MERCATUS CENTER
George Mason University

POLICY BRIEF

An Analysis of Recent Federal Data Privacy Legislation Proposals

Jennifer Huddleston

March 2019

In 2018, data privacy regulation was a topic of debate at both the state and federal levels. Legislative proposals, letters from advocacy groups,[1] and editorials all indicate that such conversations will only continue in 2019.[2] Many seem optimistic that, unlike previous attempts, bipartisan federal reform may be possible in a way that provides a clearer framework for data privacy and continues to allow America to take a lead on innovation.[3] However, policymakers should be cautious not to merely react to a perceived crisis around data privacy without considering the potential consequences of a solution. Much of the debate around data privacy comes down to individual preference, and in setting requirements, certain tradeoffs to speech, innovation, and consumer choice could make the cure worse than the disease.

In May 2018, the European Union's General Data Protection Regulation (GDPR) went into effect. US companies spent $7.8 billion to comply with GDPR.[4] According to a PwC survey, 88 percent of companies spent more than $1 million, and 40 percent of companies spent more than $10 million to comply with these new regulations.[5] Far from encouraging more competition or more privacy-centric options, these regulations have seen companies exit the market and the market share of "Big Tech" companies such as Google and Facebook grow.[6] Yet despite these consequences, many are asking if the United States should abandon its laissez-faire approach to innovation and adopt its own data privacy regulatory regime similar to GDPR.[7]

Since late 2018, the Senate has seen three major proposals regarding data privacy introduced. This brief will look at the benefits and tradeoffs of those proposals, the current framework for federal action regarding data privacy, and the likely impact of each approach on innovation and consumer choice.

CONSUMER DATA PROTECTION ACT

In November 2018, Senator Ron Wyden (D-OR) proposed the Consumer Data Protection Act.[8]

The proposal would significantly expand and change the focus of the Federal Trade Commission (FTC) on data privacy and establish a new Bureau of Technology within the commission to enforce the new regulations. This proposal calls for a dramatic increase in regulation for data privacy and cybersecurity and a change in the way data privacy and injury are understood, making that understanding similar to the one under the GDPR, and represents a significant change from the American approach.[9] Notably, the proposal would expand the definition of substantial injury regarding data breaches to include noneconomic injury.

While harms from privacy violations can occur, as discussed in previous work from the Mercatus Center at George Mason University regarding the FTC's approach to similar issues of informational harm,[10] an expansive view could negatively impact free speech by silencing speakers in favor of a preference for privacy that is not universally shared.[11] For example, a social media posting and its subsequent request for removal would require intermediaries to silence one individual in favor of the preferences of another. While there may be some situations that warrant such action—libel, personal threats, or disclosure of information that would undermine trade secrets, national security, or individual safety—an approach that always favors privacy over speech risks silencing legitimate speech. Expanding the definition of harm in such a scenario is more likely to put such rights at odds with one another. Instead, continuing the existing US approach allows common law and norms to evolve a view that more adequately balances potentially conflicting rights and preferences.

In the months since the European Union enacted the GDPR, the impact of stringent data regulations on competition and innovation has become increasingly apparent. A variety of companies, from newspapers to video games,[12] have chosen to exit the EU market, and large companies that could afford to engage in costly compliance have grown even more dominant in the data space.[13] Rather than encouraging smaller players to develop more privacy-sensitive options that could compete with and potentially challenge existing giants, concerns over compliance and the costs associated with compliance have further reduced the number of options available in the market.[14] As a result, larger players have been able to retain or even grow their market share in the face of such regulations. Given the wide range of consumer preferences when it comes to privacy, a market with more is more likely to allow consumers to find products tailored to their needs. Imposing similarly restrictive regulations in the United States under this proposal would likely see the same results regarding market concentration and decreased options for consumers.

