions since that case, judges have granted standing to plaintiffs in data breach cases. The key seems to be that plaintiffs need to show that their claim is similar to a traditional cause of action. Since the law remains unsettled concerning whether plaintiffs will be granted standing in such cases when heard in federal court,[69] a comprehensive federal privacy statute, if it included a private right of action, could increase the ability of those who suffer privacy harms to gain standing in class action suits. This would increase the deterrence effect of the law.

EU Privacy Policy

The European Union has led the way in privacy protection.[70] The EU approach to privacy is a rights-based framework. Even before the enactment of the GDPR,

64. Scholz, "Private Rights of Action," 1657.
65. Lahav, *In Praise of Litigation*, 29.
66. See Joanna C. Schwartz, "Introspection Through Litigation," *Notre Dame Law Review* 90, no. 3 (2015):1055, and Érica Gorga and Michael Halberstam, "Litigation Discovery and Corporate Governance: The Missing Story About the 'Genius of American Corporate Law,'" *Emory Law Journal* 63, no. 6 (2014): 1383,1495–1496.
67. TransUnion LLC v. Ramirez, 594 U.S. 413 (2021).
68. Jim Dempsey, "US Courts Mixed in Letting Data Breach Suits Go Forward," Opinion, *IAPP*, March 9, 2022, https://iapp.org/news/a/u-s-courts-mixed-on-letting-data-breach-suits-go-forward/.
69. Dempsey, "US Courts Mixed," 5.
70. David L. Baumer, Julia B. Earp, and J.C. Poindexter, "Internet Privacy Law: A Comparison Between the United States and the European Union," *Computers and Security* 23, no. 5 (2004): 400–412.

the European Union had stricter privacy policies than the United States. Privacy regulation in EU countries became more stringent following the implementation of the EU Privacy and Electronic Communications Directive in 2003 and 2004. The EU Privacy Directive required firms to obtain consent from users before collecting their data.[71]

The GDPR, which took effect in May 2018, imposes specific requirements on firms that collect, process, or store personal data. It applies to organizations operating within the European Union and to external organizations processing data from EU residents.[72] The GDPR specifies six principles that data controllers must apply to any collection or processing of personal data. These principles spell out how the data are to be collected, the importance of having specific, explicit purposes for collecting them, and the necessity of collecting only as many data as are necessary for processing. Other principles specify rules for handling data that include maintaining their accuracy, limits on how long they may be stored, and keeping them secure.

Policy to limit the collection, processing, use, and storage of personal data is based on the recognition that what happens to the data can contribute to tangible harms, such as identity theft and discrimination against data subjects. It can also contribute to intangible harms by creating a power imbalance between those who collect and process data and data subjects, reducing the latter's bargaining power and inhibiting them from engaging in certain activities out of fear of social censure.[73]

The principle of transparency applies to all the rights protected by the GDPR.[74] Transparency requires that the data controller provide information about the purpose of the processing, the legal basis for processing, any additional recipients of the personal data, and information about the rights of the data subject and how to exercise them.

According to the GDPR, a firm cannot process personal data unless one of six lawful conditions applies.[75] Most businesses subject to the GPDR

71. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57, no. 1 (2011): 57–71.
72. Alan Calder, *EU GDPR—An International Guide to Compliance* (Ely, UK: IT Governance Publishing, 2020), 30.
73. Orla Lynskey, *The Foundations of EU Data Protection Law* (New York: Oxford University Press, 2015), 215–216.
74. Calder, *EU GDPR*, 33.
75. Meg Leta Jones and Margot E. Kaminski, "An American's Guide to the GDPR," *Denver Law Review* 98, no. 1 (2021): 93–128. The lawful conditions are: consent of the data subject, necessity for performance of a contract, necessity for compliance with a legal obligation, necessity to protect the vital interests of the data subject or another person, necessity for a task carried out in the public interest, or necessity for the "legitimate interests" of the data controller.

process personal data either based on individual consent or their legitimate interests.[76]

