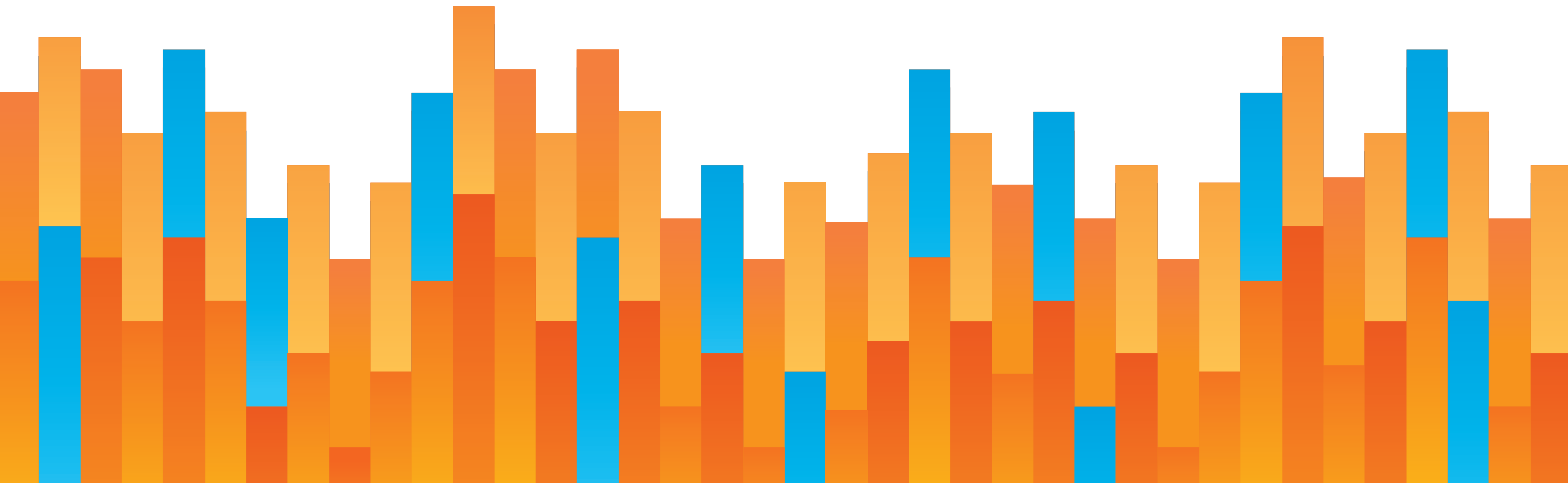
reason FOUNDATION

CONSENT REQUIREMENTS IN COMPREHENSIVE DATA PRIVACY LAWS: CURRENT PRACTICES AND THE PATH FORWARD

by Jen Sidorova and Nicole Shekhovtsova
Project Director: Max Gulker

June 2025



Reason Foundation's mission is to advance a free society by developing, applying, and promoting libertarian principles, including individual liberty, free markets, and the rule of law. We use journalism and public policy research to influence the frameworks and actions of policymakers, journalists, and opinion leaders.

Reason Foundation's nonpartisan public policy research promotes choice, competition, and a dynamic market economy as the foundation for human dignity and progress. Reason produces rigorous, peer-reviewed research and directly engages the policy process, seeking strategies that emphasize cooperation, flexibility, local knowledge, and results. Through practical and innovative approaches to complex problems, Reason seeks to change the way people think about issues, and promote policies that allow and encourage individuals and voluntary institutions to flourish.

Reason Foundation is a tax-exempt research and education organization as defined under IRS code 501(c)(3). Reason Foundation is supported by voluntary contributions from individuals, foundations, and corporations. The views are those of the author, not necessarily those of Reason Foundation or its trustees.

TABLE OF CONTENTS

PART 1 INTRODUCTION....1

PART 2 DEFINITION OF CONSENT AND CURRENT LEGISLATIVE LANDSCAPE....4

PART 3 USER EXPERIENCE AND ATTITUDES TOWARD PRIVACY....10

PART 4 IMPACT ON INDUSTRY....16

4.1 FAVORING LARGER FIRMS AND LIMITING COMPETITION....16

4.2 TECHNICAL CHALLENGES OF CONSENT MANAGEMENT....21

4.3 IMPACT ON INNOVATION AND PRODUCT DEVELOPMENT....23

PART 5 POLICY RECOMMENDATIONS....25

ABOUT THE AUTHORS....30

PART 1

INTRODUCTION

In an era where personal data is both a critical economic asset and a sensitive aspect of individual autonomy, privacy laws worldwide increasingly rely on user consent as the primary mechanism for governing data collection, processing, and sharing. However, despite its central role, the effectiveness of current digital consent frameworks remains highly contested.

This paper critically reviews how consent currently operates within major regulatory frameworks, particularly contrasting the European Union's stringent, opt-in based General Data Protection Regulation (GDPR) against the predominantly opt-out approach of the United States, exemplified by California's Consumer Privacy Act (CCPA).[1, 2]

> *… privacy laws worldwide increasingly rely on user consent as the primary mechanism for governing data collection, processing, and sharing.*

1 General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, European Parliament and Council of the European Union, April 27, 2016.

2 California Consumer Privacy Act (CCPA), California Civil Code, Title 1.81.5, §1798.100 - 1798.199, California State Legislature, June 28, 2018.

Part 2 outlines key legal frameworks and definitions. Part 3 examines how consent mechanisms shape user behavior, finding that repeated prompts often lead to disengagement rather than meaningful choice. Part 4 analyzes the broader economic effects, showing that consent requirements tend to favor large firms, raise compliance costs for smaller players, and constrain innovation. In the final section, we synthesize leading policy and academic proposals to outline a set of potential reforms. These include risk-based consent frameworks, universal privacy management tools, and co-regulatory accountability models.

The GDPR, adopted in 2016 and enacted in 2018, is built around the more stringent opt-in approach and aspires to consent that is "freely given, specific, informed, and unambiguous."[3] The CCPA, adopted in 2018 and enacted in 2020, in effect for U.S. firms doing business in California, follows an opt-out approach, where consent is presumed unless actively withdrawn. As the U.S. and other countries debate national approaches to data privacy, the debates remain unresolved.

Drawing on empirical studies, this review highlights persistent shortcomings in current consent models—from interface design flaws to the disproportionate compliance burden on smaller entities.

Drawing on empirical studies, this review highlights persistent shortcomings in current consent models—from interface design flaws to the disproportionate compliance burden on smaller entities. It concludes by identifying potential reforms aimed at balancing user autonomy, regulatory flexibility, and market competitiveness.

[3] Article 4 of the General Data Protection Regulation (GDPR)

TABLE 1: AMERICAN VS. EUROPEAN STYLE OF PRIVACY REGULATION.

	United States	**European Union**
Consent model	Notice and Opt-out	Notice and Opt-in
Implementation	Individuals are informed that certain data collection or processing practices are enabled by default, and you are provided with the opportunity to broadly object or decline participation. The assumption is that you agree to the privacy settings until you say otherwise.	Individuals are informed upfront about certain data collection or processing practices and asked to expressly consent to each. The assumption is that you do not agree to the company's privacy settings until you explicitly do.
Cultural driver	Stronger emphasis on giving individuals and companies an opportunity to freely contract and exchange information.	Emphasis on protecting individual's privacy rights and freedoms through regulatory mandates.
Example laws	• California Consumer Privacy Act (CCPA) • California Privacy Rights Act (CPRA) • Colorado Privacy Act (CPA)	General Data Protection Regulation (GDPR)

PART 2

DEFINITION OF CONSENT AND CURRENT LEGISLATIVE LANDSCAPE

Consent is a foundational principle of privacy frameworks that serves as a primary mechanism for individuals to control how their personal data is collected, processed, and shared. Across all data privacy laws and legislative proposals that have emerged in the past decade we observe two primary approaches to consent:

- Opt-in consent, where users must explicitly provide permission for their data to be collected and used; and
- Opt-out consent, where users provide permission by default and must explicitly withdraw it when they do not wish to have data collected and used.

