ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Daniel Castro

Vice President

Information Technology and Innovation Foundation

Before the

Committee on House Administration

Hearing on

"Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors"

February 16, 2022

1310 Longworth House Office Building

Washington, DC

Chairperson Lofgren, Ranking Member Davis, and members of the committee, thank you for the opportunity to appear before you to discuss privacy risks and potential reforms.

I am the vice president of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonprofit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also the director of the Center for Data Innovation, a research institute at ITIF focusing on the intersection of data, technology, and public policy.

In my testimony today, I would like to provide an overview of why Congress should pass data-privacy legislation, what that legislation should look like, and how the United States can avoid the mistakes made in the EU's General Data Protection Regulation (GDPR) and other data-privacy laws.

WHY CONGRESS SHOULD PASS DATA-PRIVACY LEGISLATION

U.S. data privacy is at a crossroads. Many consumers are justifiably frustrated by the frequency with which they learn about new data breaches and the seeming lack of accountability for those who misuse personal information. At the same time, many businesses are overwhelmed by the tsunami of new data-protection obligations they face and the growing restrictions on how they can use personal information. And all are confused by the multitude of ever-changing laws and regulations.

These conditions have created a groundswell of support for new data-protection laws. Over the past few years, federal and state lawmakers have proposed various privacy laws to regulate the collection and use of personal data. Three states—California, Virginia, and Colorado—have passed comprehensive data-privacy legislation that gives consumers in those states new rights regarding the collection of their personal information and imposes new obligations on businesses. Many other states have considered enacting similar privacy laws. Between 2018 and 2021, 34 state legislatures have introduced a total of 72 bills, which have advanced to various stages of the legislative process.

These new state privacy laws can create confusion for consumers and impose significant costs on businesses—both direct compliance costs and decreases in productivity—and undermine their ability to responsibly use data to innovate and deliver value to consumers. Moreover, these laws create high costs not just for in-state businesses, but also for out-of-state businesses that can find themselves subject to multiple and duplicative rules. For example, California's recently enacted privacy law will likely cost $78 billion annually, with California's economy bearing $46 billion and the rest of the U.S. economy bearing the other $32 billion. California small businesses will bear $9 billion of in-state costs, while out-of-state small businesses face $6 billion of costs.[1]

In the absence of federal data-privacy legislation, the growing patchwork of state privacy laws could impose out-of-state costs between $98 billion and $112 billion annually.[2] Over a 10-year period, these costs would exceed $1 trillion. The burden on small businesses would be substantial, with U.S. small businesses bearing $20 billion to $23 billion annually.[3]

WHAT FEDERAL DATA-PRIVACY LEGISLATION SHOULD ACCOMPLISH

Although the United States needs a federal data-privacy law, it should not back away from the light-touch approach it has historically taken to regulating the digital economy. Instead of pursuing a broad, European-style data-privacy law that would impose significant costs on the U.S. economy, Congress should craft targeted legislation that creates a national privacy framework that establishes basic consumer data rights, preempts state laws, ensures reliable enforcement, streamlines regulation, and minimizes the impact on innovation. Such legislation should address concrete privacy harms, not hypothetical ones, and improve transparency so consumers better understand how businesses use their data. It should strengthen oversight and enforcement through the FTC and avoid unnecessary litigation costs by not including a private right of action. It should also protect and promote innovation by minimizing compliance costs and restrictions on data use, such as by avoiding data minimization and purpose specification requirements.

First, federal data-privacy legislation should establish basic consumer data rights. Lawmakers should not treat all data the same, but instead create rules that are tailored for different types of data and the contexts in which they are collected. To that end, privacy legislation should make a distinction between sensitive and non-sensitive personal data, because sensitive personal data—such as medical or location information—presents higher risk to people if it is made public.