The GDPR requires opt-in consent for data processing, with some exceptions. Among the exceptions are when a firm processes data in pursuit of a legitimate business purpose. Advertising can be considered a legitimate business purpose, but the right to use data for advertising is constrained by other requirements of the GDPR.[77]

When a firm collects and processes data for a legitimate business purpose, it must be transparent about what kind of data it collects and its purpose for doing so. The user has the right to object and opt out of such processing. A firm must notify new users and returning users who deleted its cookies and give them a chance to opt out when they open the firm's website.[78]

After their data have been collected, data subjects have additional rights with respect to those data, including the following:

- Right of access
- Right of rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability[79]

Under the GDPR, the rights of data subjects must be balanced against other interests. For example, if an individual objects to data processing based on the processor's "legitimate interest," the law requires that the processor "demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject."[80]

The Digital Services Act, which was adopted in 2022, increases restrictions on digital advertising directed to residents of EU countries by online platforms. It includes a full ban on targeted advertising to those who are known to be minors and

---

76. See Lilian Edwards, "Data Protection: Enter the General Data Protection Regulation," in Lilian Edwards, ed., *Law, Policy, and the Internet* (Oxford, UK: Hart Publishing, 2018), cited in Jones and Kaminski, "An American's Guide," 109.
77. Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC (844/14/EN WP 217), April 9, 2014.
78. Bernd Skiera, Klaus Miller, Yuxi Jin, Lennart Kraft, René Laub, and Julia Schmitt, *The Impact of the General Data Protection Regulation (GDPR) on the Online Advertising Market* (pub. by author, 2022), 4.4.4.2.1, https://www.gdpr-impact.com/personal-data-processing-under-the-gdpr, accessed January 14, 2025.
79. Jones and Kaminski, "An American's Guide," 116.
80. General Data Protection Regulation, Right to Object, Art. 21(1), (2018) O.J. (L 127), 69 and 70, accessible at https://gdpr-info.eu/art-21-gdpr/.

on the use of sensitive data, including data on sexual orientation, political opinions, race, or health condition, for ad targeting.[81] Platforms must provide meaningful information about how users' data will be monetized and transparency about the sponsors and targeting parameters used in exposed ads. It also requires that firms make it easy for users to refuse to give consent for ad targeting using behavioral data.

EU members have also enacted the Digital Markets Act (DMA), which targets "gatekeepers" that operate "core platform services."[82] These are firms that meet quantitative thresholds, such as having a certain number of users. In 2023, seven companies qualified as gatekeepers: Amazon, Facebook, Apple, Microsoft, Alphabet (Google), Samsung, and ByteDance (TikTok). Although the DMA is primarily intended to promote competition and focuses on the rights of business users, it also has provisions that affect data privacy policy toward end users. In July 2024, the European Commission accused Facebook of violating the DMA by charging users to access its platform if they did not consent to data collection.[83] Gatekeeper platforms cannot refuse to provide core platform services to those who opt out of certain kinds of data processing, though they can provide "a less personalized but equivalent alternative."[84]

In addition to obligations connected to the rights of data subjects, the GDPR requires data controllers to maintain records of their data processing activities.[85] Companies whose core activities include processing data regularly and systematically on a large scale are required to employ data protection officers.[86]

GDPR enforcement

EU data protection regulation has been criticized as "overly bureaucratic and top-down, lacking on-the-ground oversight."[87] Several changes to privacy policy

81. Lex Zard and Alan M. Sears, "Targeted Advertising and Consumer Law in the EU," *Vanderbilt Journal of Transnational Law* 56, no. 3 (2023): 838.
82. Rupprecht Podszun, "From Competition Law to Platform Regulation—Regulatory Choices for the Digital Markets Act," *Economics* 17, no. 1 (2023): 2.
83. Adam Satariano, "Ad-Free Option for Meta Users Violates Law, E.U. Declares," *New York Times,* July 1, 2024.
84. Regulation (EU) 2022/1925, (2022) O.J. (L 265) 1-66, available at https://eur-lex.europa.eu/eli/reg/2022/1925/oj.
85. Jones and Kaminski, "An American's Guide," 117.
86. "Recital 97—Data Protection Officer," Intersoft Consulting, accessed on January 14, 2025, https://gdpr-info.eu/recitals/no-97/.
87. Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Boston: MIT Press, 2015), cited in Inbar Mizarhi-Borohovich, Abraham Newman, and Ido Sivan-Sevilla, "The Civic Transformation of Data Privacy Implementation in Europe," *Western European Politics* 47, no. 3 (2023): 672.

