Consumer-Focused Data Privacy: A Public Policy Primer

Tirzah Duren and Isaac Schick

Introduction

In recent efforts to legislate on privacy, regulators seek to protect consumers from unethical or unpopular data practices. However, approaches that cast a wide net of protections result in rules that contradict each other and fail to focus their protections on the consumer. To put the consumer at the center of data privacy, policymakers need to focus on informed consumer consent that covers derived data and implement sectoral policies that avoid the pitfalls of omnibus legislation.

Consumer Costs of Data Privacy Lapses

While data privacy and security are distinct topics — with privacy focused on *what* information is collected and security focused on the *protection* of that information against nefarious actors — the topics overlap in the event of a data breach. The risk of a data breach, in which information is accessed without consent from the owner, integrates the practical side of security with conversations about what types of data should even be collected and put at risk in the first place.

The risk of a data breach is not limited to specific types of companies. Breaches have affected diverse companies such as Nieman Marcus, Marriott, MGM Grand, and LinkedIn.[1] This exposed information can reveal passwords, phone numbers, and other personal identifiable information that allows nefarious actors direct contact with consumers or consumer financial accounts. The permanent nature of data in some of the hacks allows for harm years after the fact in the form of blackmail, which occurred in the Ashley Madison.com breach.[2]

Hacks like these have prompted many Americans to take a more interventionist stance on data protection policy. According to 2021 polling from Pew Research, 75 percent of Americans

[1] Abi Tyas Yunggal, "The 68 Biggest Data Breaches," *UpGuard*, Mar. 2, 2023.

[2] Zak Doffman, "Ashley Madison Hack Returns To 'Haunt' Its Victims: 32 Million Users Now Watch and Wait," *Forbes*, Feb. 1, 2020.

support more data privacy regulation than currently exists.[3] This desire for more oversight is coupled with a lack of understanding about what the current data landscape looks like. In the same study, 59 percent of respondents said they understood very little to nothing about what companies did with their data, and only 6 percent said they actually knew. An even larger majority (81 percent) said the risks of data collection outweighed the benefits — benefits which few respondents seemed to understand.

The amalgamation of privacy and security within the public conscience is shown by some recent legislation, including Europe's General Data Protection Regulation (GDPR).

This legislation has, unfortunately, become a model for implementing "data rights."[4] Comparatively, the United States has already implemented several key pieces of legislation that protect user data without enshrining vague legal rights.

Privacy Overview

The current privacy policy landscape could be characterized by two regulatory approaches, with one being narrow and focusing on specific industries and consumers, and the other approach creating overarching and broad protections through mandates. The U.S. generally focuses on specific industries, such as financial protections through the Securities and Exchange Commission, healthcare through the Health Insurance Portability and Accountability Act (HIPAA),[5] and consumer financial services through the Gramm-Leach-Bliley Act (GLBA).[6]

The U.S. also has the Children's Online Privacy Protection Act (COPPA), which establishes protections for those under 13 years old by requiring businesses targeting youth to obtain parental consent, publicly post data practices, and allow users to view and request the deletion of data.[7]

On the other side of the Atlantic, the European Union (EU) has created what is often viewed as a regulatory standard for data protection. The GDPR is a collection of certain "rights" that EU consumers have over their data privacy. These include the "right to be forgotten," the right to object to certain uses of data including profiling, the right to rectification of incomplete or incorrect data, the right of portability or the ability to transfer data from one company to another, and the right of access to know how data are being processed.

The GDPR model is being exported to other jurisdictions looking to implement

[3] Brooke Auxier and Lee Rainie, "Key takeaways on Americans' views about privacy, surveillance and data-sharing," *Pew Research Center*, Nov. 15, 2019.
[4] "General Data Protection Regulation," *Intersoft Consulting*, European Parliament and Council, Apr. 27, 2016.
[5] Congress.gov. "Text - H.R.3103 - 104th Congress (1995-1996): Health Insurance Portability and Accountability Act of 1996." August 21, 1996.
[6] Congress.gov. "S.900 - 106th Congress (1999-2000): Gramm-Leach-Bliley Act." November 12, 1999.
[7] ftc.gov. "Children's Online Privacy Protection Rule ('COPPA')," January 17, 2013.

sweeping data reforms. California has already passed the California Consumer Privacy Act (CCPA), which uses similar rights-based and overarching policy approaches.[8] Other states have followed suit. Because the GDPR model has already proven extremely costly for the Europeans, its use among states will likely impose similar costs as more jurisdictions implement their own versions.

Cost of Current Landscape

Because implementation of these laws among the states creates a patchwork of diverging policy regimes, the compliance cost of the current approach is estimated to be between $98 and 112 billion per year.[9] As costly as the current patchwork approach is, implementing federal legislation modeled after the GDPR would be even more so. Estimates by the Information Technology and Innovation Foundation (ITIF) found that federal legislation mirroring the GDPR or CCPA would cost roughly $122 billion per year.[10]

A study by Deloitte analyzed the GDPR, specifically honing in on advertising practices, and once again found significant costs. The study focused on firms that use direct marketing and found a loss of EU GDP of roughly $90 billion[11] and a potential loss of employment of 1.3 million.[12]

Any data privacy legislation would impose some costs, but the high price tag should caution lawmakers against placing burdensome regulations on companies without balancing them against consumer harm and forgone benefits.