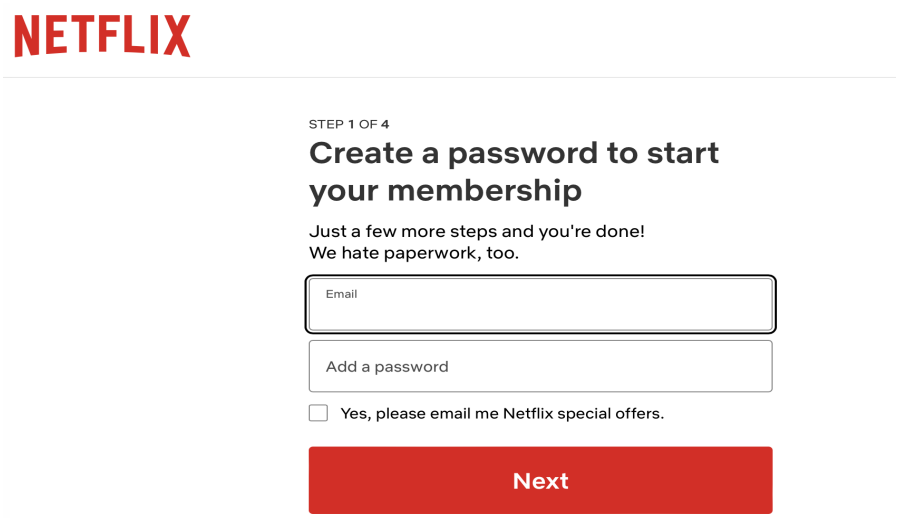
The EU's GDPR, sets out stringent requirements for opt-in consent—it must be "freely given, specific, informed, and unambiguous."[4] The GDPR governs the processing of personal data and applies to any organization—regardless of where it is based—that offers goods or services to individuals in the EU or monitors their behavior within the EU. The GDPR imposes one of the strictest standards requiring an opt-in consent, which means that an individual must take affirmative steps, such as ticking a box or signing a document, to

[4] Article 4 of the General Data Protection Regulation (GDPR).

agree to the collection of data. For example, websites that use cookies to track users' behavior or personalized ads must first ask for permission through a pop-up banner when they first visit the website.

Figure 1 shows Netflix's sign-up page in Europe, which explicitly requires users to actively tick a checkbox to opt in to receive promotional emails.

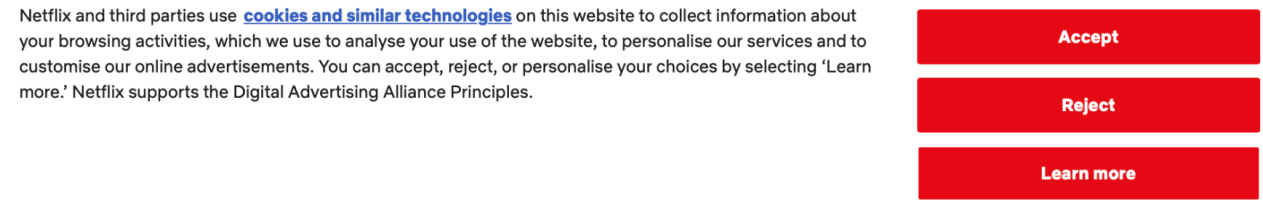
FIGURE 1: NETFLIX WEBPAGE IN EU JURISDICTION



Source: Author's screen capture of the Netflix website in EU jurisdiction.

Netflix's European website also provides users with a clear choice to accept or reject cookies, aligning with GDPR's explicit consent requirements (Figure 2):

FIGURE 2: NETFLIX COOKIE POLICY IN EU JURISDICTION



Source: Author's screen capture of the Netflix website in EU jurisdiction.

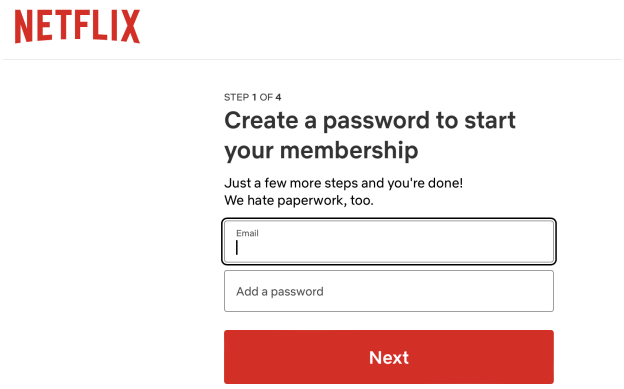
The United States does not have a federal law analogous to GDPR. Instead, data privacy is primarily regulated at the state level, resulting in a fragmented legal landscape with overlapping territorial scopes. For instance, the California Consumer Privacy Act (CCPA), as amended by CPRA, applies to any business that "does business" in California and meets

certain thresholds—such as having annual gross revenues over $25 million; buying, selling, or sharing the personal information of 100,000 or more consumers; or deriving 50% or more of its annual revenue from selling personal information.[5] In the absence of overriding federal legislation, California's rules effectively function as a national standard for many large digital firms operating across the U.S.[6]

The CCPA takes an opt-out approach to consent for the usage of data, in contrast to GDPR. Businesses must inform consumers and allow them to opt out of the "sale" or sharing of personal data, rather than obtain prior consent.[7] This allows companies to collect and process data by default, requiring users to take action to restrict the use of their personal information.

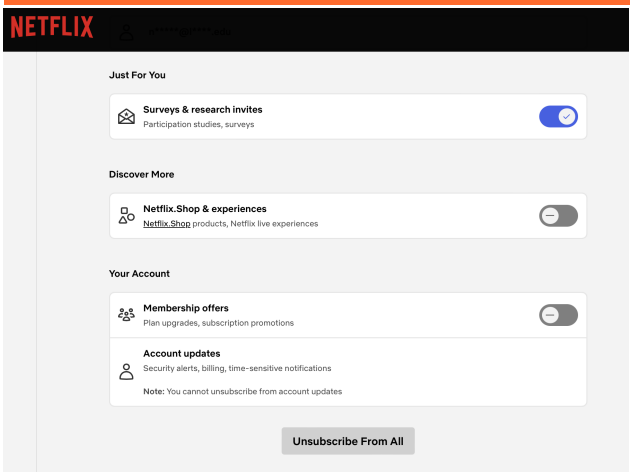
When a user signs up for Netflix in the U.S., he or she will automatically start receiving email communications by default and can later unsubscribe to opt out (Figure 3). This exemplifies the American opt-out consent approach, where users must actively seek ways to limit communication rather than explicitly agreeing upfront.

FIGURE 3: NETFLIX WEBPAGE IN US JURISDICTION



Source: Author's screen capture of the Netflix website in US jurisdiction.

FIGURE 4: NETFLIX COOKIE POLICY IN US JURISDICTION



Source: Author's screen capture of the Netflix website in US jurisdiction.

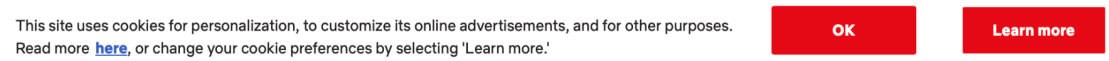
5 The California Consumer Privacy Act (CCPA) was amended by the California Privacy Rights Act (CPRA), with the changes taking effect in 2023.

6 *Section 1798.140. of the California Consumer Privacy Act (CCPA).*

7 California Consumer Privacy Act (CCPA), California Civil Code, Title 1.81.5, §1798.100 - 1798.199, California State Legislature, June 28, 2018.