The idea is to create a sliding scale where the most sensitive personal data collected in the most sensitive contexts (e.g., a doctor's office collecting a patient's health data) is subject to the strictest rules and penalties to prevent misuse, and non-sensitive data collected in a non-sensitive context (e.g., a grocery store tracking what kind of cereal shoppers buy) would be subject to the fewest requirements. With a tiered set of rules like this, consumers would receive stronger privacy protections where it matters most, and businesses could avoid undue compliance burdens.

Congress should give individuals the right to know how organizations collect and use any of their personal data or when their information has been part of a data breach, but consider limiting other rights, such as the right to access, port, delete, or rectify their data, to only sensitive data in certain contexts. For example, consumers should have a right to obtain a copy of their health or financial data and move it to a competing service.[4] Similarly, Congress should establish user consent requirements for data collection, sharing, and use based on a similar sliding scale. For example, health apps should need to obtain permission from consumers before sharing their sensitive health information with third-party researchers, but florists should be able to send their loyal customers a coupon unless they opt out.

Second, lawmakers should establish uniform privacy rules for the entire nation by preempting state and local privacy laws. Consumers should have the same protections regardless of where they live, and companies should not be faced with 50 different sets of laws and regulations. A patchwork of state laws with varying definitions and standards creates a complex regulatory minefield for businesses to navigate, especially if potential violations risk costly litigation. The goal of Congress should be to minimize unnecessary compliance costs for businesses so that they can concentrate their resources not on hiring more privacy lawyers to protect them from potential fines for non-compliance but on investments that will lead to more secure and privacy-preserving products and services.

Third, Congress should ensure there is robust and reliable enforcement of federal privacy law. Congress should give the Federal Trade Commission (FTC) sufficient resources and authority to fine organizations that impose actual harms on individuals through data misuse. Congress should also give the FTC authority to conduct limited rulemakings for data privacy for issues like deciding the right way for companies to disclose their data-handling practices. However, the legislation should be very specific in how the FTC can exercise its authority to ensure regulators do not impose heavy-handed rules about the design of user experiences for websites and mobile apps (i.e., "dark patterns").

Enforcement is important because it enables regulators to have oversight over organizations while ensuring they are held accountable when they do not follow the rules. However, Congress should be careful not to create duplicative or inconsistent enforcement mechanisms that would impose high costs for organizations. Indeed, if both regulators and private parties can pursue cases for identical reasons, firms can be tied up in lawsuits for years and pay hefty fees for each incident. To that end, Congress should not allow a private right of action, and instead rely on federal and state regulators to hold organizations accountable. In addition, organizations should only be subject to significant fines if they have caused actual economic harm. And to avoid unnecessary litigation, federal privacy legislation should allow for a reasonable period of time for organizations to address a violation without penalty in cases with no demonstrable consumer harm (e.g., establish a 60-day notice and cure period).

Fourth, Congress should set a goal of repealing and replacing potentially duplicative or contradictory federal privacy laws. The U.S. code is littered with privacy statutes—from major sections on health and financial data to narrow ones on video rental histories—and each one has its own set of definitions and rules to comply with.[5] Congress should create a roadmap to repeal and replace all of them with a single, comprehensive data-privacy law. Such a major overhaul may sound daunting, but the alternative—adding another layer to the pile—will undermine the purpose of new legislation.

Finally, federal data-privacy legislation should minimize the impact on innovation. To that end, Congress should not include data-minimization requirements, purpose-specification requirements, or privacy-by-design requirements because these provisions can reduce access to data, limit data sharing, and constrain its use, thereby limiting innovation. For example, purpose-specification requirements obligate organizations to disclose to users the purposes for which they are collecting information and then not use this collected data for any other reasons. This requirement limits organizations from reusing data for new purposes, which limits innovation. Purpose-specification requirements also limit organizations that may already be collecting useful data from extracting value from that information, such as by applying data analytics. Neither should Congress impose limitations on data retention or automated decision-making, as these provisions would similarly restrict organizations from efficiently using data.

