Statement before the House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
On Protecting Consumer Privacy in the Era of Big Data

How the US Can Leapfrog the EU

The Role of Technology and Education in Online Privacy

Roslyn Layton
Visiting Scholar

February 26, 2019

Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Committee, thank you for the opportunity to discuss protecting consumer privacy in the era of Big Data. It is an honor. I am heartened by your bipartisanship on this important issue.

My testimony is informed by working in this field for more than a decade, including at a European university. My academic research explores online privacy as a comprehensive framework incorporating institutions, business practices, the type of technologies, and, most important, the level of the user's knowledge.[1] As a mother of three Danish-American children, I also have a personal interest in whether the European rules work.

My goal is for Congress to learn about the results of the General Data Protection Regulation (GDPR), avoid its mistakes, and ultimately leapfrog Europe with a better framework. In this testimony, I will discuss privacy-enhancing technology and competition, data security, the importance of a strong federal standard, and the role of consumer education.

How Privacy-Enhancing Technologies Can Promote Competition

Many Americans are persuaded by lofty descriptions of the GDPR—contrasting the legislation with what they see as a morally inferior laissez faire approach at home—both because they confuse data privacy and protection and because they are not familiar with America's own substantive protections. Journalists and commentators glibly refer to the US as the "Wild West," as if there are no laws or regulation on data privacy and protection.[2] In fact, there are literally hundreds of laws relating to privacy and data protection in the US—including common law torts, criminal laws, evidentiary privileges, federal statues, and state laws.[3] The EU's laws are relatively new, officially dating from this century, and they still lack the runway of judicial scrutiny and case law that characterizes US law.

A popular misconception about the GDPR is that it protects privacy; it does not. In fact, the word "privacy" does not even appear in the final text of the GDPR, except in a footnote.[4] Rather, the GDPR is about data protection or, more correctly, data governance.[5] Data privacy is about the use of data by people who are allowed to have it. Data protection, on the other hand, refers to technical systems that keep data out of the hands of people who should not have it. By its very name, the GDPR regulates the processing of personal data, not privacy.

The American notion of privacy is predicated largely on freedom from government intrusion and as a counterweight to the growth of the administrative state.[6] The Bill of Rights' Third, Fourth, and Fifth Amendments responded to the egregious British abuses of personal privacy, including the quartering of soldiers in private homes, the search and seizure of colonists' property, and forcing colonists to divulge information. Some of the first laws in the new republic were enacted

to protect privacy in mail. These were followed by laws constraining the government's use of the census[7] and its ability to compel information in court.[8] The 1966 Freedom of Information Act ensured that people could access records held by the government. Given this history of pushing back against government intrusion, it is reasonable to be skeptical that increasing government power is now the key to privacy in the US.

To analyze a policy like the GDPR, we must set aside the political pronouncements and evaluate its real-world effects. Since the implementation of the GDPR, Google, Facebook, and Amazon have increased their market share in the EU.[9] In spite of some years of notice about the GDPR's coming implementation, only 20 percent of EU companies, primarily the large firms, are digitized.[10] There is little to no data that shows that small to medium sized companies are growing in the EU as a result of the regulation.[11] The European Commission's Digital Scoreboard reports shows a consistent lag in the SME segment, particularly to modernize their websites and market outside their own EU countries.[12] One study suggests that small- and medium-sized ad tech competitors have lost up to one-third of their market position since the GDPR took effect.[13] The GDPR does not bode well for cutting-edge firms, as scientists describe it as fundamentally incompatible with artificial intelligence and big data.[14] This is indeed a perverse outcome for a regulation that promised to level the playing field.

But for those who study the empirical outcomes of regulation, it is not a surprise. As Nobel Prize Economist George Stigler observed more than 40 years ago, "Regulation is acquired by industry and operated for its benefit."[15] The GDPR is a barrier to market entry that punishes small firms, rewards large ones, and creates a cozy relationship between regulators and the firms they regulate.