Also, Netflix's U.S. website employs a simpler cookie notification approach, informing users of cookie usage without providing an explicit "Reject" option:

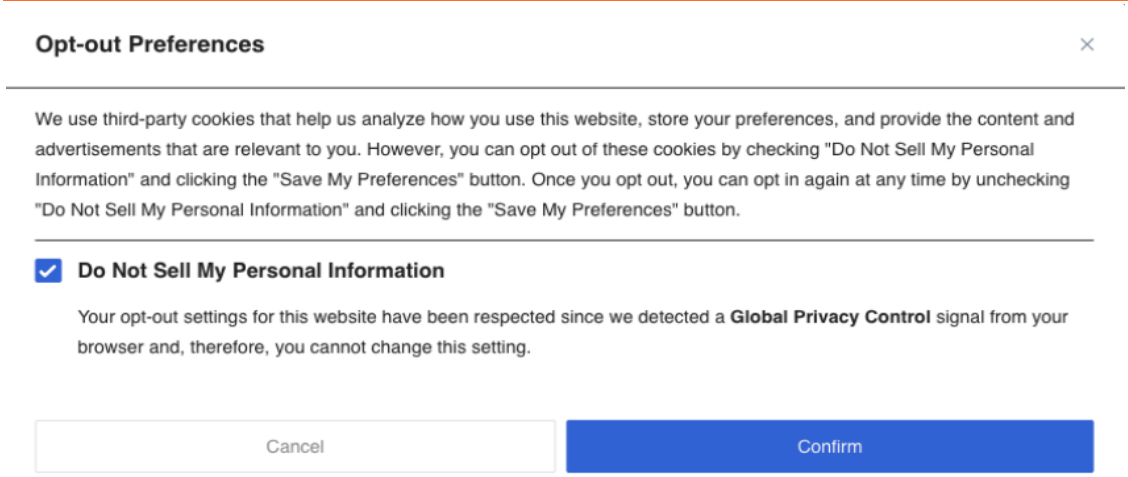
FIGURE 5: NETFLIX COOKIE POLICY IN US JURISDICTION



Source: Author's screen capture of the Netflix website in US jurisdiction.

Because of this opt-out mechanism, the CCPA also requires a clear "Do Not Sell or Share My Personal Information" link for users to opt out of the sale of their personal information (Figure 6). Consequently, companies are permitted to collect and process user data by default, shifting the responsibility onto individuals to restrict the usage of their personal information.

FIGURE 6: CCPA STYLE OPT-OUT REQUIREMENT WINDOW



Source: Author's screen capture of CCPA opt-out preferences in US jurisdiction.

Most major digital services in the U.S. rely on opt-out frameworks for both data collection and communications. For example, Hulu accounts are by default enrolled in promotional email and ad targeting, with users having to manually opt out if desired. Hulu's policy explicitly states "You may opt out of receiving promotional communications by clicking the 'unsubscribe' link" in emails—implying consent is assumed until one opts out.[8] Similarly, Hulu's cookie use is automatic; the company provides an opt-out mechanism (e.g. a browser cookie or "Do Not Sell" form) if users proactively indicate their preference. Disney+ follows

[8] Hulu, Privacy Policy, https://press.hulu.com/privacy-policy/ (accessed 10 Apr. 2025).

a comparable model: When creating an account, users are "given the opportunity to consent" to marketing, but if they do nothing, they will receive emails by default, with the option to later unsubscribe in settings.[9] Amazon Prime Video, and Amazon generally, also presumes consent for personalization and marketing. U.S. users do not see an opt-in consent screen for cookies or ads—they are simply presented with a privacy notice and can find opt-out links like ad preference centers or unsubscribe options if they seek them. The consistency of these practices across big streaming platforms shows that the responsibility is on privacy-conscious consumers to go into account settings or footers to opt out.

As a result, companies in opt-out jurisdictions can more easily gather user data without interrupting the user experience, which many businesses see as a practical and commercially beneficial approach. If customers strongly preferred a strict opt-in, one might expect at least one of these streaming giants to differentiate by offering it as a competitive feature. So far, however, major U.S. platforms do not do so voluntarily, suggesting that the market—even with significant player competition—has not rewarded an opt-in model enough to entice providers to adopt it.

If customers strongly preferred a strict opt-in, one might expect at least one of these streaming giants to differentiate by offering it as a competitive feature.

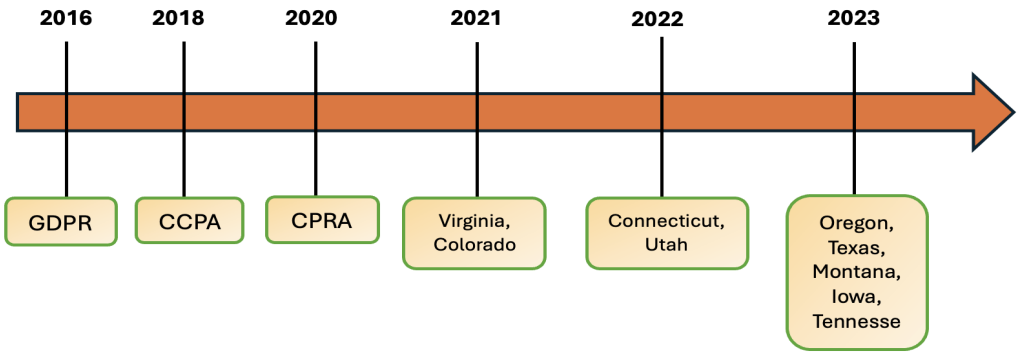
There is little evidence that any service has gained a competitive edge by adopting the European standard. If Disney+ had made all tracking or marketing *opt-in only* as a selling point, it is not clear if users would switch to Netflix or Amazon–and indeed Disney has not chosen to do so in the U.S. What we observe is that voluntary opt-in mechanisms are rare in opt-out jurisdictions because they have not delivered obvious competitive advantages in attracting or retaining users.

There are nine states—Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas, and Virginia—that have adopted more stringent consent rules than

[9] Disney+, "How to opt out of data sharing for the Disney+, Hulu, Max Bundle," https://help.disneyplus.com/article/disneyplus-en-us-data-sharing (accessed 10 Apr. 2025).

California for sensitive data processing that are similar to the GDPR's. The Colorado Privacy Act (CPA) rules, for example, requires valid consent to be clear and affirmative, freely given, specific, informed and unambiguous, meaning it must involve a clear action indicating acceptance, and be revocable without penalty.[10]

FIGURE 7: TIMELINE OF COMPREHENSIVE PRIVACY LAWS ADOPTIONS (THE DATES ON WHICH THE LAW WAS ENACTED AND WHEN IT TOOK EFFECT DIFFER)



There is currently no comprehensive federal privacy law in the U.S. that would unify the approaches to consent across the states, and the effort to regulate privacy remains state-driven. The American Data Privacy Protection Act (ADPPA), proposed in 2022, and the American Privacy Rights Act (APRA), proposed in 2024, are the most significant efforts to regulate privacy at the national level to date.[11, 12] These proposed bills aimed to standardize consent mechanisms across the U.S. by drawing from existing frameworks while tailoring their approaches to protect sensitive data more effectively.

The ADPPA introduced a hybrid approach, combining aspects of both opt-in and opt-out consent depending on data. Sensitive data, such as health, biometric, or financial information, requires affirmative express consent, while non-sensitive data might still operate under an opt-out framework. APRA emphasized an affirmative express consent model for sensitive data collection, similar to the GDPR's. This was an attempt to balance between the privacy rights of consumers and the use of data for innovation. Both bills also proposed that the Federal Trade Commission (FTC) should be empowered to establish a centralized opt-out mechanism, which would allow individuals to opt out of all data transfers covered by the regulations.