Contradictions in GDPR "Rights"

When the EU enacted the GDPR it was seen as the most comprehensive data legislation to date. Through the extensive list of rights, in effect, the GDPR places the ownership of data with the individual regardless of how it was collected. Contrary to typical property agreements, the individual can rescind or change permissions at any time.

Among the established rights is the right to be forgotten, which appears straightforward; however, tracking what information has been collected is no simple task. Establishing a broad right such as this is in direct opposition to emerging technologies that could facilitate other areas of data protection. One example is ongoing experimentation using blockchain technology to manage personal data.[13]

[8] oag.ca.gov. "California Consumer Privacy Act (CCPA)," January 1, 2023.

[9] Daniel Castro, Luke Dascoli and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," *Information Technology & Innovation Foundation*, Jan. 24, 2022.

[10] Alan McQuinn and Daniel Castro, "The Cost of an Unnecessarily Stringent Federal Data Privacy Law," *Information Technology & Innovation Foundation*, Aug. 5, 2019.

[11] Currency conversion on 2/22/2023.

[12] "Economic impact assessment of the proposed European General Data Protection Regulation," *Deloitte*, Dec. 16, 2013.

[13] Shobanadevi, Sumegh Tharewal, Mukesh Soni, D. Dinesh Kumar, Ihtiram Raza Khan and Pankaj Kumar, "Novel identity management system using smart

Comprehensive laws fail to account for novel data structures. Blockchains, for example, are typically immutable and thus incompatible with a right to be forgotten. Likewise, the right to rectification, which involves editing existing data, is fundamentally incompatible with blockchain technology.

An additional example of potential contradictions in these comprehensive data "rights" is the right to portability. The ability to transfer data to different companies runs counter to principles of data security.

Likewise, the FTC has filed complaints against companies for inadequate data protection. The U.S. law COPPA requires that "The operator must also take reasonable steps to release children's personal information only to service providers and third-parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner."[14]

However, the right of portability allows the consumer to move data from one company to another, potentially opening their data to susceptibility. This attempt at regulating data privacy results in sacrificing data security. If the U.S. government took similar actions, it could create overlapping jurisdiction regarding responsibility for data protection.

Consumer Benefits and Consent

Despite difficulties in creating effective regulations, the increased presence of online services means it is essential to balance security with the wishes and behaviors of consumers.

Pew Research reports that 72 percent of U.S. adults use at least one form of social media, which is a massive increase from a mere 5 percent in 2005. According to the data set, the percentage of Facebook users remained high even after the Cambridge Analytica Scandal in 2018.[15] Consumers may state their security concerns, but their behavior is not generally demonstrative of severe concern. Despite widely publicized security concerns regarding TikTok, the social network has experienced massive growth and was ranked sixth in monthly active users at the beginning of this year.[16]

Looking solely at behavior clearly suggests that for social media users, the perceived benefits outweigh the perceived risk. This phenomenon is often referred to as the privacy paradox, which essentially explains that users claim to care about privacy but will make little effort to change their behaviors to protect it.[17] Behavior shows that

blockchain technology," *Springer Nature*, Oct. 12, 2021.

[14] "Part 312 - Children's Online Privacy Protection Rule," *Code of Federal Regulations*, Children's Online Privacy Protection Rule, Jan. 17, 2013.

[15] "Social Media Fact Sheet," *Pew Research Center*, Apr. 7, 2021.

[16] S. Dixon, "Most popular social networks worldwide as of January 2023, ranked by number of monthly active users," *Statista*, Feb. 14, 2023.

[17] Susanne Barth and Menno D.T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual

convenience and low prices — often free in the case of social media — offer a temptation too appealing for privacy concerns to outweigh.

The paradox could have numerous explanations, but it is not necessarily illogical. Despite claims about the value of data — such as the argument in *The Economist* in 2017 that data had surpassed oil as the most valuable resource — the value of personal data is not greater than the perceived value of services consumers receive.[18]

The market value of personal data comes from large data sets, while individual data are not worth a lot. The *Financial Times* released a data calculator which accounts for different factors that influence the value of consumer data.

The actual value, according to the calculator, starts at less than a penny.[19] On the higher end, victims of the Equifax data breach were eligible for a maximum of $125 per person,[20] but that sum is more indicative of legal actions by the FTC and not the actual market value.[21] Either way, the worth of data is not nearly the same value as the services provided in exchange.

According to a 2018 study, Facebook users would require more than $1,000 to deactivate their accounts for a year.[22] Additionally, the worth of Amazon Prime is estimated to be $646 more than the cost. The value derived from digital and data-intensive platforms can be worth more to consumers than their data. Regulators should respect this tradeoff.[23]

Lack of Widespread Knowledge

While decision-makers should respect consumer consent, grey areas can arise due to a lack of widespread knowledge regarding data practices. For instance, the term "data" is not uniform. In terms of tech, a working paper by Wolfgang Kerber from the University of Marburg divides data into information that is provided voluntarily, information that is observed through mechanisms such as cookies or tracking, and information that is derived from the previous two categories.[24]

---

online behavior – A systematic literature review," *El Sevier*, Apr. 14, 2017.