But in some ways the Wyden proposal takes things a step further than the recent European regulations by imposing harsher penalties for violations. While the maximum fines for violations mirror GDPR,[15] one notable feature of this proposal is that it includes jail time in certain

circumstances for executives whose companies violate the regulations.[16] Such a criminal sanction does not line up with the realities of either decision-making or incentives influencing decisions around privacy.[17]

Another key feature of this proposal is the creation of a Do Not Track registry that would essentially create a universal opt-out option for consumers modeled after the Do Not Call system.[18] Innovative market solutions such as ad blockers and Do Not Track extensions could provide a wider variety of options for a similar purpose without the same impact as regulation,[19] but this model would at least theoretically still function as an opt-out system rather than an opt-in.[20] In fact, various options to avoid cookies, ads, and other methods of tracking are available to consumers who wish to use them now. However, given the severity of sanctions for violation, it is likely that most actors would err on the side of caution, resulting in a far more restrictive approach to such a registry that results in it functioning more like an opt-in than an opt-out system. Yet research shows that consumers are rarely more informed under opt-in regimes than opt-out. What's more, opt-in systems increase costs for companies who bear the burden of regulatory compliance and forgo the higher revenue of opt-out regimes.[21]

As an alternative, various working groups have come up with protocols and best practices regarding "Do Not Track."[22] These non-enforceable norms or standards, also called soft laws, provide an innovation-friendly approach that can better balance consumer needs and the needs of industry.[23] For example, the World Wide Web Consortium has addressed a variety of concerns through best practices such as developing a working draft on complying with consumer notices of Do Not Track in a uniform way to respect users' preferences.[24] Similarly, the National Telecommunications and Information Administration (NTIA), through cooperation between government, industry leaders, and civil society advocates, developed best practices for the commercial use of facial recognition software including addressing a number of potential data security concerns.[25] Of course, such tools only work if industry players buy into them, or if industry polices itself, or if consumers themselves keep businesses in check.[26] While some dispute about the definition and enforcement of Do Not Track policies continue, many have adopted such industry principles already.[27] Still, taking a soft-law or self-governing approach through working groups and the development of best practices is more likely to be able to consider the realities of industry decisions around available technologies and come to a consensus that reflects both consumers' desires and these realities.

The bill does provide exceptions for nonprofits, journalists, and smaller companies. These companies are less likely to be able to afford the initial compliance burden and would be more likely to face difficult choices and potentially crushing liability.[28] Such carve-outs also show an attempt to learn from the lessons of GDPR. Still, these carve-outs could discourage a new company from ever growing large enough to challenge existing market incumbents, since at a certain point additional growth also requires a significant increase in regulatory compliance costs.[29]

In general, the Consumer Data Protection Act would shift the United States' approach to inno-

vation from a laissez-faire to a precautionary regime that values a particular privacy preference above other options.

DATA CARE ACT

In December 2018, Senator Brian Schatz (D-HI) proposed the Data Care Act.[30] This proposal would give broad regulatory authority to the FTC, which would likely introduce significant compliance burdens on companies that would have to transfer innovative resources and energies to regulatory compliance efforts.

A key distinguishing feature of the Data Care Act is the idea of information fiduciaries.[31] The act would establish a duty of care for consumer data for covered entities that would be similar to the heightened duties regarding personal information that currently apply to institutions such as banks and hospitals.[32]

However, the concept of information fiduciaries is less practical than traditional fiduciary relationships, like those found with trustees or financial institutions. In a traditional fiduciary relationship, the vulnerability associated with disclosure is readily apparent.[33] But concerning "personal" information online, there seems to be a wider variety of preferences and understanding of what information should be covered as well as more disagreement over what information makes one vulnerable.[34] Establishing such a requirement would force innovators to value privacy over other benefits that consumers may actually prefer.[35] A company would be forced to place significant resources in ensuring privacy, including potentially charging for a product rather than having added revenue to support it. In many cases consumers have indicated that they would be unwilling to pay for what are currently data-supported products such as social media.[36] For more sensitive information such as Social Security numbers or financial information, consumers tend to be more willing to pay for privacy or services, and that is reflected in their selection of intermediaries and the offerings on the market.[37]