10 Colorado Privacy Act Rules, 4 Colo. Code Regs. § 904-3 (2023).

11 American Data Privacy Protection Act, H.R. 8152, 117th Cong. (2022).

12 American Privacy Rights Act, S. 117th Cong. (2024).

PART 3

USER EXPERIENCE AND ATTITUDES TOWARD PRIVACY

To fully assess the impact of data privacy regulations, researchers have analyzed user experience across multiple studies. Early academic research of privacy regulations pointed to potential issues of user comprehension of privacy settings. Neil Richards and Woodrow Hartzog in their 2019 article for *Washington University Law Review* argue that digital consent often fails to meet the "knowing and voluntary" standard—that is, a fully informed and uncoerced agreement—reducing it in practice to a superficial formality.[13] A 2015 study led by Joseph Turow at the University of Pennsylvania, with a sample of 1,506 Americans, found that many users do not fully comprehend privacy policies because they falsely believe the law offers stronger protections than it does—such as assuming companies need permission to share data—and because they feel resigned to constant surveillance, believing they have little power to opt out.[14]

[13] Neil M. Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Washington University Law Review* 96, no. 6 (2019). 1461–1476. https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview (accessed 10 Apr. 2025).

[14] Joseph Turow, Michael Hennessy, and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Annenberg School for Communication, University of Pennsylvania, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060 (accessed 10 Apr. 2025).

Such findings prompted early regulatory efforts focused on protecting consumer rights through explicit opt-in mechanisms. This approach aligns closely with the European model of data protection that is prominent in the GDPR. However, to this day there is no research that in any way affirms opt-in mechanisms alone effectively enhance users' understanding of privacy policies.

One 2020 study found that persuasive rather than purely informative language significantly increases opt-in rates, which means that subtle changes in wording can substantially influence user behavior.

A few studies have criticized design choices that could alter what choices consumers make. Daniel Solove's 2023 study of frequent consent prompts published in the *Boston University Law Review* shows that these prompts lead to habituation, ultimately causing users to disengage and accept terms without fully understanding their implications.[15] One 2020 study found that persuasive rather than purely informative language significantly increases opt-in rates, which means that subtle changes in wording can substantially influence user behavior.[16] Another 2020 study by researchers from Denmark, the U.S., and the U.K. revealed that many Consent Management Platforms (CMPs) intentionally use designs that make refusing consent substantially more challenging compared to acceptance. For example, the removal of easily accessible opt-out options from initial consent screens notably increases acceptance rates, while providing more granular details upfront reduce them.[17] Additionally, a 2019 meta-study by Princeton researchers found that certain interface strategies—such as prominently highlighting preferred choices or repeatedly

15 Daniel Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law," George Washington University Law School, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743 (accessed 10 Apr. 2025).

16 Caterina D'Assergio, Puneet Manchanda, Elisa Montaguti, and Sara Valentini, "The Race for Data: Utilizing Informative or Persuasive Cues to Gain Opt-in?" Working paper, 17 October 2022. www.ssrn.com/abstract=4250389 (accessed 10 Apr. 2025).

17 Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence." In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321 (accessed 10 Apr. 2025).

prompting users to decide—can steer users' choices or limit their understanding, potentially undermining truly informed consent.[18]

These design issues are not unique to the digital consent context. In fact, they closely mirror challenges observed historically in traditional marketing. Persuasive techniques employed through advertising, packaging, or product placement have long influenced consumer decision-making—sometimes causing consumers to accept terms or conditions without fully evaluating their implications.[19, 20] Thus, it remains unclear whether the issues related to digital consent differ fundamentally from those encountered in online and offline marketplaces, where design and marketing regularly influence consumer behavior.

Persuasive techniques employed through advertising, packaging, or product placement have long influenced consumer decision-making—sometimes causing consumers to accept terms or conditions without fully evaluating their implications.

Are there alternative explanations of user behavior described in these findings? While researchers observe behavioral changes that they interpret as fatigue or lack of comprehension, it could be the case that the user is just displaying a lack of concern about sharing certain types of data. However, researchers do not consider this alternative explanation, which opens up a possibility for different explanations of the result that we will discuss below.

In a survey environment there is some indication that Americans claim that they care about privacy. For example, Pew Research findings suggest a growing concern among

18 Arunesh Mathur, Jonathan Mayer, "What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. https://ar5iv.labs.arxiv.org/html/2101.04843 (accessed 10 Apr. 2025).

19 Paurav Shukla, "The influence of creative packaging design on customer motivation to process and purchase decisions," *Journal of Business Research* vol. 147, August 2022, https://bit.ly/3H4yfo8 (accessed 10 Apr. 2025).

20 Annye Braca, "Developing Persuasive Systems For Marketing: The Interplay Of Persuasion Techniques, Customer Traits And Persuasive Message Design," *Italian Journal of Marketing,* August 2023, https://link.springer.com/article/10.1007/s43039-023-00077-0 (Accessed 10 Apr. 2025).

respondents about how their personal data is used, showing a notable increase from 64% in 2019 to 71% in 2023.[21] However, this survey does not ask participants to consider the costs involved in implementing privacy protections. In real-life scenarios, protecting privacy comes with tangible costs, such as the time and effort required to adjust privacy settings. When faced with these costs, individuals may choose not to invest the necessary effort.[22] Consequently, revealed preferences for privacy are substantially weaker than stated preferences reported in surveys.

> *… revealed preferences for privacy are substantially weaker than stated preferences reported in surveys.*

Within the digital environment, users are facing multiple notices and pop-ups and as a result adopt practical heuristics.[23, 24] This behavior may reflect not only cognitive fatigue, but also a general lack of sustained concern about the routine collection of certain types of personal data. For many individuals, adjusting privacy settings across every platform is perceived as time-consuming and unnecessary—particularly when the perceived risks are low. For example, according to Pew Research, most Americans click "agree" without reading the content of the notice.[25] A strict opt-in system assumes everyone cares about all their data, all the time. But what we observe is a more selective concern: People care about

21 Michelle Faverio, "Key findings about Americans and data privacy," Pew Research Center, October 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ (accessed 10 Apr. 2025).

22 Hanbyul Choi, "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior Vol. 81,* April 2018, https://www.Sciencedirect.Com/Science/Article/Pii/S0747563217306817 (Accessed 10 Apr. 2025).

23 Brooke E. Auxier, "Americans And Privacy: Concerned, Confused And Feeling Lack Of Control Over Their Personal Information," Pew Research Center, November 2019, https://www.Pewresearch.Org/Internet/2019/11/15/Americans-Attitudes-And-Experiences-With-Privacy-Policies-And-Laws (Accessed 10 Apr. 2025).

24 Daphne Fernanda F. B. De Carvalho, "Evaluating Cognitive Privacy Heuristics That Influence Facebook Users Data Disclosure," *Journal of Internet Services and Applications*, December 2022, https://www.Researchgate.Net/Publication/367197342_Evaluating_Cognitive_Privacy_Heuristics_That_Influence_Facebook_Users_Data_Disclosure (Accessed 10 Apr. 2025).

25 Colleen McClain, "How Americans View Data Privacy," Pew Research Center, October 2023, https://www.Pewresearch.Org/Internet/2023/10/18/How-Americans-View-Data-Privacy (Accessed 10 Apr. 2025).

some data some of the time. In many cases, user inaction in response to consent prompts is not solely a result of "consent fatigue," but rather suggests a more selective approach to privacy—where concern varies based on context, perceived sensitivity, and individual risk assessment.[26]

For example, when presented with the opportunity to opt out of targeted advertising through the Ad Choices program—a self-regulatory initiative by the digital advertising industry that allows users to manage their ad preferences—only 0.23% of ad impressions resulted in user action, suggesting that the overwhelming majority either accepted the default or did not find it worth the effort to opt out.[27] In practice, opt-out defaults leverage this behavior by keeping privacy on "autopilot" for the majority of cases, yet still giving individuals the flexibility to step in and protect their data when it truly matters to them. This behavioral insight helps explain why even in competitive markets, companies rarely adopt a strict opt-in approach voluntarily. Opt-out defaults are not just a business strategy—they are often a better fit with consumer psychology.

Opt-out defaults are not just a business strategy—they are often a better fit with consumer psychology.