came about as a result of the GDPR, including a common set of rules for each EU member country, an increase in the size of penalties that can be imposed on large transnational firms, and a rule that offers third parties like nongovernmental organizations (NGOs) an explicit role in the enforcement process.[88]

Many NGOs have mobilized in defense of privacy, among them civil liberties organizations and consumer protection organizations.[89] Many of the largest transnational GDPR cases were initiated by NGOs. Max Schrems, an Austrian lawyer and privacy activist, helped establish an NGO, None of Your Business (NOYB), to go after companies that violate the GDPR to gain a competitive advantage.[90]

So far, there is little evidence that regulatory action has led to fundamental changes in the way personal data are used for digital advertising in the European Union.[91] Due to the complexity and opacity of the digital advertising ecosystem, there are obstacles to GDPR enforcement.[92] In several recent cases involving data used for digital advertising, data protection authorities have accused platforms of noncompliance with GDPR rules; however, current market practices are likely to persist until the Court of Justice of the European Union hands down final rulings.[93]

Consequences of EU privacy regulation

GDPR requirements are costly for firms but can also be costly for users. Firms that collect data must obtain permission from users to process their data, which involves three steps: (1) "specifying purposes for data processing for which permission is being provided;"(2) requesting permission and storing a record of it; and (3), carrying out transfers of data to other firms "in accordance with permissions that the user has provided."[94]

88. Mizarhi-Borohovich et al., "Civic Transformation," 675.
89. Mizarhi-Borohovich et al., 676.
90. Warwick Ashford, "Max Schrems Champions NGO to Fight for GDPR Rights," *Computer Weekly*, January 9, 2018.
91. Catherine Armitage, Nick Botton, Louis Dejeu-Castang, and Laureline Lemoine, *Towards a More Transparent, Balanced, and Sustainable Digital Advertising Ecosystem: Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers, and Advertisers* (Brussels: European Commission, 2023), 251.
92. Armitage et al., *Advertising Ecosystem*, 252.
93. Armitage et al., 253.
94. Skiera et al., *Impact of the GDPR, 7.1*, https://www.gdpr-impact.com/getting-user-permission-for-personal-data-processing-via-the-transparency-and-consent-framework-tcf, accessed January 14, 2025.

Obtaining permission can be especially costly for firms that use the data for programmatic advertising. Online publishers and others that collect data for programmatic advertising typically share the data with a large number of vendors. Users must grant permission for each vendor and each purpose for which a vendor intends to use the data. The firm that wishes to collect the data must provide information about each vendor to each data subject. Consent management platforms make it easy for users who are willing to grant blanket consent for each firm involved to process their data, but for those who intend to grant consent for a subset of vendors and purposes, doing so can be time-consuming.

Firms have taken several steps to respond to GDPR rules, but the resulting reduction in collection and processing of personalized data has been costly. Seeking users' consent to collect data as required by the GDPR leads to a reduction in the share of users about whom firms have data they can use for targeted advertising. If advertisers do not have data to target ads to a particular user, they can still show ads to that user, but the ads may be less effective. One study estimates that advertisers in the European Union will pay between 18 and 23 percent less to advertise to users for whom tracking is disabled compared to what they pay if tracking is enabled.[95] This reduces revenue to publishers and other service providers, which means they will likely reduce the quality of the free content they provide online.

Some publishers have been able to maintain or increase their revenue without tracking by, for example, making better use of contextual advertising.[96] But, as noted below, as they track fewer users, empirical evidence suggests that publishers have lost revenue in the aggregate. Tracking makes it possible to monitor and limit the ads shown to a particular user based on recency and frequency, while also enabling AdTech firms to estimate the relationship between ad impressions and purchase decisions.