Additionally, this act places broader regulatory authority regarding data privacy with the FTC. This would likely result in an increased regulatory burden. However, it is possible this could merely result in formalizing the existing strategies engaged in through various consent decrees, providing more transparency and certainty to innovators about what constitutes violations.[38] Ideally, such regulations could incorporate recommended self-regulatory best practices or be developed through multistakeholder initiatives to be more adaptive and forward-looking rather than, like the GDPR, possibly prevent new innovative online intermediaries from ever getting off the ground owing to burdensome regulatory requirements. Failing to clarify the appropriate bounds of such delegation would result in a greater risk that the regulatory approach would be more restrictive and prescriptive than the current policy.

The Data Care Act would change the relationship between innovators, consumers, and regulators to be centered more around privacy than other goals, ultimately emulating the European approach to data privacy.

AMERICAN DATA DISSEMINATION ACT

The most recent proposal from Senator Marco Rubio (R-FL), the American Data Dissemination (ADD) Act,[39] would impose privacy regulations on private actors similar to those currently imposed on government actors and would also preempt states in imposing additional regulations. While this approach would solve some of the more disruptive problems of laws such as the California Consumer Privacy Act (CCPA), it still has several potential concerning consequences that could limit innovation, eliminate choices consumers enjoy, and still have a particularly burdensome impact on smaller players.

First, applying the current government standards to private actors does not consider the differences between such actors in the reasons for collecting data, the way they are used, or the incentives for data security. While individuals may choose not to use a certain service because of their preferences for privacy, they typically do not have the same choice to opt out when it comes to government data collection. Likewise, government incentives regarding safeguarding data may be based less on preferences or individuals' desire for privacy and more on preventing the potential harm to government interests, such as national security, that could come from such a data breach.[40]

Another concern is that the proposal's broad definition of covered entities could include any service that uses the internet and collects records. As Will Rinehart points out, "There is hardly a business in America that wouldn't be included with that kind of expansive definition."[41] The use of data and information is not merely limited to the internet intermediaries one typically thinks of, such as social media sites. Changes to data regulation are not limited to but can impact everything from brick-and-mortar businesses' loyalty programs to newer technologies that are still developing, such as the internet of things.[42] Data privacy legislation will have an impact on both innovation and consumer choices beyond just online behavior, and the broader the definition of covered entities, the more industries that will be impacted. As a result small business would likely be particularly impacted by these regulatory and compliance costs limiting new entrants seeking to provide innovative products.[43]

By preempting state laws regarding data privacy such as the CCPA, the ADD Act would address a potentially growing problem of states attempting to impose regulatory frameworks on the internet. Given the borderless nature of data flows, such preemption will likely be essential for any federal data privacy policy.[44] Federal preemption of state laws concerning data privacy could prevent the development of a patchwork of state laws, which would place burdens on speech and interstate commerce.[45] Preemption would also eliminate the risk that a state-based system would also further

complicate compliance for online actors and other data collectors who would have to consider numerous and possibly conflicting standards.[46]

CONTINUATION OF THE AMERICAN MODEL

Of course, an alternative to any of the current proposals is merely to maintain the laissez-faire regulation model that has allowed the United States to be a leader in technology. Seven of the ten largest tech companies are American, while only one is European.[47] The United States' success as a leader in technological innovation stems largely from this liberal approach to innovation that has encouraged new ventures online with minimal government regulation, while the European precautionary and regulatory approach has largely quashed innovation.[48] Still, with states like California now enacting their own data privacy policies, federal action may be necessary to prevent an individual state from unfairly disrupting markets and the framework initially established for the internet.[49]