Neither opt-in nor opt-out are entirely universal solutions. Strict opt-in approaches could work but at a substantial cost to data-driven business models that rely heavily on user tracking. Opt-out solutions may be more practical for businesses seeking to preserve access to valuable data streams, given that many users don't proactively opt out. Each approach introduces distinct trade-offs: Strict opt-in can significantly reduce user engagement with targeted ads, while opt-out may lead to lower consumer understanding of privacy implications. Simplifying consent prompts also involves trade-offs, potentially limiting users' control over their data, but offering greater clarity and convenience.

[26] Long Chen, Patrick Bolton, and Bengt R. Holmström, "Understanding Big Data: Data Calculus in the Digital Era," Rotman School of Management Working Paper No. 3791018, Columbia Business School Research Paper, February 25, 2021, https://ssrn.com/abstract=3791018 (accessed 10 Apr. 2025).

[27] Garret Johnson, Scott Shriver, Shaoyin Dun, "Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?," *Marketing Science* (39:1), pp. 33-5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020503 (accessed 10 Apr. 2025).

> *Younger generations, including Millennials and Gen Z that are now between the ages or 13 and 44, show diminishing concerns about traditional notions of privacy, which is reflected in the greater amount of personal information they willingly share online.*

There is another important caveat regarding user behavior that policymakers should consider: Attitudes towards privacy are evolving. Younger generations, including Millennials and Gen Z that are now between the ages or 13 and 44, show diminishing concerns about traditional notions of privacy, which is reflected in the greater amount of personal information they willingly share online, particularly on public social media profiles and platforms that offer personalized experiences in exchange for data.[28] However, these generations remain highly concerned about data security and self-directed control over sensitive information. Rather than depending solely on privacy tools provided by platforms, they are more inclined to proactively use technologies such as VPNs, encrypted messaging apps, and other user-driven privacy-preserving measures.[29] These trends indicate that data security and personal control may become more central to privacy in the future. Policymakers should therefore consider that newer generations of users are likely to prefer managing their privacy through technologies they actively choose and control, rather than relying on default platform-provided options.

[28] Chris DeBrusk and Ana Kreacic, "How Gen Z Uses Social Media Is Causing A Data Privacy Paradox," Oliver Wyman Forum, August 23, 2023 https://www.oliverwymanforum.com/gen-z/2023/aug/how-gen-z-uses-social-media-is-causing-a-data-privacy-paradox.html and Sara Karlovitch, "Gen Z is more likely to be OK with targeted ads — here's what the numbers say," Marketing Dive, August 25, 2023, https://www.marketingdive.com/news/allow-tracking-younger-consumers-more-likely-okay-with-target/691452/ (accessed 10 Apr. 2025).

[29] Jason Oeltjen, "What leaders need to know about generational privacy preferences," *Security Magazine,* January 7, 2025 https://www.securitymagazine.com/articles/101274-what-leaders-need-to-know-about-generational-privacy-preferences (accessed 10 Apr. 2025).

PART 4

IMPACT ON INDUSTRY

4.1 FAVORING LARGER FIRMS AND LIMITING COMPETITION

Privacy laws based both on opt-in and opt-out consent frameworks can disadvantage smaller firms relative to larger ones, including innovative but small startups. According to a report from the Regulatory Studies Center at George Washington University, GDPR's opt-in provisions have especially burdened smaller firms, which face higher compliance costs and lower user engagement because of consent requirements.[30] In the United States, the growing patchwork of state laws has raised compliance costs. Startups already spend hundreds of thousands to comply, and each additional state law adds $15,000–$60,000 in costs, according to a 2023 industry report.[31]

For small companies, obtaining explicit consent imposes additional transaction costs that they may struggle to absorb, limiting their capacity to gather data for targeted services and advertising. Meanwhile, larger platforms can absorb these costs easier, leveraging their

30 Aryamala Prasad, "Unintended Consequences of GDPR: A Two-Year Lookback," Regulatory Studies Center, George Washington University, 3 Sept. 2020. www.regulatorystudies.columbian.gwu.edu/unintended-consequences-gdpr (accessed 10 Apr. 2025).

31 Report, "Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups," Engine, March 2023, https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf, as well as: Nathan Lindfors, "The American Privacy Rights Act and What It Means for Startups," Engine, April 11, 2024, https://www.engine.is/news/category/the-american-privacy-rights-act-and-what-it-means-for-startups (accessed 10 Apr. 2025).

resources to consolidate user data across multiple services without repeated consent. Companies like Google and Facebook, which benefit from expansive service ecosystems, can capture comprehensive consumer profiles under GDPR, further strengthening their competitive advantage.[32]

Companies like Google and Facebook, which benefit from expansive service ecosystems, can capture comprehensive consumer profiles under GDPR, further strengthening their competitive advantage.

Explicit consent affects firms of all sizes, because without explicit consent businesses can no longer track user behavior across websites or share data with third parties. Studies show that requiring explicit consent deters users from engaging on websites, either by increasing their awareness of data policies or disrupting the online experience.[33, 34, 35]

Large companies like Google have leveraged GDPR provisions by unifying privacy notices across products, allowing seamless data flow between services.[36] This is because GDPR permits internal data sharing once an initial consent is obtained. This approach lets Google create a comprehensive user profile that bolsters their market dominance, while smaller firms—restricted by the need for separate, specific consents—struggle to compete. External

32 James Campbell, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," *Journal of Economics & Management Strategy 24* (2015). https://onlinelibrary.wiley.com/doi/abs/10.1111/jems.12079 (accessed 10 Apr. 2025).

33 Caterina D'Assergio, Puneet Manchanda, Elisa Montaguti, and Sara Valentini, "The Race for Data: Utilizing Informative or Persuasive Cues to Gain Opt-in?" Working paper, 17 October 2022. www.ssrn.com/abstract=4250389 (accessed 10 Apr. 2025).

34 Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence." In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321 (accessed 10 Apr. 2025).

35 Arunesh Mathur, Jonathan Mayer, "What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. https://ar5iv.labs.arxiv.org/html/2101.04843 (accessed 10 Apr. 2025).

36 Damien Geradin, Theano Karanikioti, and Dimitrios Katsifis, "GDPR Myopia: How a Well-Intended Regulation Ended Up Favoring Google in Ad Tech," TILEC Discussion Paper No. 2020-012, May 11, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130 (accessed 10 Apr. 2025).

data sharing, by contrast, remains tightly regulated, requiring specific consent and additional monitoring to ensure compliance, adding further hurdles for smaller firms attempting to compete in data-driven markets.

> *This disparity in data access and consent compliance has reinforced the advantages of larger firms, creating what some researchers call "selective consent."*

This disparity in data access and consent compliance has reinforced the advantages of larger firms, creating what some researchers call "selective consent." Guy Aridor, Yeon-Koo Che, and Tobias Salz found that consumers are more likely to provide consent to websites they trust and frequently use, which tend to be larger, well-established platforms.[37] Smaller or newer firms, which consumers interact with less frequently, face higher opt-out rates and thus collect less data. This selective consent behavior reinforces the dominance of larger platforms, making it increasingly difficult for smaller companies to compete as effectively.

Research by James Campbell et al. reveals that consumers are generally more comfortable sharing data with companies they recognize, granting these firms an edge in capturing user consent.[38] This trust allows big companies to accumulate more data, thereby reinforcing their dominance, while smaller firms face greater difficulty in building similar levels of consumer trust.

Larger firms have also demonstrated an ability to turn consent requirements into business gains. A study by Miguel Godinho de Matos and Idris Adjerid illustrates how a major European telecommunications company (TELCO, short for Telecommunications Company) leveraged GDPR compliance for competitive advantage, expanding its customer base

[37] Guy Aridor & Yeon-Koo Che & Tobias Salz, 2023. "The effect of privacy regulation on the data industry: empirical evidence from GDPR," *The RAND Journal of Economics*, vol 54(4), pages 695-730. https://www.nber.org/papers/w26900 (accessed 10 Apr. 2025).