The enactment of the GDPR reflects demand for "data transparency" and individual empowerment in the context of growth in online collection and processing of personal data.[97] But concrete transparency practices mandated by the

95. See René Laub, Klaus M. Miller, and Bernd Skiera, "The Economic Value of User Tracking and Behavioral Targeting for Publishers" (Working Paper, Goethe University, Frankfurt, 2022), 38, and Garrett A. Johnson, Scott Shriver, and Shaoyin Du, "Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?," *Marketing Science* 39 (1): 33–51. Laub, Miller, and Skiera find that the difference is about 23 percent in the European Union.
96. Skiera et al., *Impact of the GDPR, 5.2.2.1,* https://www.gdpr-impact.com/effects-of-the-requirement-for-a-legal-basis-for-data-processing-on-the-online-advertising-market, accessed January 14, 2025.
97. Frederik Schade, "Dark Sides of Data Transparency: Organized Immaturity After GDPR?" *Business Ethics Quarterly* 33, no. 3 (2023): 474.

GDPR produce "new types, forms, or levels of opacity."[98] Organizations selectively disclose information that serves their interests, rely on ambiguous statements to avoid conflict, and use information disclosures to limit liability rather than communicate clearly with users.[99] Furthermore, lax enforcement means that only a small percentage of complaints filed about GDPR violations has been addressed.[100]

Empirical evidence

Early on, EU privacy regulation had significant impacts on the online economy. Avi Goldfarb and Catherine Tucker report empirical estimates about the impact of the EU Privacy Directive, which requires user consent to collect personal data.[101] It became more difficult to obtain data as people opted out of data collection. The authors found a 65-percent reduction in the effectiveness of banner ads following the implementation of the directive, if effectiveness is defined as stated intent to purchase a product or service being advertised.[102] The reductions in ad effectiveness were larger for websites with more general content that could not easily be linked with a specific product.[103] Contextual ads that are not targeted based on personal information are relatively more effective on sites with more specialized content.

More recently, the GDPR has contributed to decreased investment in technology ventures, encouraged app exit, discouraged app development, decreased the usage of tracking technology tools, decreased e-commerce revenue, and increased market concentration in the advertising sector.[104] But concentration among technology vendors seems only to have temporarily increased following implementation of the GDPR.[105]

By raising the marginal cost of data, the GDPR has motivated firms to reduce the amount of data stored (by 26 percent) and data processing (by 15 per-

98. Schade, "Dark Sides," 481.
99. Schade, 482.
100. The number of fines and sanctions levied in the two years after the GDPR was implemented amounted to less than 1 percent of complaints filed about GDPR violations within its first year. See Schade, "Dark Sides," 492.
101. Goldfarb and Tucker, "Privacy Regulation," 63–65.
102. Goldfarb and Tucker, 64.
103. Goldfarb and Tucker, 70.
104. Mert Demirer, Diego J. Jiménez Hernández, Dean Li, and Sida Peng, "Data, Privacy Laws, and Firm Production: Evidence from the GDPR" (NBER Working Paper No. 32146, National Bureau of Economic Research, Cambridge, MA, February 2024), 5.
105. Garrett A. Johnson, Scott K. Shriver, and Samuel G. Goldberg, "Privacy and Market Concentration: Intended and Unintended Consequences of GDPR," *Management Science* 69, no. 10 (2023): 5695–5721.

cent) in producing goods and services.[106] Larger firms have seen smaller reductions in data storage and processing due to the GDPR.