In fact, the American regulatory model is capable of fostering innovation while dealing with privacy problems as they appear. Under the current system, the FTC has dealt with data breaches and information privacy through its enforcement under unfair and deceptive practices authority. This has led it to focus on consumer harm and address issues on a case-by-case basis. As a result, companies can provide a variety of options to consumers while still allowing the FTC to address issues of companies engaging in practices that harm consumers.[50] Facebook is likely to face record fines owing to its violations of existing consent decrees with the FTC, which would affirm the FTC's authority to intervene in and correct such violations.[51]

Of course, this approach is not without its own drawbacks. For example, addressing problems on a case-by-case basis does nothing to establish broadly applicable norms that new innovators can rely on when determining what actions are necessary for compliance with agency standards.[52] The resulting treatment can seem random to the parties involved because the results of regulation are determined by various parties' desire to avoid litigation and quickly reach an agreement owing to both legal and public factors.[53] The regulatory interventions themselves may fail to adapt and change with evolving industry standards, forcing first-movers out of the market while similar behavior becomes, in time, generally tolerated.[54]

In addition to the FTC, a wide variety of multistakeholder groups and industry coalitions has worked to develop best practices and other informal forms of self-regulation and soft law. But often the success of such processes depends on forming a consensus in the industry that will adopt those best practices. Embracing industry standards and focusing only on cases of demonstrable harm seems to be the most effective approach to regulation that, at once, provides protections to consumers and minimizes disincentives to innovation.[55]

As states like California have enacted their own data privacy laws, companies could face an even more crushing regulatory landscape in the absence of federal action.[56] Because of the borderless nature of the internet, without such laws being struck down by preemption or the courts, innovators would face a situation that requires them to either pick and choose which states to provide products in or to invest in complicated compliance with 50 or more regulatory schemes.[57] For example, an Illinois law governing biometric information privacy prevented Illinois residents from being able to use the Google Arts & Culture Face Match.[58] More general privacy laws could prevent new products from reaching consumers and segment usage in a way that makes it incredibly difficult for new competitors to truly challenge the existing giants who can afford to comply in all 50 states.[59] It is also almost inevitable that such laws would come into conflict with First Amendment expression and speech rights as individuals or entities are forced to remove information.[60]

The current approach has allowed the United States to cultivate a sunny climate for innovation that has yielded generous fruits in terms of convenience and variety in consumer products. However, with the emergence of state laws and other regulatory regimes like GDPR, the absence of federal law could allow for the springtime of American innovation to turn into winter.

CONCLUSION

The presumption that data privacy is broken based on individual incidents such as breaches rather than real harm to consumers or competition could lead to tradeoffs that impact innovation and remove choices that consumers actually enjoy. Many of the proposed solutions could result in valuing privacy over innovation and choice. As a result, such changes could unintentionally lock in the current options and prevent new players from arising and providing better products. Ideally, policy proposals should focus on remedying actual harms while allowing as much freedom to innovate as possible, lest America surrender its technological leadership.

ABOUT THE AUTHOR

Jennifer Huddleston is a research fellow at the Mercatus Center at George Mason University. Her research focuses on the intersection of emerging technology and law with a particular interest in the interactions between technology and the administrative state. Her work covers topics including judicial deference, liability protection for internet platforms, autonomous vehicles and other disruptive transportation technologies, the regulation of data privacy, and the benefits of technology and innovation.