To do business in the EU today, the average firm of 500 employees must spend about $3 million to comply with the GDPR.[16] Thousands of US firms have decided it is not worthwhile and have exited.[17] No longer visible in the EU are the *Chicago Tribune* and the hundreds of outlets from Tribune Publishing.[18] This is concerning because the EU is the destination of about two-thirds of America's exports of digital media, goods, and services.[19] Indeed, the GDPR can be examined as a trade barrier to keep small American firms out so that small European firms can get a foothold.[20]

Of course, $3 million, or even $300 million, is nothing for Google, Facebook, and Amazon (The Fortune 500 firms have reportedly earmarked $8 billion for GDPR upgrades.[21]), but it would bankrupt many online enterprises in the US. Indeed, less than half of eligible firms are fully compliant with the GDPR; one-fifth say that full compliance is impossible.[22] The direct welfare loss is estimated be about €260 per European citizen.[23] If a similar regulation were enacted in

the US, total GDPR compliance costs for US firms alone could reach $150 billion, twice what the US spends on broadband network investment[24] and one-third of annual e-commerce revenue in the US.[25]

The GDPR has affected not just American media outlets, but also their advertisers. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance with the GDPR has caused ripple effects in ancillary markets. Independent ad exchanges noted prices plummeting 20 to 40 percent.[26] Some advertisers report being shut out from exchanges.[27] The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third-party chipmakers, component suppliers, and software vendors that have never interfaced with end users, as European courts have ruled that any part of the internet ecosystem can be liable for data breaches.[28]

Many American retailers, game companies, and service providers no longer operate in the EU. The Williams-Sonoma and Pottery Barn websites are dark.[29] The San Francisco–based Klout, an innovative online service that used social media analytics to rate its users according to online social influence, closed down completely.[30] Drawbridge, an identity-management company from San Mateo, California, exited the EU and sold off its ad-tracking business because of the GDPR.[31] Verve, a leading mobile marketing platform with offices in six US cities, closed its European operation in advance of the GDPR, affecting 15 EU employees.[32]

Valve, an award-winning video game company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance.[33] Uber Entertainment, also based in Washington, similarly shut down one of its most popular games entirely after a six-year run because upgrading the platform to GDPR compliance was too expensive.[34] California-based Gravity Interactive no longer offers games in the EU and refunded its European customers.[35]

The Las Vegas–based Brent Ozar Unlimited, which offers a range of information technology and software support services, stopped serving the EU.[36] San Francisco's Payver, the dashboard camera app that pays drivers to collect road information on potholes, fallen road signs, and other inputs to build maps to improve the safety of self-driving cars, no longer supports the EU.[37] Legal news website Above the Law describes the EU closures of Ragnarok Online, Unroll.me, SMNC, Tunngle, and Steel Root, noting that the GPDR is splintering the internet and that GDPR policymakers refused to listen to concerns from startups before the launch and now refuse to fix its problems.[38] Even the Association of National Advertisers website is not available in the EU.[39]

The regulation has hurt European venture capital. An important study published by the National Bureau of Economic Research and coauthored by the Federal Trade Commission's (FTC) former chief economist notes a $3.38 million decrease in total dollars raised per country per week from

July 2017 to September 2018, a 17.6 percent reduction in weekly venture deals, and a 39.6 percent decrease in the amount raised per deal. The numbers are associated with between 3,000 and 30,000 job losses.[40]

The GDPR might be justified if it created greater trust in the digital ecosystem, but there is no such evidence. After a decade of GDPR-type regulations—in which users endure intrusive pop-ups and disclosures on every digital property they visit[41]—Europeans report no greater sense of trust online.[42] More than half of survey respondents in the United Kingdom say that they feel no better off since the GDPR took effect and that it as not helped them understand how their data is used.[43] As of 2017, only 30 percent of Europeans shop outside their own country (a paltry increase of 10 percent in a decade), demonstrating that the European Commission's Digital Single Market goals are still elusive.[44]

The other misconception of the GDPR is that its grab bag of 45 enterprise regulations magically delivers consumer protection, but these have not been tested scientifically. Regulation ensures compliance to an explicit mandated standard, not consumer protection, something that by definition varies from person to person. As such, I am similarly skeptical of the California Consumer Privacy Act (CCPA), which has even more enterprise requirements—77.

Indeed, if EU and California provisions were so laudable, why are we not demanding that American government institutions also uphold these standards? Such rules would likely cripple, both logistically and financially, the hundreds of personal data-collection agencies of the federal government and thousands in state and local government. With the mantra of "if in doubt, opt out," about half a million Australians rejected that country's national electronic health record, causing the federal computer system to crash in July 2018 and casting doubt on the underlying economics of the model.[45]

What then can policymakers do to ensure that policies promote competition? For one, they can ensure that the privacy framework does not unduly burden small and medium sized firms. Policies should focus on proven, legitimate practices that can prevent harm, not require compliance for a laundry list of "designer" provisions.