In a study of online search and browsing behavior using a panel across four countries, Yu Zhao et al. found that panelists from the United Kingdom and Spain visited 14.9 percent more domains and spent 44.7 percent more time on the web after GDPR relative to non-EU panelists (from the United States and Brazil).[107] The authors suggested that these differences include a combination of increased privacy benefits and costs exemplified by "the inefficiency firms face to reach out to consumers" as a result of the GDPR.[108] EU panelists also submitted more search terms per topic, which may reflect higher information friction.[109]

Other studies show declines in profits and sales for online firms operating in the European Union. Large technology companies did not experience a statistically significant decline, but the profit decline experienced by small technology companies was almost double the average effect.[110]

Research has not shown that the GDPR has affected the quantity or quality of content provided by online news and media websites. In a study covering a two-year period during the implementation of the GDPR, online content providers did not alter their advertising intensity or the quantity or quality of their content, although they reduced third-party tracking.[111] The question is why such firms have not been negatively impacted like many others have. The authors of the study speculate that news and media sites with numerous EU visitors either continue to collect personal data as before, justifying doing so based on their legitimate business interests, or that, following enactment of the GDPR, they temporarily reduced tracking but found ways to revamp their data collection efforts several months later.[112]

---

106. Demirer et al., "Data, Privacy Laws, and Firm Production," 2.
107. Yu Zhao, Pinar Yildirim, and Pradeep Chintagunta, "Privacy Regulations and Online Search Friction: Evidence from GDPR" (MSI Report No. 23-41, Marketing Science Institute Working Paper Series 2023, New York, NY, November 2023), 2–3.
108. Zhao et al. find that with less ability to collect data on consumers, firms will have a harder time matching online products and services with consumer characteristics and interests.
109. Zhao et al., "Privacy Regulations," 4.
110. Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally" (Oxford Martin School Working Paper 2022-1, University of Oxford, Oxford, UK, January 2022), 1.
111. Vincent Lefrere, Logan Warberg, Cristobal Cheyre, Veronica Marotta, and Alessandro Acquisti, "Does Privacy Regulation Harm Content Providers? A Longitudinal Analysis of the Impact of the GDPR," (forthcoming in *Management Science*), November 15, 2024, 48–49, https://ssrn.com/abstract=4329013.
112. Lefrere et al., "A Longitudinal Analysis," 6.

A study of the impact of the GDPR on advertisers found modest decreases in the performance of ads, their bid prices, and publishers' ad revenue.[113] Publishers of certain types of content, such as sports, were able to mitigate the consequences of reduced data through contextual targeting.

The GDPR and the future of the online economy in EU member countries

In response to revenue losses resulting from GDPR implementation, some firms, such as the *Washington Post, have implemented cookie paywalls*.[114] These give users a choice between opting into tracking and paying for content without being tracked. Some have questioned whether requiring tracking in exchange for access to free content is consistent with the principle stated in the GDPR that consent for data collection must be freely given.[115]

As firms continue to collect data from consumers to use for online behavioral advertising, questions have been raised about whether the associated business model needs major reform to fully comply with the GDPR. The online behavioral advertising business model relies largely on real-time bidding (RTB), an auction process by which advertisers bid to show ads to groups of users based on the users' profiles.[116] Websites seek user consent before anyone knows what kinds of data "will be combined, collected, or retained in order to inform the bids."[117] User profiles are created and shared "within an ecosystem comprising thousands of organizations."[118] In order to comply with the GDPR, when a new user visits the website of a firm that relies on RTB, the owner of the website must request the user's permission to allow hundreds of vendors to acquire or process that person's data. If a vendor uses the data for more than one purpose, they must obtain consent for each one.[119]

---

113. Pengyuan Wang, Li Jiang, and Jian Yang, "The Early Impact of GDPR Compliance on Display Advertising: The Case of an Ad Publisher," *Journal of Marketing Research* 61, no. 1 (2024): 70–91.
114. Skiera et al., *Impact of the GDPR, 5.2.2.2*, https://www.gdpr-impact.com/effects-of-the-requirement-for-a-legal-basis-for-data-processing-on-the-online-advertising-market.html?q=Washington%20Post#effects-on-the-user-3, accessed January 14, 2025.
115. Skiera et al., 5.2.2.2.
116. Michael Veale, Midas Nouwens, and Cristiana Santos, "Impossible Asks: Can the Transparency and Consent Framework Ever Authorize Real-Time Bidding After the Belgian DPA Decision?," *Technology and Regulation* 2022 (2022): 12.
117. Veale et al., "Impossible Asks," 19.
118. UK Information Commissioner's Office, *Update Report into AdTech and Real-Time Bidding*, June 20, 2019.
119. Skiera et al., *Impact of the GDPR, 4.4.4.2.2*, https://www.gdpr-impact.com/personal-data-processing-under-the-gdpr, accessed January 14, 2025.