[18] Leeward Capital Management, "The world's most valuable resource is no longer oil, but data," *The Economist*, May 6, 2017.

[19] Emily Steel, Callum Locke, Emily Cadman and Ben Freese, "How much is your personal data worth," *Financial Times*, June 12, 2013.

[20] Robert Schoshinski, "Equifax data breach: Pick free credit monitoring," *Federal Trade Commission*, July 31, 2019.

[21] The victims were eligible for free credit monitoring or a $125 payout. However, the funding for the payout was capped and the high number of claims drew concerns from the FTC that they would not be able to pay that amount to all victims.

[22] Jay R. Corrigan, Saleem Alhabash, Matthew Rousu, and Sean B. Cash, "How much is social media worth? Estimating the value of Facebook by paying users to stop using it," *Plos One*, Dec. 19, 2018.

[23] Krisztina Pusok, Edward Longe and Tirzah Duren, "Self-Preferencing and Big Tech," *The Lost Economy*, May 2016.

[24] Woldgang Kerber, "Digital markets, data, and privacy: Competition law, consumer law, and data protection," *Philipps-University Marburg, School of Business and Economics,* Feb 2016.

While most consumers have enough understanding of the data they explicitly enter and provide to websites, the other two categories are where consent becomes more complicated. According to a 2011 study conducted by CyLab at Carnegie Mellon University, which tested nine tools designed to prevent online behavioral advertising (essentially a practice that uses data from tracking tools like cookies), all nine tools presented a challenge for users. User error in this study made it difficult for consumers to take advantage of privacy settings even when they were available.[25]

One way around this is the requirement to opt-in. The GDPR opt-in requirement resulted in a 12.5 percent reduction in observed consumers, but caused the remaining consumers to be visible for longer.[26] In sum, the opt-in requirement did not result in a significant change in a business's ability to make data-derived decisions. Opting-in may be one way to ensure consumer consent, but it should be strengthened by requirements of easily understandable explanations of data practices to ensure that consent is informed.

Confusion and misconceptions regarding data practices contribute to the phenomenon that scholars Omer Tene and Jules Polonetsky refer to as the "creepy factor."[27] This occurs through uses of data perceived as unexpected or distasteful. One demonstrative example occurred when Target used to purchase data to predict pregnancy and then target consumers with relevant ads. Few would be upset or surprised that Target has data on consumer purchases, but the ability of the company to accurately predict personal life cycle and health developments is what many consumers perceive as a creepy violation of privacy.

The GDPR in the European Union contains a right against profiling unless it is necessary, authorized by the state, or consented to, which would run in conflict with online behavioral advertising. However, despite being included in a data privacy bill, profiling has less to do with what type of data is collected and more to do with what is done with it after the fact.[28] Such practices often offer consumer benefits.

In economic models that use data from consumers' buying decisions to offer personalized pricing, the ultimate benefit to the consumer is dependent on the relative competitiveness and other features of the specific marketplace.[29] While these findings are based off models, airlines have been observed to

[25] Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay and Yang Wang, "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," *Cylab*, Oct. 31, 2011.

[26] Guy Aridor, Yeon-Koo Che and Tobias Salz, "The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR," *National Bureau of Economic Research*, March 2020.

[27] Omer Tene and Jules Polonetsky, "A Theory of Creepy: Technology, Privacy, and Shifting Social Norms," *Yale J.L & Tech, vol. 16,* 2013.

[28] "Automated individual decision-making, including profiling," *Intersoft Consulting*, General Data Protection Regulation, Apr. 27, 2016.

[29] ibid.

practice price discrimination depending on the time of day consumers make their purchases.[30] This pattern shows that data practices can influence consumer welfare within the right context.

The lack of understanding and the creepy factor that consumers are dealing with makes it difficult to establish privacy legislation that addresses their concerns. Consent-based legislation is important, but it is difficult for consumers to meaningfully provide consent to processes that they do not understand. To address this problem, lawmakers should focus on ensuring privacy practices are easily understandable. Applying informed consent to derived data would establish consumer protections without regulating beneficial business practices out of existence.

Conclusion

To enact privacy legislation that protects consumer data while respecting consumer choices, lawmakers need to focus on limited protections that address current inconsistencies. Of first importance is responding to consumers' lack of understanding. Privacy agreements are difficult to read and digest. Regulations that require a simple and public explanation of practices would establish protections for informed consent.

Along with the need for informed consent is respect for consumer choices. To implement consumer-focused data protections without burdening businesses, lawmakers need to enact protections against targeted harms while not listing endless "rights" that contradict standard practices. Without a comprehensive alternative to the GDPR that puts consumer consent and sectoral policymaking first, more governments will adopt contradictory rights-based omnibus bills.

[30] Diego Escobari, Nicholas G. Rupp and Joseph Meskey, "An Analysis of Dynamic Price Discrimination in Airlines," *Social Science Research Network*, Apr. 12, 2018.