HOW TO AVOID THE MISTAKES OF THE GDPR AND OTHER PRIVACY LAWS

Consumers and businesses would clearly benefit from a federal data-privacy law, but imposing a European-style law on American businesses recovering from a global pandemic would slow economic recovery by saddling companies with unnecessary red tape while limiting beneficial uses of data. Indeed, Congress can

benefit from hindsight by looking back at some of the negative consequences of GDPR, which went into effect in May 2018, and other privacy laws.

Avoid Excessive Compliance Costs

Congress should avoid enacting a privacy law that imposes excessive compliance costs. The GDPR has imposed massive compliance costs on businesses, not only in the EU but around the world. The Global Fortune 500 has spent an estimated €7 billion in compliance costs for GDPR.[6] In one survey, over 40 percent of companies, including U.S. firms with a data presence in the EU, had spent $10.1 million in compliance efforts.[7] In another, companies reported spending an average of $1.3 million in 2017 on GDPR compliance and were expected to spend an additional $1.8 million in 2018.[8]

Understand That More Regulation Does Not Always Benefit Consumers

Although some tout the GDPR as the gold standard for consumer protection, it has not always lived up to its reputation. For example, the law has had virtually no impact on consumer trust in the digital economy: Six months after it went into effect, consumer trust in the Internet was at its lowest in a decade in the EU.[9] A year after the law went into effect, nearly two-thirds of Europeans (63 percent) had never heard of the GDPR (31 percent) or did not know exactly what it is (32 percent).[10] The European Commission has found that "at a country level there is no consistent relationship between awareness of GDPR and the level of control respondents feel they have over the personal information they post online."[11] Moreover, many of these costs appear to do nothing to enhance consumer privacy. According to an October 2018 survey, a majority of companies that have appointed a data-protection officer (52 percent) say they established one for compliance reasons only, and that the role does not serve a valuable business function.[12]

Ensure Sufficient Resources for Regulators

Congress should ensure regulators have sufficient resources to handle any new obligations. The GDPR caught many regulators flat-footed. For example, the UK's Information Commissioner's Office (ICO) said its staff and services were overwhelmed by companies "over-reporting" potential data breaches because of concerns over high penalties if they failed to notify the data-protection authority (DPA) within the GDPR's tight 72-hour reporting deadlines.[13] Similarly, a spokesman of CNIL, the French DPA, declared that "the resources of the CNIL are insufficient" to enforce the GDPR.[14]

Beware of Unintended Consequences

Perhaps the most important lesson for policymakers from the GDPR is to beware of the unintended consequences of poorly crafted data-privacy legislation. For example, because the drafters of the GDPR never fully considered the implications of the law on emerging technologies like artificial intelligence and blockchain, they included a number of provisions that make it difficult, and sometimes virtually impossible, for businesses to use them.[15]

Some of the most significant unintended consequences are economic. For example, the GDPR has negatively impacted venture funding for EU tech firms. Between May 2018 and April 2019, the overall venture funding for EU tech firms decreased by $14.1 million per month per member state.[16] The decrease in investments for

young ventures caused by the GDPR could result in a yearly loss of up to approximately 30,000 jobs in the EU.[17] Or consider that 55 percent of the 539 mergers and acquisitions (M&A) professionals from Europe, Africa, and the Middle East surveyed in July 2018 declared having worked on transactions that did not go through due to concerns about companies' compliance with the GDPR.[18]

Some of these unintended consequences are also felt directly by consumers. Two months after the GDPR went into effect, a third of the largest U.S. news websites had to block access to the EU as they had not yet managed to comply.[19] Almost a year later, in March 2019, 1,129 U.S. news websites still remain blocked, including Pulitzer prize-winning publishers like the *Chicago Tribune*.[20] Companies have also interrupted some of their online services in the EU because of concerns over complying with the GDPR, including Czech platform Seznam, which had to shut down its student social network, and online gaming company Gravity Interactive, which blocked European users from accessing its games and services.[21]