If anything, the policy should promote firms to use data. Indeed, the trouble with today's economy is not that there is too much use of data, but too little. A lack of "information intensity" is holding back the so-called other 70 percent of American economy, sectors such as transportation and health care, the latter of which consumes almost one-fifth of gross domestic product.[46] Outside of certain applications, the traditional healthcare industry is woefully inefficient; digital industries are 8 times more productive and innovative. If the US does not innovate these other sectors, other nations will beat us to it. China is already on track with an "Internet Plus" policy

which supports the digitization of industries, including healthcare and government.[47]

Ideally we need a technologically neutral national framework with a consistent application across enterprises. It should support consumers' expectations to have same protections on all online entities.[48] The law should make distinctions between personally identifiable information which deserves protection, but not require same high standard for public data, de-identified, and anonymized data which do not carry the same risks. Unlike the GDPR, the US policy should not make it more expensive to do business, reduce consumer freedom, or inhibit innovation.

Some of America's greatest resources are intellectual capital and creative ingenuity. We should build on our technology prowess to create world-class, scientifically superior privacy design. There are hundreds of privacy-enhancing technologies.[49] No one technology is best for all companies, and in practice, companies use a mix of technologies. Congress should incentivize the development of such technologies through grants and competitions and provide safe harbors for their research, development, and practice.

Congress should also be wary of mandates that all companies use the same technology, it removes the means for companies to compete and their incentive to innovate a better technology. Moreover, a monoculture of mandated technology is an attack surface for cyber criminals.

I commend the work by the National Institute of Standards and Technology to inform this effort.[50] Moreover, the FTC's budget and authority should be expanded to accommodate the needed economists, technologists, and other professionals to enforce privacy protections. Presently, the FTC has a mere 80 economists and 800 attorneys. The consumer-protection function of the FTC should be strengthened by aggregating the consumer protection resources now frittered across a series of federal agencies and consolidating them under one roof at the FTC.[51]

The Role of Data Security

I have noted the security fallout from the GDPR,[52] but there are even more fundamental security problems. In their rush to declare moral superiority over the US, European policymakers disregarded the existential threats to privacy by network hardware manufacturers Huawei, ZTE, and Lenovo.[53] European authorities, wanting to get networks cheaply, blessed the construction of communications networks with equipment from dubious Chinese vendors. Data-protection standards mean little if affiliates of the Chinese government and military can access our data in the cloud, through backdoors, by hacking, or through other illicit means.

Fortunately, the US does not have this problem to the same extent. The US recognized the risk at the outset, understood that security is worth paying for, and limited its exposure to these firms. I applaud Congress for its leadership with H.R. 4747,[54] and I hope it stays the course. I

also support the role of cyber insurance to help firms assess and address security risks.[55]

How Common Standards Ensure Equal Privacy Protections for All Americans

The GDPR was created to bring a single standard of data protection to the EU. If each US state makes its own rules, we will become the Balkanized Europe, which the GDPR sought to remedy. The idea of a single national market is central to America's founding and was espoused by James Madison and Alexander Hamilton.[56] This framework was essential for our country to launch and commercialize the internet economy, and today the US accounts for one-third of the world's internet economy.[57] In the process of adjudication of privacy violations, it is not fair that residents of some states get payouts while others do not. America's internet companies are national, if not global, so enforcement must proceed federally from the FTC to ensure fairness. Importantly, Congress should adopt safeguards against rent-seeking by self-interested actors to abuse consumer protection laws to enrich themselves through litigation.

The Role of Consumer Education and Meaningful Transparency

My final point is the most important: There is no consumer protection without consumer education. After a decade of increasing data-protection regulation in the EU, Europeans do not report greater trust online. This is because the EU substitutes the *bureaucratization of data protection* for the *natural right of privacy*. Increasing the number of agencies and bureaucrats who govern our data does not increase our privacy.