The Interactive Advertising Bureau (IAB) is a membership organization that launched an industry initiative, the Transparency and Consent Framework (TCF), to help firms get users' permission to collect and process data as part of the RTB system.[120] Users can grant blanket consent for all partner vendors, all purposes, or both when a firm requests to collect and process their data.

The Belgian Data Protection Authority (DPA) recently decided a case that will require IAB to revamp the TCF system based on the assertion that its current approach is not in compliance with the GDPR.[121] The Belgian DPA determined that TCF fails to comply with GDPR principles of transparency, fairness, accountability, and the conditions under which it is legal to process consumer data.[122]

Based on the Belgian DPA's decision, there is reason to ask whether the requirements of the GDPR are "irreconcilable with the fundamental functioning of RTB."[123] In what it is requiring of the IAB, the Belgian DPA emphasizes the transparency principle. It asserts that information provided to data subjects about the processing of their personal data should be "comprehensible, concise, and prevent unpleasant surprises for data subjects" that might result in the future.[124]

The GDPR specifies that user-friendly information is particularly important when the complexity of the process makes "it difficult for the data subject to know and understand whether, by whom, and for what purpose personal data" are being collected.[125] But many website visitors are asked to consent to data processing without understanding what RTB entails.[126] In a survey conducted in the United Kingdom, 63 percent of respondents perceived advertising based on RTB to be acceptable. But after the participants were given information on how RTB works, the percentage that said that RTB was acceptable fell to 36 percent.[127]

Given the political power of activist organizations, it would not be surprising if they put pressure on European data protection officials to enforce the

120. Veale et al., "Impossible Asks," 12.
121. Veale et al., 14.
122. Natasha Lomas, "IAB Europe's Ad Tracking Consent Framework Found to Fail GDPR Standard," *TechCrunch*, October 16, 2020.
123. Veale et al, "Impossible Asks," 19.
124. Veale et al., 19.
125. "Recital 58—The Principle of Transparency," accessed on February 27, 2025, Intersoft Consulting, https://gdpr-info.eu/recitals/no-58/.
126. Michael Veale and Frederik Zuiderveen Borgesius, "AdTech and Real-Time Bidding Under European Data Protection Law," *German Law Journal* 23, no. 2 (2022): 250.
127. In Michael Worledge and Mike Bamford, *Adtech Market Research Report* (Wilmslow, Cheshire: UK Information Commissioner's Office, March 2019), the instruction about RTB given to each participant stated that websites share the following kinds of information with advertisers: browsing history; device identifiers such as model of phone, operating system, and IP address; location; gender; year of birth; past purchase history; and search history.

GDPR more strictly in the future, making it more difficult to obtain consent from users to sell or share data with the numerous vendors involved. This could lead to further reductions in online behavioral advertising. Privacy advocacy organizations like NOYB are pursuing cases that, if decided in their favor, would make it more difficult to collect data for online behavioral advertising.[128]

Alternative Futures

Users of online services have legal rights, which vary by jurisdiction, to limit data collected about them, usually via opting in or opting out of data collection on websites they visit. Perceiving that some users value privacy highly, entrepreneurs have offered a variety of services to limit data collection. Privately provided services to limit data collection include Apple's app tracking transparency, browsers that have limited or deprecated the use of cookies, and companies that provide ad-blocking services, such as AdBlock Plus. When platforms like Apple take actions that make it harder to track their users, they have an incentive to do so in a way that restricts third-party tracking without similarly restricting their own ability to collect and profit from their users' data.[129]

As a growing number of users opt out of data collection or targeted advertising, online service providers have responded in a variety of ways. Some have resorted to charging higher fees for content, and others have used a white-listing strategy or an ad recovery strategy in response to the use of ad-blocking software. Adblockers may white-list publishers that agree to display ads that comply with quality standards, but such ads are only displayed to users who accept the publisher's white-listed status.[130] Because of the revenue lost due to the use of ad-blocking applications, some publishers use an ad-block circumvention strategy that enables them to keep showing ads to consumers who use an adblocker.[131]