Policymakers should also consider how individuals might misuse new privacy laws. For example, one of Finland's highest courts ruled in August 2018 that the GDPR's "right to be forgotten" could give a convicted murderer the right to have publicly available information about his crime removed from Google search listings, superseding the country's and the EU's own laws protecting freedom of speech and the right to access information.[22] Online tools have also been created to weaponize the GDPR against companies, such as overloading businesses with GDPR-authorized data requests that must be addressed within 30 days with the stated purpose to "waste their time."[23]

The COVID-19 pandemic also offered a lesson on the unintended consequences of the GDPR. At the beginning of the pandemic, Italy, one of the countries in Europe hit hardest by COVID-19, found that the GDPR prevented businesses from taking basic steps to track and trace potential infections, such as employers recording body temperatures to ensure compliance with safety protocols for essential workers. Similarly, the French data regulators noted that the GDPR prevented employers from using thermal cameras to automatically check temperatures of their workers.[24]

As the pandemic progressed, it became clear that the GDPR had also become a barrier to biomedical research—the very research necessary to save lives and reopen the economy. The GDPR creates significant challenges for research organizations in the EU sharing data with researchers located in most countries outside the EU. Indeed, a team of researchers from the United States, Canada, and the EU published an article in *Science* arguing that "the GDPR's limitation on data transfers will hamper science globally in general and biomedical science in particular."[25]

Prevent Costly Lawsuits

In addition to the GDPR, Congress can learn from some of the state privacy laws. In particular, the Illinois Biometric Information Privacy Act (BIPA) demonstrates the risk of costly litigation when privacy laws create a privacy right of action. BIPA was designed to regulate the collection of biometric data by companies operating in Illinois or whose products reached consumers in that state. Although BIPA passed into law in 2008, it was not until 2019 that the Illinois Supreme Court held that individuals are not required to show actual harm to bring consumer class action lawsuits and employer lawsuits. This ruling means that individuals can file

lawsuits even when there has only been a technical violation of the law.[26] Since then, the number of BIPA lawsuits has skyrocketed—In 2019, there were around 300 lawsuits, and the number of cases referencing BIPA doubled in 2020.

California offers another example of this dynamic. The California Consumer Privacy Act of 2018 (CCPA) applies to firms that do business in California, including those without a physical presence. The law allows consumers to seek damages when their personal information is inappropriately accessed or disclosed because a business failed to maintain reasonable security procedures. Since California enacted the law in 2020, plaintiffs have filed approximately 195 lawsuits against businesses in many different industries.[27]

Lawsuits can lead to major settlements, thereby threatening the viability of smaller businesses and imposing steep costs on larger ones. Even if a business can prevail in a lawsuit, the costs of the lawsuit are often significant, especially in state courts that are often more favorable for plaintiffs in class action litigation compared with federal courts and allow for expensive discovery processes, such as requesting documents and witness interviews, that can drive up the costs of litigation very quickly.

CONCLUSION

It is essential for Congress to craft well-designed federal data-privacy legislation. Poorly designed data-privacy laws can impose a substantial toll on the economy through both direct compliance costs and indirect costs from lower productivity and constraints on innovation. Unnecessarily restrictive rules for the digital economy reduce innovation in ways that harm both businesses and consumers. By raising compliance costs, increasing legal risks, and reducing the effectiveness of online business models, poorly drafted rules can lead to a reduction in the supply of, and demand for, digital services.

It is equally important for Congress to proceed swiftly with new data-privacy legislation. In the absence of a new law, states will continue to enact their own competing, and potentially contradictory, data-privacy laws. One of the primary purposes of the GDPR was to harmonize data-protection laws across EU member states, and ironically, by pushing for new laws modeled after the GDPR, state legislatures are creating the exact type of fragmentation in the United States that the EU created the GDPR to solve.

To avoid conflicting laws and unnecessary costs, Congress should act swiftly to pass comprehensive privacy legislation that preempts state laws, streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation (e.g., by avoiding requirements for data minimization, universal opt-in, purpose specification, limitations on data retention, or privacy-by-design). This legislation should not include a private right of action and instead rely on federal and state regulators for enforcement. Establishing a comprehensive federal privacy law would also simplify compliance for businesses, especially small businesses working across multiple U.S. jurisdictions, as well as help consumers better understand their privacy rights and avoid the confusion resulting from a patchwork of state laws.