NOTES

1. Levi Sumagaysay, "Is It Time for a Federal Data Protection Agency?," *Mercury News*, January 18, 2019.
2. "There's Hope for Federal Online Privacy Legislation," *Washington Post*, January 21, 2019.
3. *Washington Post*, "There's Hope for Federal Online Privacy Legislation."
4. Oliver Smith, "The GDPR Racket: Who's Making Money from This $9 Billion Shakedown," *Forbes*, May 2, 2018.
5. PwC, "Pulse Survey: GDPR Budgets Top $10 Million for 40% of Surveyed Companies," accessed January 29, 2019, https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html.
6. Nick Kostov and Sam Schechner, "Google Emerges as Early Winner from Europe's New Data Privacy Law," *Wall Street Journal*, May 31, 2018; Adam D. Thierer, "GDPR Compliance: The Price of Privacy Protections," *Technology Liberation Front*, July 9, 2018.
7. David Meyer, "In the Wake of GDPR, Will the U.S. Embrace Data Privacy?," *Fortune*, November 29, 2018.
8. S. 2188, 115th Cong. (2018).
9. Katherine Goodloe and Melody Ramsey, "Wyden Releases Draft Privacy Bill Increasing FTC Authority, Providing for Civil Fines, and Criminal Penalties," *Inside Privacy*, November 9, 2018.
10. Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
11. Koopman et al., "Informational Injury."
12. Alex Hearn and Martin Belam, "LA Times among U.S.-Based News Sites Blocking EU Users due to GDPR," *Guardian*, May 25, 2018; Matthew Gault, "Why Europe's New Privacy Laws Are Causing Some Online Games to Shut Down," *Motherboard*, May 18, 2018.
13. Alec Stapp, "Against Privacy Fundamentalism in the United States," Niskanen Center, November 19, 2018, https://niskanencenter.org/blog/against-privacy-fundamentalism-in-the-united-states/.
14. Stapp, "Against Privacy Fundamentalism."
15. Robert Hackett, "Sen. Wyden Proposed a CEO-Felling Data Privacy Law. Is Big Tech Ready for It?," *Fortune*, November 3, 2018.
16. Colin Lecher, "Sen. Ron Wyden Proposes Bill That Could Jail Executives Who Mishandle Data," *Verge*, November 1, 2018.
17. Taylor Armerding, "Don't Expect Jailed CEOs, but Wyden at Least Puts Consumer Privacy on the Table," *Forbes*, November 7, 2018.
18. Goodloe and Ramsey, "Wyden Releases Draft Privacy Bill."
19. Kevin Purdy, "What 'Do Not Track' Is and Why It's Important," *LifeHacker*, February 22, 2011.
20. Will Rinehart, *Opt-In Mandates Shouldn't Be Included in Privacy Laws* (Washington, DC: American Action Forum, 2018).
21. Rinehart, *Opt-In Mandates*.
22. "Tracking Compliance and Scope, W3C Working Draft," World Wide Web Consortium, January 22, 2019, https://www.w3.org/TR/tracking-compliance/.
23. Ryan Hagemann, Jennifer Huddleston, and Adam D. Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future," *Colorado Technology Law Journal* (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539.
24. World Wide Web Consortium, "Tracking Compliance and Scope."
25. National Telecommunications and Information Administration, *Privacy Best Practice Recommendations for Commercial*

Facial Recognition Use, n.d., https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf. The document has several prescriptions: encourage transparency, develop good data management practices, allow people to control the sharing of their data, use security safeguards, ensure data quality, and allow problem resolution and redress.