[38] James Campbell, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," MIT Initiative on the Digital Economy, 2015, http://dx.doi.org/10.2139/ssrn.1729405 (accessed 10 Apr. 2025).

through a "permissioning" campaign designed to secure renewed customer consent.[39] This campaign enabled the firm to broaden its marketing reach and ultimately increase revenue, underscoring how larger firms can use regulatory constraints to their advantage.

> *… when privacy is made as convenient as a single tap, users will take it. But this opt-out wave forced advertising platforms to overhaul their targeting strategies and led to billions in lost ad revenue.*

Another illustration of these dynamics is Apple's implementation of App Tracking Transparency (ATT). In 2022, rather than bombarding users with intricate consent forms for each app, Apple forced a simple yes/no prompt for cross-app tracking permission on iOS. Only about 25% of users consented to tracking, leaving roughly 75% effectively "opted out."[40] This extremely significant opt-out shows that when privacy is made as convenient as a single tap, users will take it. But this opt-out wave forced advertising platforms to overhaul their targeting strategies and led to billions in lost ad revenue. The immediate outcome was a major blow to the personalized advertising ecosystem. Facebook/Meta estimated that Apple's change would cost the social media platform about $10 billion in ad revenue for 2022.[41] Other platforms dependent on third-party tracking (Snapchat, YouTube, etc.) saw similar hits, with one report finding social media companies collectively lost around $10 billion in the wake of the implementation of ATT.[42]

39 Miguel Godinho de Matos and Idris Adjerid, "Consumer Consent and Firm Targeting after GDPR: The Case of a Large Telecom Provider," (July 31, 2019). *Management Science* 2019, https://ssrn.com/abstract=3777417 or http://dx.doi.org/10.2139/ssrn.3777417 (accessed 10 Apr. 2025).

40 "Report: Apple's ATT opt-in rates at 25% overall," IAPP, 6 May 2022, https://iapp.org/news/b/report-att-opt-in-rates-at-25-overall# (accessed 10 Apr. 2025).

41 Kif Leswing, "Facebook Says Apple iOS Privacy Change Will Result in $10 Billion Revenue Hit This Year," CNBC, Feb. 2, 2022 https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html#:~:text=Facebook%20says%20Apple%20iOS%20privacy,sales%20by%20about%20%2410%20billion (accessed 10 Apr. 2025).

42 Emma Roth, "Apple's App Tracking Policy Reportedly Cost Social Media Platforms Nearly $10 Billion: Snapchat, Facebook, Twitter, and YouTube All Took a Hit," The Verge, Oct. 31, 2021, https://www.theverge.com/2021/10/31/22756135/apple-app-tracking-transparency-policy-snapchat-facebook-twitter-youtube-lose-10-billion# (accessed 10 Apr. 2025).

Meanwhile, players that did not rely on invasive tracking—notably Apple itself, with its own ad network and massive collection of first-party data—were relatively advantaged. Businesses that were not dependent on tracking grew even more powerful as those that were had to rethink their strategies.[43]

In effect, Apple's opt-in regime rebalanced the digital ad market: It hurt the bottom line of ad-driven firms and arguably strengthened Apple's competitive position (a point not lost on regulators, as seen by a French competition authority fine over ATT's implementation).[44]

"In effect, Apple's opt-in regime rebalanced the digital ad market: It hurt the bottom line of ad-driven firms and arguably strengthened Apple's competitive position..."

Apple did not see users leave its platform—iPhone sales and use continued to grow, showing that stricter privacy didn't repel consumers (it may have enhanced Apple's reputation instead). And while some smaller app developers initially feared they'd be ruined by loss of ad revenue, the ecosystem adjusted. A comprehensive study of App Store data found that after an initial dip, the number of apps on iOS quickly recovered and developers did not broadly exit the market post-ATT.[45] Developers shifted to other monetization methods (more in-app purchases, subscriptions, using Apple's payment systems or contextual ads) rather than abandoning the platform.

[43] Sara Morrison, "The Winners and Losers of Apple's Anti-Tracking Feature: Apple's Big Privacy Update Came Out a Year Ago. What Did It Do for You?" Vox, April 29, 2022, https://www.vox.com/recode/23045136/apple-app-tracking-transparency-privacy-ads# (accessed 10 Apr. 2025).

[44] Florence Loeve, "Apple Hit with $162 Million French Antitrust Fine Over Privacy Tool," *Reuters*, March 31, 2025, https://www.Reuters.Com/Technology/French-Antitrust-Regulator-Fines-Apple-150-Million-Euros-Over-Privacy-Tool-2025-03-31/ (Accessed 10 Apr. 2025).

[45] Cristobal Cheyre, Benjamin T. Leyden, "Did Apple's App Tracking Transparency Framework Harm the App Ecosystem?" July 1, 2024, SSRN (Social Science Research Network), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4453463#:~:text=ecosystem%20create%20new%20apps%2C%20update,SDK (accessed 10 Apr. 2025).

The Apple example demonstrates that an opt-in approach can succeed for established businesses that have sufficient market power to set their own rules and, in certain cases, enhance the user experience. Apple occupied a unique position because its business model depended heavily on its proprietary ad network and extensive first-party data. Additionally, Apple's move served as an effective marketing strategy, allowing the company to showcase itself to users as highly privacy friendly. However, this approach might not have worked as effectively for smaller firms or competitors—a point explored further in the next section.

4.2 TECHNICAL CHALLENGES OF CONSENT MANAGEMENT

Consent implementation can be difficult from a technical standpoint, requiring a large upfront investment and reworking of current tools. According to a study by the University of California, Berkeley, the initial cost of complying with the California Consumer Privacy Act (CCPA) was estimated to be around $55 billion for businesses in the state—roughly 1.8% of California's GDP.[46] Maintaining GDPR compliance is not a one-time investment; according to a global survey, 88% of global companies surveyed by PWC spend more than $1 million yearly, with 40% spending more than $10 million.[47]

> *Consent tracking was not initially considered when building traditional IT infrastructure, such as electronic health record systems that are widely used in healthcare.*

Companies that employ Consent Management Platforms (CMPs), software tools that help websites collect and manage user consent for processing personal data, have several technical difficulties, particularly when integrating them with older IT systems. Consent tracking was not initially considered when building traditional IT infrastructure, such as

[46] Association of National Advertisers, "California Estimates $55 Billion Initial Cost for State Businesses to Comply with New Data Privacy Law," Sept. 2019, https://www.Ana.Net/Content/Show/Id/Pr-New-Law-Cost#:~:Text=The%20report%20estimates%20the%20initial,Be%20covered%20by%20the%20ccpa (Accessed 10 Apr. 2025).

[47] PwC, "Privacy Reset: from compliance to trust-building," (2021) https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html (accessed 10 Apr. 2025).

electronic health record systems that are widely used in healthcare.[48] Consent data frequently becomes dispersed among healthcare systems as a result of the growing use of analytics software, patient engagement platforms, and customer relationship management (CRM) tools by healthcare providers for outreach, education, and individualized care.[49] This fragmentation makes it more difficult to consistently apply consent preferences and calls for intricate, frequently manual integration efforts.

Another significant challenge is adapting CMPs to comply with multiple jurisdictional privacy laws simultaneously. Early CMP solutions were often narrowly tailored to GDPR requirements and struggled to integrate new models, such as California's opt-out provisions under CPRA, including the "Do Not Sell My Info" link and browser signals like the Global Privacy Control (GPC). Organizations now frequently employ geo-specific consent interfaces to manage these differing standards. For example, an EU-based user might encounter detailed GDPR consent banners, whereas a Californian user sees simplified opt-out notices tailored for CPRA compliance. The task of dynamically delivering correct consent notices based on user location is technically intricate, because it requires advanced geolocation detection and flexible interface designs.[50]

> *The technical challenges of consent management don't end after implementation—they require constant attention.*

The technical challenges of consent management don't end after implementation—they require constant attention. Companies must continuously monitor and document users' consent choices, keeping detailed records of what each person agreed to, when they agreed to it, and how their data is allowed to be used. These records must be accurate and readily accessible in case regulators or users request them. On top of that, businesses are responsible for making sure that all third-party partners—such as advertisers, analytics

48 R S Evans, "Electronic Health Records: Then, Now, And In The Future," *Yearbook Of Medical Informatics 2016*, https://Pmc.Ncbi.Nlm.Nih.Gov/Articles/Pmc5171496/ (Accessed 10 Apr. 2025).