Thank you again for this opportunity to appear before you today.

REFERENCES

[1] Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," (Information Technology and Innovation Foundation, January 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.

[2] Ibid.

[3] Ibid.

[4] Daniel Castro, "Improving Consumer Welfare with Data Portability," (Center for Data Innovation, November 2021), https://www2.datainnovation.org/2021-data-portability.pdf.

[5] For example, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA) apply to data in the health, financial, and educational sectors, respectively.

[6] Forbes, "The GDPR Racket: Who's Making Money From This $9bn Business Shakedown" (May 2, 2018), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#38765ac234a2.

[7] PriceWaterhouseCoopers, "Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies" (December 9, 2017), https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html.

[8] IAPP and Ernst & Young, "Annual Governance Report 2018" (IAPP and Ernst & Young, 2018), https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.

[9] Daniel Castro and Eline Chivot, "The GDPR Was Supposed to Boost Consumer Trust. Has it Succeeded?" European Views, June 6, 2019, https://www.european-views.com/2019/06/the-gdpr-was-supposed-to-boost-consumer-trust-has-it-succeeded/.

[10] European Commission, "Special Eurobarometer 487a, The General Data Protection Regulation" (June 2019), http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222.

[11] Ibid.

[12] IAPP and Ernst & Young, "Annual Governance Report 2018" (IAPP and Ernst & Young, 2018), https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.

[13] Information Commissioner's Office, "CBI Cyber Security: Business Insight Conference. ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference" (ICO, September 12, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/.

[14] Wall Street Journal, "European Privacy Regulators Find Their Workload Expands Along With Authority" (April 12, 2019), https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402.

[15] Eline Chivot and Daniel Castro, "The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy," Center for Data Innovation, May 13, 2019, https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/.

[16] Jian Jia, Ginger Zhe Jin, and Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment" (May 31, 2019), http://dx.doi.org/10.2139/ssrn.3278912.

[17] Jian Jia, Ginger Zhe Jin, and Liad Wagman, "The short-run effects of GDPR on technology venture investment" (VOX CEPR Policy Portal, January 7, 2019), https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.

[18] Merrill Corporation, "GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey" (Merrill Corporation, November 13, 2018), https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html.

[19] NiemanLab, "More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect" (August 7, 2018), https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

[20] Joseph O'Connor, "Websites not available in the European Union after GDPR" (March 20, 2019), https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr.

[21] CNN Business, "These companies are getting killed by GDPR" (May 11, 2018), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

[22] Center for Data Innovation, "The EU's Right to Be Forgotten Is Now Being Used to Protect Murderers" (September 21, 2018), https://www.datainnovation.org/2018/09/the-eus-right-to-be-forgotten-is-now-being-used-to-protect-murderers/.

[23] Ship Your Enemies GDPR, "Ship Your Enemies GDPR," (n.d.) https://shipyourenemiesgdpr.com/.

[24] Daniel Castro, "The Pandemic Reveals Some of the Noxious Side Effects of the GDPR," April 14, 2021, Center for Data Innovation, https://datainnovation.org/2021/04/the-pandemic-reveals-some-of-the-noxious-side-effects-of-the-gdpr/.

[25] Jasper Bovenberg et al., "How to Fix the GDPR's Frustration of Global Biomedical Research," *Science*, October 2, 2020, Vol. 370, No. 6512, pp. 40-42, https://www.science.org/doi/abs/10.1126/science.abd2499.

[26] "The BIPA Litigation Landscape and What Lies Ahead," Woodruff Sawyer, April 1, 2021, https://woodruffsawyer.com/cyber-liability/bipa-litigation-landscape/.

[27] "CCPA Litigation Tracker, Updated as of December 2021," Perkin Coie, n.d., https://www.perkinscoie.com/en/ccpa-litigation-tracker.html (access February 14, 2022).