One view is that the future, like the past, will involve an arms race "between web users and advertisers as each party develops ever more sophisti-

128. See for example, "'Pay or OK' at Der Spiegel: Noyb Sues Hamburg DPA," *NOYB*, August 1, 2024, https://noyb.eu/en/pay-or-ok-der-spiegel-noyb-sues-hamburg-dpa.
129. With IOS 14.5, Apple introduced an opt-in mechanism that imposes more restrictive privacy rules on competing app developers than Apple applies to its own apps, thereby giving itself an advantage over competing apps in terms of collecting data that can be used for targeted advertising. See Giuseppe Colangelo, "The Privacy–Antitrust Curse: Insights from GDPR Application in Competition Law Proceedings," *The Antitrust Bulletin* (2024).
130. Ashutosh Singh, S. Sajeesh, and Pradeep Bhardwaj, "Whitelisting Versus Advertising-Recovery: Strategies to Overcome Advertising Blocking by Consumers," *European Journal of Operational Research* 318, no. 1 (2024): 217–229.
131. Singh et al., "Whitelisting," 218.

cated methods for avoiding and delivering ads."[132] There is, however, the chance for entrepreneurs to develop mutually beneficial solutions: instead of firms further limiting their data collection and targeted advertising, technology could be used to make advertising and associated profiling more transparent to users, enabling them to exercise greater choice about the kinds of ads they see, while also restricting how their online profile may be used for targeting, so as to better protect their privacy.[133]

Regulation, such as the GDPR, contributes to the arms race between users and advertisers. An important question is the extent to which regulation will lead to reductions in programmatic advertising, and, if it does, how this will affect the quality of online content. Although intuition suggests that reduced advertising revenue due to less personalized advertising would reduce the quality of online content, this is not necessarily the case.

Some evidence points to the possibility that a considerable amount of revenue from programmatic advertising goes to sites presenting fake news and misinformation, because those sites attract lots of user attention.[134] If firms used less personalized advertising and more contextual advertising, advertisers might pay more to advertise on sites providing quality content.

Before programmatic advertising became predominant, marketing strategies focused on long-term brand awareness, relying partly "on cultivating brand loyalty over the long term by establishing positive associations with consumers' favored editorial products."[135] Higher-quality editorial products could thus generate more advertising revenue. But as more advertising emphasizes behavioral targeting, advertisers have tended to focus on short-term interactions with consumers when they seem most likely to buy in response to viewing an ad.[136] The quality of the content on the site where they advertise is less important to advertisers who use this approach.

Programmatic advertising involves the coordination of many different firms each time an ad is placed, reducing the control or knowledge of brands

132. Alexander Zambrano and Caleb Pickard, "A Defense of Ad Blocking and Consumer Inattention," *Ethics and Information Technology* 20, no. 3 (2018): 154.
133. For an example of a proposal of this kind, see Javier Parra-Arnau, Jagdish Prasad Archara, and Claude Castellucia, "MyAdChoices: Bringing Transparency and Control to Online Advertising," *ACM Transactions on the Web* 11, no.1 (2016): 1–47.
134. Garett Sloane and Jack Neff, "Advertisers Waste 23% of Programmatic Ad Dollars, ANA Study Finds," *Ad Age*, June 19, 2023.
135. Joshua A. Braun and Jessica L. Eklund, "Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism," *Digital Journalism* 7, no. 1 (2019): 3.
136. Braun and Eklund, "Fake News," 3.

about the sites on which their ads appear.[137] With less knowledge and control, their ads are more likely to end up on sites providing lower-quality content, which may include misinformation. Thus, one argument for using stricter privacy regulation to reduce or eliminate programmatic advertising is that doing so could result in a greater proportion of advertising revenue being directed to publishers providing information of higher quality.