26. Joseph Lorenzo Hall, "Pinterest Moves to Support Do Not Track," Center for Democracy and Technology, July 26, 2013.
27. Leslie Harris, "The Bizarre, Belated Assault on Do Not Track," *Huffington Post*, December 4, 2012.
28. Andrea O'Sullivan and Christian McGuire, "Why More Regulation Might Be on Facebook's Christmas List," *The Bridge*, December 4, 2018.
29. W. Mark Crain and Nicole V. Crain, *The Cost of Federal Regulations to the U.S. Economy, Manufacturing, and Small Business* (Washington, DC: National Association of Manufacturers, 2014), 7. This report discusses more generally how regulations can discourage small businesses from investing in growth.
30. S. 3744, 115th Cong. (2018).
31. Jack M. Balkin, "Information Fiduciaries and the First Amendment," *UC Davis Law Review* 49, no. 4 (2016): 1186. This article introduces the concept of information fiduciaries.
32. Dell Cameron, "Democrats Want Internet Companies to Be Liable Like Banks and Hospitals," *Gizmodo*, December 12, 2018.
33. *Hospital Products Ltd. v United States Surgical Corporation*, [1984] HCA 64, 156 CLR 41 (Austl.).
34. Emily Tabatabai and Shea Leitch, "States Continue to Expand Definition of 'Personal Information,'" *Privacy Tracker*, February 27, 2017.
35. Rinehart, *Opt-In Mandates*. This report discusses various surveys regarding consumer preferences for benefits or privacy concerning various personal information.
36. Rani Molla, "How Much Would You Pay for Facebook without Ads," *Recode*, April 11, 2018.
37. Rinehart, *Opt-In Mandates*.
38. *Privacy & Data Security: Update: 2017* (Washington, DC: Federal Trade Commission, 2017). This report shows the FTC's current approach.
39. American Data Dissemination Act of 2019, 116th Cong. (2019).
40. Susan Landau, "Understanding Data Breaches as National Security Threats," *Lawfare*, February 26, 2018.
41. Will Rinehart, "Understanding the American Data Dissemination Act," American Action Forum, January 17, 2019.
42. Julia Van Greiken, "How the GDPR Affects Loyalty Programs," *IT Governance*, April 13, 2018; Cathleen Berger, "The Clash of GDPR and IoT," *Medium*, May 22, 2018.
43. Brent Skorup and Jennifer Huddleston, "It's Not about Facebook; It's about the Next Facebook," *RealClearPolicy*, June 1, 2018.
44. Alec Stapp and Ryan Hagemann, *Request for Comments on Developing the Administration's Approach to Consumer Privacy* (Washington, DC: Niskanen Center, 2018).
45. Jennifer Huddleston, "The Problem of Patchwork Privacy," *Technology Liberation Front*, August 15, 2018.
46. Jennifer Huddleston, "When States Get It Wrong and the Case for Federal Preemption," *The Bridge*, October 23, 2018.
47. Kristin Stoller, "The World's Largest Tech Companies 2018: Apple, Samsung Take Top Spots Again," *Forbes*, June 6, 2018.
48. Adam Thierer, "What 20 Years of Internet Law Teaches Us about Innovation Policy," Federalist Society, May 12, 2016.
49. Jeff Kosseff, "Ten Reasons Why California's New Data Protection Law Is Unworkable, Burdensome, and Possibly Unconstitutional," *Technology & Marketing Law Blog*, July 9, 2018 (this article describes the negative impact of California's

law); Ryan Hagemann, "Commemorating 20 Years of Grade-A Internet Policy," Niskanen Center, June 30, 2017.

50. Neil Chilson, *When Considering Federal Privacy Legislation* (Washington, DC: Regulatory Transparency Project, 2018).
51. Tony Romm and Elizabeth Dwoskin, "U.S. Regulators Have Met to Discuss Record-Setting Fines against Facebook for Privacy Violations," *Washington Post*, January 18, 2019.
52. Jennifer Huddleston, "Unprecedented: The Issue of Agency Action by Consent Order on Innovation," *Plain Text*, September 22, 2017.
53. Huddleston, "Unprecedented."
54. Huddleston; Koopman et al., "Informational Injury."
55. Chilson, *When Considering Federal Privacy Legislation*.
56. Kosseff, "Ten Reasons Why"; Huddleston, "Unprecedented"; Stapp and Hagemann, "Request for Comments."
57. Christine McDaniel, "The Trade Issue No One Is Talking About," *The Hill*, December 20, 2018. This article discusses the borderless nature of data and the potential impact of data regulations on trade.
58. Ally Marotti, "Google's Art Selfies Aren't Available in Illinois. Here's Why.," *Chicago Tribune*, January 17, 2018.
59. Wayne Winegarden, "States Where Regulations Harm Small Business Most," *Forbes*, July 28, 2015. This article discusses more generally the impact of additional state regulations on small businesses.
60. George Brock, "How the 'Right to Be Forgotten' Puts Privacy and Free Speech on a Collision Course," *The Conversation*, November 18, 2016.