49 Iman Kassam, Daria Ilkina, Jessica Kemp, "Patient Perspectives And Preferences For Consent In The Digital Health Context: State-Of-The-Art Literature Review," *Journal Of Medical Internet Research.* 2023 Feb, https://Pmc.Ncbi.Nlm.Nih.Gov/Articles/Pmc9960046 (Accessed 10 Apr. 2025).

50 UC Berkeley CLTC, "Comparing Effects of and Responses to the GDPR and CCPA/CPRA."

providers, or data processors—follow these same rules. This makes managing vendors far more complex and increases the risk of legal liability.

Internally, implementing CMPs demands significant cultural and organizational shifts. Developers and product teams must embed privacy considerations into the early stages of development processes—a concept known as "Privacy by Design." However, research indicates developers often treat privacy compliance as a lower-priority task, leading to inconsistent quality in implementation and heightened risk of regulatory noncompliance.[51]

As Congress considers imposing a national comprehensive privacy law with an imposed mechanism of consent, technical challenges involving consent roll-out need to be re-examined.

4.3 IMPACT ON INNOVATION AND PRODUCT DEVELOPMENT

Beyond immediate compliance and operational challenges, consent requirements under privacy laws pose long-term impacts on innovation, particularly for data-reliant industries like artificial intelligence.

Avi Goldfarb and Catherine Tucker suggest that restrictions on data flow can slow down the development of new technologies, as data access is critical to refining algorithms and advancing artificial intelligence.[52] This is because these regulations can inadvertently impede the ability of companies to drive innovation by limiting access to necessary datasets.

> *“Studies highlight how compliance costs—from implementing consent management to reengineering business processes—place a disproportionate burden on smaller firms.”*

[51] Ibid.

[52] Avi Goldfarb and Catherine Tucker, “Privacy and Innovation,” Rotman School of Management, University of Toronto; MIT Sloan School of Management; 2012 https://www.journals.uchicago.edu/doi/full/10.1086/663156 (accessed 10 Apr. 2025).

For startups and SMEs, these requirements are even more challenging. Studies highlight how compliance costs—from implementing consent management to reengineering business processes—place a disproportionate burden on smaller firms.

However, some businesses are using these regulations as a catalyst for privacy-enhancing technologies (PETs) and privacy-preserving machine-learning solutions.[53] These technologies enable companies to meet compliance demands while still driving innovation, showing how regulatory challenges can sometimes inspire creative solutions. For instance, Apple has integrated differential privacy into its Photos app to analyze user behavior without collecting personally identifiable data, thereby enhancing features like Memories while preserving user privacy.[54]

[53] Reza Shokri and Vitaly Shmatikov, "Privacy-Preserving Deep Learning," in Proceedings of the 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton) (September 2015), https://www.researchgate.net/publication/319769902_Privacy-preserving_deep_learning (accessed 10 Apr. 2025).

[54] Apple Website, "Understanding Aggregate Trends For Apple Intelligence Using Differential Privacy," April 2025, https://Machinelearning.Apple.Com/Research/Differential-Privacy-Aggregate-Trends?Utm.Com (Accessed 1 May 2025).

PART 5

POLICY RECOMMENDATIONS

Current evidence on user behavior suggests that neither opt-in nor opt-out approaches are universally effective or reflective of actual consumer preferences. Policymakers should recognize that user comprehension, ease of use, selective concern, and evolving attitudes towards privacy and data security all play key roles in shaping user responses. The complex interaction between design, defaults, user psychology, and market dynamics highlighted here suggests the need for flexible, nuanced privacy regulations that would balance consumer autonomy and practical business needs.

“Current evidence on user behavior suggests that neither opt-in nor opt-out approaches are universally effective or reflective of actual consumer preferences.”

Despite their different methods, both opt-in and opt-out approaches cause challenges such as consent fatigue, design flaws, and the over-reliance on default settings that can undermine the user’s ability to make a fully informed choice. While the opt-in method aims

to enhance user control and trust by requiring a deliberate act of consent, its complexity can result in lower engagement and higher compliance costs—issues that disproportionately affect smaller businesses. The opt-out approach, though simpler for users, may inadvertently favor larger firms that can optimize their interfaces and leverage default settings to maintain data collection with minimal user intervention. Both frameworks, therefore, expose a tension between ensuring genuine informed consent and creating environments that are both user-friendly and enhance privacy.

Drawing on academic research, policy white papers, and emerging industry practices, we propose a framework that aims to make consent mechanisms more practical.

In some sectors, like healthcare and traditional marketing, consent is collected through a single, well-structured process rather than through constant, disruptive pop-ups. These systems are designed to obtain informed agreement efficiently by accounting for the type of data being collected, how often it's collected, and the potential risks involved.

> *Low-risk data—such as non-identifying or publicly available information used for essential services—could require only a one-time or simplified consent.*

Policymakers could adopt a similar model online by defining clear categories of data. This could look like a tiered consent system where data is classified into levels of risk and sensitivity, and consent processes are matched accordingly. Low-risk data—such as non-identifying or publicly available information used for essential services—could require only a one-time or simplified consent. In contrast, sensitive data—such as biometric, geolocation, health, or financial information, particularly involving minors—would trigger more detailed and explicit consent. Drawing from how other industries handle this balance can help digital privacy rules protect users without overwhelming them—ensuring both autonomy and ease of use.

To support this system in practice, policymakers should also encourage the development of universal privacy management tools—such as a dedicated privacy app or browser extension—that allow users to send a single, system-wide opt-out signal to every website

and app they interact with. While some browsers already incorporate privacy features like a "Do Not Track" function, these tools are often underused or not fully integrated into everyday user workflows. A universal tool would consolidate disparate privacy settings into one intuitive interface, reducing the cognitive load on users who currently face a barrage of pop-ups and fragmented consent requests. By automating the process of opting out of data collection across platforms, such a tool could enhance consumer control, streamline the consent process, and serve as a practical benchmark for ethical data practices—offering valuable insights before policymakers consider additional regulatory measures. Policymakers, therefore, should avoid imposing rules or restrictions that could inadvertently hinder the market-driven development and adoption of these innovative privacy solutions.

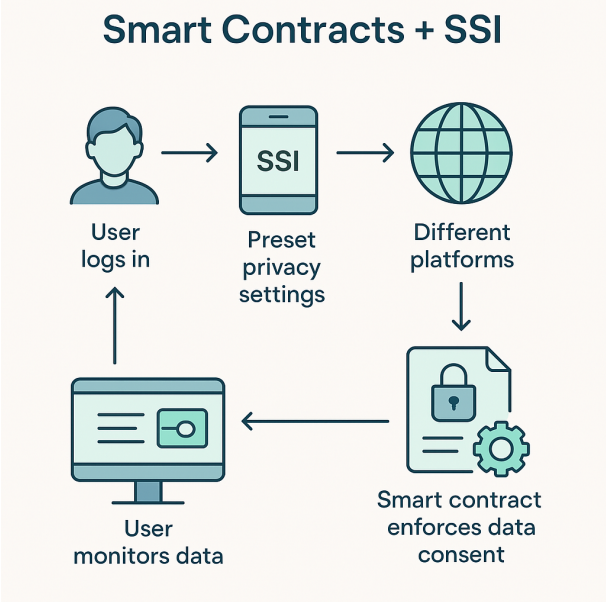
Rather than relying solely on regulatory mandates for every detail, policymakers should encourage and endorse voluntary industry standards that improve privacy in user-friendly ways. For example, policymakers could support the adoption of browser-based universal opt-out signals (like Global Privacy Control) as a standard mechanism for consumer choice online. GPC emerged from a collaboration of privacy tech and browser vendors, and by July 2024 it was recognized in several state privacy laws as a legitimate opt-out mechanism.