Moreover, making a disclosure more explicit does not give us more privacy. Our policy should support the ability for people to acquire digital competence so that they can make informed decisions about the online products and services they use. People are empowered through education, not bureaucratization.[58]

While we may experience a general creepiness about growing technology, it is not inherently harmful to collect and process data from individuals and give them incentives to share. Indeed, it does not appear that policymakers have identified, let alone quantified, the harm that proposed legislation would mitigate. Moreover, there are significant costs associated with regulation, and benefits do not flow equally to consumers. While some may appreciate the regulator's heavy hand, many will find it intrusive.[59] The FTC's unfairness test with its precepts of informational injury as it applies to deception (which subverts consumer choice), financial, health/safety, unwarranted intrusion, and reputation could be a helpful tool in this regard.

Upon introduction, new technologies such as the camera, transistors, and RFID chips creeped

people out, but these technologies have tremendously benefited our society. This privacy panic cycle of trust, panic, deflation, and acceptance is well-documented for more than a century.[60] When asked which has most improved life in the past 50 years, Americans note technology more than four times as often as medicine, civil rights, or the economy.[61]

Regulatory advocates may be noble and well-intentioned in their desire to protect consumers, but regulation is never neutral. It is subject to biased human decision-making and interpretation. Nor is regulation necessarily quick or effective. GDPR policymakers claim that it will be at least two years to conclude a major enforcement.[62] Moreover, California, which before its CCPA already had more privacy laws than any state, does not report that its residents felt more safe, private, or secure.

I applaud President Barack Obama's leadership on his 2012 Online Bill of Rights for Consumers (and, indeed, the provisions are not controversial today).[63] Hundreds of privacy enforcements have been made over the years, however, it appears that certain consent decrees against major Silicon Valley companies were not enforced during his administration. Americans should not have to rely on the whims of political administrations to protect themselves. Americans should be able to choose increasingly better privacy-enhancing technologies that are divorced from politics. Moreover, the more educated people are about the technologies they use, they less they need regulators to choose for them.

I humbly submit that Congress review the empirical research on privacy and data protection that the Europeans ignored, notably the process for innovation in privacy-enhancing technologies and the primacy of user knowledge as a component of online trust.[64] The US does not need to copy the European Union on data protection. It can fundamentally improve on the GDPR by making a policy that actually works—promoting privacy without destroying prosperity, empowering people to make informed decisions, and ensuring innovators the freedom to invent and improve privacy-enhancing technology.

---

[1] Roslyn Layton, "How the GDRP Compares to Best Practices for Privacy, Accountability and Trust," March 31, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.
[2] See, for example, Joe Nocera, "The Wild West of Privacy," *New York Times*, February 24, 2014, https://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html.
[3] See Daniel J. Solove, "A Brief History of Information Privacy Law," in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, ed. Kristen J. Mathews (New York, Practising Law Institute, 2006).
[4] European Union, General Data Protection Regulation, note 18, https://gdpr-info.eu/.
[5] Evidon, "What Is the GDPR?," https://www.evidon.com/education-portal/videos/what-is-the-gdpr/.
[6] See Solove, "A Brief History of Information Privacy Law," 1-5, 1-6.
[7] See Solove, "A Brief History of Information Privacy Law," 7.
[8] See, for example, *Boyd v. United States*, 116 US 616 (1886).