But rather than discouraging programmatic advertising, other approaches may be equally or more effective in getting advertisers to spend a greater share of their advertising dollars on sites that provide quality content. Having its products associated with misinformation, disinformation, and fake news harms a company's reputation.[138] As marketers become more aware of the risks associated with programmatic advertising, they can partner with others in the AdTech ecosystem to develop better brand safety and suitability strategies to guide their ad spending.[139]

Conclusion

Concerns about data privacy have led to growing regulation of the data collection and processing practices of online firms, more so in the European Union than in the United States. Several US states have enacted privacy laws that include provisions similar to the GDPR, but they are not as stringent. Large platforms are under pressure from regulators—particularly in the European Union—and from consumers everywhere to limit their data collection, especially by third parties, to make it more transparent, and to give data subjects more control over their data.

The GDPR has had unintended consequences, such as reducing the revenue and profits of small online firms more than it reduces them for large firms. It seems also to have reduced innovation. It could lead to major changes in the business model of exchanging data for services in the future, depending on how it is enforced.

In spite of growing regulation, which has raised transaction costs and had some impact on market structure, particularly in Europe, the dynamism of the online economy offers promise that entrepreneurial solutions to privacy problems that are mutually beneficial can arise, particularly from the private sector. Firms are experimenting with more privacy-sensitive approaches to data collec-

137. Braun and Eklund, 3.
138. Jessica Miles, "In the Age of Misinformation, How Misleading Content Impacts Digital Advertising," *B&T*, August 2, 2022.
139. Miles, "Age of Misinformation."

tion and processing. The biggest impact so far, however, seems to be a growing number of users who opt out, which has the potential to reduce profits and motivate some online service providers to alter their business models.

California and a few other states are taking an approach that is similar in important ways to the GDPR. Unlike the GDPR, however, the strictest state laws do not limit firms to only selling the data of users who have opted *in*; instead, they allow firms to provide the option to opt *out* of data collection. Default settings make a difference. Users are less likely to permit their data to be collected if firms must require them to opt in before doing so than if firms may collect data from anyone who fails to opt out.[140] Nevertheless, strict state laws such as the CPRA pose a significant threat to the viability of the business model of exchanging data for services. The CPRA is problematic to the extent that it takes a heavy-handed approach in requiring firms to document the value of the data they collect to be permitted to offer differential benefits to those who do not opt out of data collection.

It is not clear whether a more top-down approach, as exemplified by the GDPR and related rules in the European Union, will result in better outcomes for data subjects. Over time, firms find ways to adhere to the letter of the law even while, in many cases, their disclosures about data collection and processing remain opaque. Rather than leading to a new business model that radically transforms the online economy, as suggested by some privacy proponents,[141] the benefits for consumer privacy so far have been marginal, and the GDPR is a costly way to achieve those changes.

Since it would be hard to repeal the cumbersome requirements of the GDPR that constrain online firms doing business in Europe, the federal and state governments in the United States should be careful not to imitate the EU model too closely. But by trial and error, with the checks and balances that constrain our political system, we can hope that legislation, regulation, and institutional change can contribute to the evolution of the online economy. Data collection and processing can occur transparently, with respect for consumer preferences, while continuing to encourage innovation and offer opportunities for the mutually beneficial exchange of data for services.

---

140. Young Min Baek, Young Bae, Irkwon Jeong, Eunmee Kim, and June Woong Rhee, "Changing the Default Setting for Information Privacy Protection: What and Whose Personal Information Can Be Better Protected?," *Social Science Journal* 51, no. 4 (2014): 523–533.

141. An example of a radically different business model is a system in which all internet users would be able to fully control the data that is collected about them online and use data intermediaries to bargain for monetary exchanges that enable them to earn revenue from all the data they are willing to exchange. A similar vision is laid out in John K. Thompson, *Data for All* (Shelter Island, NY: Manning Publications, 2023).

About the Author

Tracy Miller was Senior Research Editor at the Mercatus Center at George Mason University. His research interests include antitrust policy, environmental policy, health economics, and transportation policy. Miller has published articles on health policy, fiscal policy, antitrust policy, privacy policy, and transportation policy. He received his PhD in economics from the University of Chicago.