One promising approach is the use of federated identity systems—where a single login and set of privacy settings follow the user across different websites and apps.

Policymakers should also explore tools that let users set their privacy preferences once and have them automatically respected across the internet. One promising approach is the use of federated identity systems—where a single login and set of privacy settings follow the user across different websites and apps. This would reduce the need for repetitive consent pop-ups and make privacy protection more seamless. A more advanced version of this idea is Self-Sovereign Identity (SSI). With SSI, users would control their own digital identity and privacy settings, and decide who gets access to what. Imagine signing up for a new app and having your pre-set choices—like "do not share my data"—applied instantly, without having to go through another settings menu. To make this work, government and industry could collaborate on interoperability standards to ensure that different services recognize and honor these settings. Certification systems could help prevent misuse and build trust. In the

future, even smart contracts could be used to enforce privacy terms—automatically deleting your data after a set period or limiting its use to a specific purpose. These tools would reduce the need to rely on company promises and shift more control to users.

FIGURE 8: SMART CONTRACTS AND SELF SOVEREIGNTY IDENTITY (SSI)



To support adoption of flexible, user-centric privacy tools such as universal opt-out mechanisms and tiered consent frameworks, policymakers should pursue a co-regulatory model that would allow industry alliances take the lead in developing voluntary privacy accountability codes that could later be approved by the designated authority such as FTC.

For example, an alliance of social media platforms could create an accountability code for personalized advertising that would require participating companies to implement intuitive and user-friendly consent mechanisms, consistently honor universal opt-out signals, and undergo annual independent privacy audits. To encourage broad industry participation, policymakers should structure incentives such as a presumption of regulatory compliance or reduced enforcement penalties for companies adhering to FTC-approved codes. This would give companies flexibility to build practical, privacy-preserving solutions without rigid regulatory mandates, while ensuring consumer protections remain robust.

However, the Supreme Court's recent *Loper Bright* decision ended judicial deference to agencies interpreting ambiguous statutes.[55] This means that without explicit legislative authorization, the FTC currently lacks the firm legal basis required to formally approve or enforce voluntary industry codes. Therefore, Congress needs to explicitly grant the FTC authority to review, approve, and oversee industry-led privacy accountability frameworks beyond existing narrow applications (such as the COPPA Safe Harbor).

[55] *Loper Bright Enterprises, Inc. v. Raimondo*, 603 U.S. __ (2024), https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf (accessed 10 Apr. 2025).

> *…Congress needs to explicitly grant the FTC authority to review, approve, and oversee industry-led privacy accountability frameworks beyond existing narrow applications…*

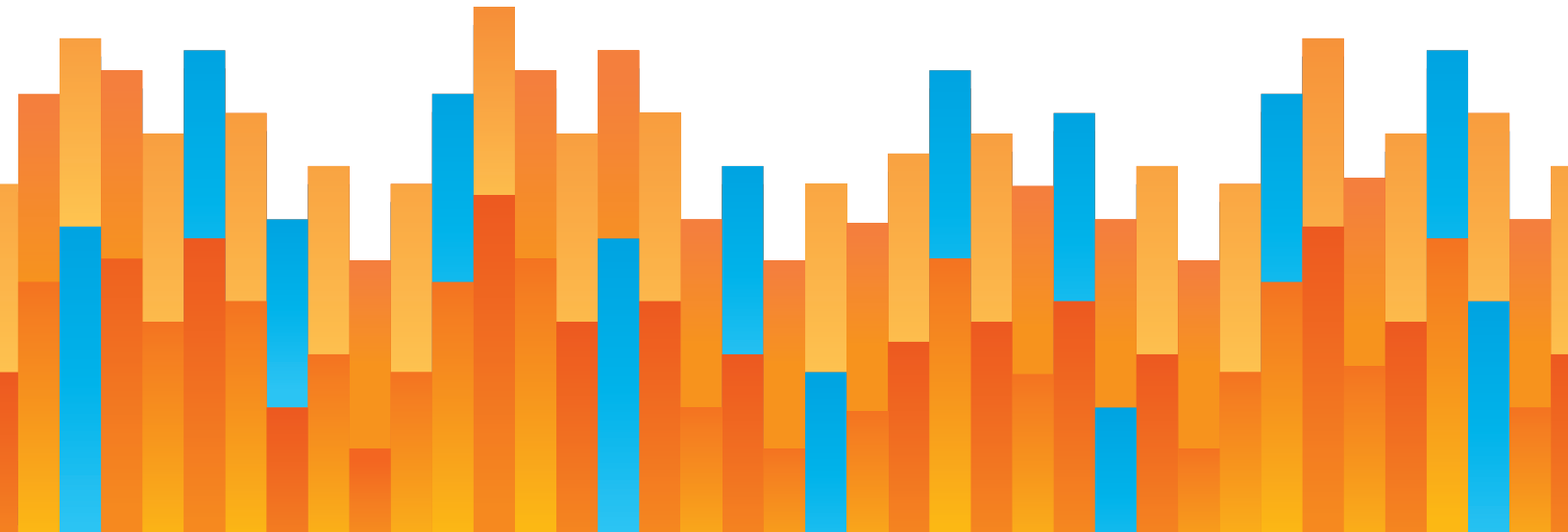
Regulators and industry both should pivot to an outcomes-based approach for privacy. The ultimate goal is to protect consumers from harmful data practices (discrimination, unwanted surveillance, breaches, etc.) and preserve their autonomy. Consent is a means to that end, not an end in itself. Policies should thus measure success not by "how many consent boxes were checked" but by concrete outcomes—e.g. reductions in inappropriate data uses, high rates of consumer satisfaction with privacy experiences. This might mean simplifying consent in some areas and strengthening enforcement in others. For low-risk data uses, lengthy consent banners could be replaced with contextual disclosures or implied consent coupled with strong user control (let users change settings at any time). For high-risk uses (such as sensitive data, children's data, or profiling), regulators could require privacy-by-design measures in addition to initial consent—for instance, if an app accesses a user's location, the operating system could periodically prompt the user to reconfirm permission or display contextual reminders such as, "You haven't used this app in a while; do you still want it to track your location?" These periodic reminders, guided by policy but implemented at the platform level, may be more effective than a single consent that users may eventually forget.

ABOUT THE AUTHORS

Jen Sidorova is a policy analyst at Reason Foundation. Her areas of expertise include technology policy, pension reform, recruitment and retention of public sector employees, and housing regulation.

Jen's recent academic work has been presented at panels at the 45th Association for Public Policy Analysis and Management (APPAM) Fall Research Conference, the 2024 Workshop on the Economics of Information Security (WEIS), as well as the International Studies Association (ISA) 2024 Annual Convention and 2025 Midwest Political Science Association (MPSA).

Her recent chapter on "Military cybercapacity: measures, drivers and effects" was published in the *Research Handbook of Cyberwarfare,* published by Edward Elgar Publishing. Her latest film on rent regulation, “Shabbification: The Story of Rent Control," was featured at the 2024 Anthem Film Festival in Las Vegas and is now streamed on CiVL.

Sidorova holds Master of Arts degrees in economics and political science from Stony Brook University. She is an alumnus of the Oskar Morgenstern Fellowship at the Mercatus Center, as well as the Cybersecurity Summer Institute at Georgia Tech.

Nicole Shekhovtsova is a technology policy analyst at Reason Foundation, specializing in privacy, digital assets, and artificial intelligence regulation. She holds a Master of Laws from the George Washington University Law School.