[9] Mark Scott, Laurens Cerulus, and Laura Kayali, "Six Months in, Europe's Privacy Revolution Favors Google, Facebook," *Politico*, November 27, 2018, https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/.
[10] European Commission, "Integration of Digital Technology," 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf.
[11] https://ec.europa.eu/digital-single-market/en/digital-scoreboard
[12] European Commission, "Better Access for Consumers and Business to Online Goods," 2015, https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods.
[13] Björn Grelf, "Study: Google Is the Biggest Beneficiary of the GDPR," Cliqz, October 10, 2018, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.
[14] For further discussion on how GDPR blocks innovation, see Roslyn Layton and Julian Mclendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," *Federalist Society Review* 19 (October 29, 2018): 245, https://fedsoc-cms-public.s3.amazonaws.com/update/pdf/nv29MXryrqablN7n8h6WzAJ9yhbZBKITKOM-wMzVe.pdf.
[15] George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics* 2, no. 1 (1971): 3–21.
[16] International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018," 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.
[17] Jeff South, "More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect," Nieman Lab, August 7, 2018, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.
[18] Barbara Kollmeyer, "Chicago Tribune, Los Angeles Times Go Dark in Europe After GDPR Fail," MarketWatch, May 25, 2018, https://www.marketwatch.com/story/chicago-tribune-la-times-go-dark-in-europe-after-gdpr-fail-2018-05-25.
[19] US International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, https://www.usitc.gov/publications/332/pub4716_0.pdf.
[20] Daniel Lyons, "GDPR: Privacy as Europe's Tariff by Other Means?," AEIdeas, July 3, 2018, http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.
[21] https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
[22] International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018."
[23] Hosuk Lee-Makiyama, "The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs," in *Protection of Information and the Right to Privacy—A New Equilibrium?*, ed. Luciano Floridi (Springer, 2014), 85–94. This methodology is expanded in Erik Van der Marel et al., "A Methodology to Estimate the Costs of Data Regulations," *International Economics* 146 (2016): 12–39.
[24] Jonathan Spalter, "Broadband CapEx Investment Looking Up in 2017," USTelecom, July 25, 2018, https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017.
[25] US Census Bureau, "Quarterly Retail E-Commerce Sales 1st Quarter 2018," May 17, 2018, https://www2.census.gov/retail/releases/historical/ecomm/18q1.pdf.
[26] Jessica Davies, 'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers, Digiday (June 4, 2018), https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.
[27] Catherine Armitage, "Life After GDPR: What Next for the Advertising Industry?," World Federation of Advertisers, July 10, 2018, https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/.
[28] European Union, Judgment of the Court (Grand Chamber), June 5, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN.
[29] Associated Press, "Amid Confusion, EU Data Privacy Law Goes into Effect," WTOP, May 25, 2018, https://wtop.com/news/2018/05/amid-confusion-eu-data-privacy-law-goes-into-effect/.
[30] Jon Russel, "RIP Klout," TechCrunch, May 2018, https://techcrunch.com/2018/05/10/rip-klout/.
[31] Allison Schiff, "Drawbridge Sells Its Media Arm and Exits Ad Tech," AdExchanger, May 8, 2018, https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/.
[32] Ronan Shields." Verve to Focus on US Growth as It Plans Closure of European Offices Ahead of GDPR," Drum, April 18, 2018, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr.
[33] Steam, "Super Monday Night Combat," https://steamcommunity.com/app/104700/allnews/.

[34] Owen Good, "Super Monday Night Combat Will Close Down, Citing EU's New Digital Privacy Law," Polygon, April 28, 2018, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr.
[35] Warportal, "Important Notice Regarding European Region Access," http://blog.warpportal.com/?p=10892.
[36] Brent Ozar, "GDPR: Why We Stopped Selling Stuff to Europe," December 18, 2017, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.
[37] Payver (@getpayver), "Sorry European Payver users! Come May 24th we're discontinuing Payver support in Europe due to #GDPR. Talk to your lawmakers...,"Twitter, April 5, 2018, 5:30 p.m., https://twitter.com/getpayver/status/981992477392437249.
[38] Techdirt, "Companies Respond to the GDPR by Blocking All EU Users," Above the Law, May 11, 2018, https://abovethelaw.com/legal-innovation-center/2018/05/11/companies-respond-to-the-gdpr-by-blocking-all-eu-users/.
[39] George P. Slefo, "ANA Doesn't Have GDPR-Compliant Website; Says It Will Be up in 'Two Weeks,'" AdAge, June 7, 2018, https://adage.com/article/digital/ana-misses-deadline-create-gdpr-compliant-website/313775/.
[40] Jian Jia, Ginger Zhe Jin, Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment" (working paper, National Bureau of Economic Research, November 2018), https://www.nber.org/papers/w25248
[41] GDPR pop-up disclosures have become so intrusive that Europeans download pop-up blockers on their phones.
[42] Daniel Castro and Alan McQuinn, "The Economic Cost of the European Union's Cookie Notification Policy," Information Technology & Innovation Foundation, November 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.
[43] GDPR three months on: Most consumers feel no better off. Marketing Week. Lucy Tesseras 24 August 2018. https://www.marketingweek.com/2018/08/24/gdpr-three-months-on/?ct_5bf3f166954e0=5bf3f16695585
[44] European Commission, "Use of Internet Services," 2018, 4, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf.
[45] Layton and Mclendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course."
[46] Bret Swanson. "Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation." Summary of Forthcoming Report. AEI. February 2019.
[47] http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm
[48] http://www.aei.org/publication/fcc-privacy-regulation-will-limit-competition-market-really-needs-online-advertising/
[49] For a discussion of privacy enhancing technologies, see Roslyn Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions of Online Privacy," August 20, 2018, 8, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf
[50] See US Department of Commerce, National Institute of Standards and Technology, "Cybersecurity Framework," https://www.nist.gov/cyberframework; and US Department of Commerce, National Institute of Standards and Technology, "Privacy Framework," https://www.nist.gov/privacy-framework.
[51] See Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings," 7.
[52] See Layton and Mclendon Supra 41, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," 246. The GDPR has created an existential security threat for the WHOIS database, a key internet function. "In addition, misapplication of the GDPR is hindering commerce and consumer protection because domain name providers are using it as an excuse to restrict access to WHOIS data, not just in the EU but also in the US and elsewhere. WHOIS data has been publicly available since the dawn of the commercial internet. It provides basic contact information for holders of domain names and is critical for online trust and accountability. Consumers and businesses use WHOIS data to confirm who is on the other side of web sites they engage with. Law enforcement agencies and other groups use WHOIS data to combat identity theft, theft of intellectual property, cyberattacks, illicit sale of opioids, sex trafficking, and other clearly illegal conduct online. ICANN's Government Advisory Committee and law enforcement agencies across the globe are already warning that consumer protection and criminal investigations are being stymied. Congress should consider requiring domain name providers to make the same WHOIS data available that they gave been providing for more than 20 years."

[53] Roslyn Layton, "Trump Should Ignore Chinese Manufacturers' Phony Promises," *Forbes*, February 20, 2019, https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignore-chinese-manufacturers-phony-promises/#257b924d50ec.
[54] Defending U.S. Government Communications Act, H.R. 4747, 115th Cong., https://www.congress.gov/bill/115th-congress/house-bill/4747.
[55] Hurwitz, Justin (Gus), Cyberensuring Security (September 1, 2017). Connecticut Law Review, Vol. 49, No. 5, 2017. Available at SSRN: https://ssrn.com/abstract=3314400
[56] Roslyn Layton, "California's Privacy Proposal Failed, but It Probably Violated the Constitution Anyway," AEIdeas, September 18, 2017, http://www.aei.org/publication/californias-privacy-proposal-failed-but-it-probably-violated-the-constitution-anyway/. For an abbreviated version, see Roslyn Layton, "Internet Privacy Legislation," American Enterprise Institute, http://www.aei.org/multimedia/internet-privacy-legislation-in-60-seconds/.
[57] CompTIA, "IT Industry Outlook 2018," January 2018, https://www.comptia.org/resources/it-industry-outlook-2018.
[58] For a discussion of online privacy education, see Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings," 12.
[59] A forthcoming event will describe the costs and benefits of digital rights, data protection, and data privacy. Society for Benefit-Cost Analysis, 2019 Annual Conference, March 13–15, 2019, https://benefitcostanalysis.org/2019-annual-conference.
[60] Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology & Innovation Foundation, September 2015, http://www2.itif.org/2015-privacy-panic.pdf.
[61] Mark Strauss, "Four-in-Ten Americans Credit Technology with Improving Life Most in the Past 50 Years," Pew Research Center, October 12, 2017, http://www.pewresearch.org/fact-tank/2017/10/12/four-in-ten-americans-credit-technology-with-improving-life-most-in-the-past-50-years/.
[62] Jan Philipp Albrecht, "Press Conference by Jan Philipp Albrecht (Greens/EFA, DE), Rapporteur, on General Data Protection Regulation," European Parliament, June 15, 2018, https://multimedia.europarl.europa.eu/en/albrecht-general-data-protection-regulation_I155149-A_ra.
[63] Roslyn Layton, "A Look at the Growing Consensus on Online Privacy Legislation: What's Missing?," AEIdeas, October 29, 2018, http://www.aei.org/publication/a-look-at-the-growing-consensus-on-online-privacy-legislation-whats-missing/.
[64] European Union Agency for Network and Information Security, *Privacy and Data Protection by Design—From Policy to Engineering*, December 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.