Questions for the Record before the Senate Judiciary Committee
On the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation

Roslyn Layton
Visiting Scholar

April 3, 2019

Chairman Graham, Ranking Member Feinstein, and Members of the Committee, thank you for the opportunity to provide additional testimony for the record. Please find my answers to your questions. For ease of reading, the answers to the questions are organized by the respective committee member.

Questions for the Record from Sen. Lindsey Graham (R-SC)

Sen. Graham: What are the specific areas of the CCPA that could have a negative impact on competition and innovation? What areas of the CCPA need more clarity, improvement, or removal?

Layton:
The CCPA and any kind of privacy legislation will need to overcome the following issues

1. Violation of free speech as described in ***Sorrell v. IMS Health Inc.***, 564 U.S. 552 (2011).
2. The Dormant Commerce Clause
3. Standing to sue *Spokeo*, Inc. v. Robins, 578 U.S. ___ (2016)

Following are the specific problems with the CCPA. These are also detailed in other testimonies.[1]

- Personal information is defined too broadly. A good definition of personal information should be narrow and limited to specific discrete categories of personal information and should explicitly exclude de-identified and aggregated data
- The CCPA defines "sale" expansively, covering many commonplace practices that businesses rely on to provide goods and services to consumers. More generally, there are millions of nonprofit services not engaged in sales at all, but rather downloads of white papers, sign-ups for events, and so on. These activities should not be construed as "sales."
- There is a prohibition on differing service based on consumer privacy choices. This is likely a regulatory takings. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups and nonprofit organizations
- There are privacy and security problems with CCPA's right to access and delete that create opportunities for fraud or needless requirements for additional data collection.
- The private right of action creates uncertainty for startups. No matter how thorough a company's data security practice safe, determining whether they were legally "reasonable" is not amenable to early adjudication in a lawsuit.
- The CCPA's small business exemption fails to capture startups.
- The design and procedure of the opt-out function does not sync with startups practices.
- The CCPA imposes significant compliance burdens for the diverse business models represented in California's startup ecosystem.

- In total, the sheer length and complexity of the CCPA is daunting, even for certified privacy professionals.
- The CCPA was hastily prepared to avoid review as a ballot measure.

A leading Santa Clara University law professor and more than 40 California based privacy professionals and lawyers attest to the hasty, sloppy process to make the law.[2] The view that the CCPA was hastily pasted together is also the Senate testimony of Evan Engstrom, executive director of Engine Advocacy and Research Foundation in San Francisco. He noted to the Senate Commerce Committee:

> While CCPA's objectives are laudable, the process leading to its passage was not. Although the ballot initiative's authors clearly spent considerable time on their proposal, the legislature spent less than a week translating the initiative's general ideas into actual bill text. As a result, California legislators were unable to fully evaluate the bill, its impact on California's startup community, or its actual value to consumers. This rushed process resulted in a well-intentioned law that is full of typos, contradictions, security loopholes, and vague obligations.[3]

Pam Dixon of the World Privacy Forum who has studied privacy for more than 25 years noted that the CCPA reflects essentially the preference of a single privacy advocate and did not take into account the multi-stakeholder process.[4]

Congress should scrap the CCPA. It is a European control-based regime that is not appropriate for the dynamic American system. The US should reboot its efforts with a trust-based system.

Questions from Sen. Charles Grassley (R-IA)

Sen. Grassley: Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.

Layton: The foundations of a market economy include good information, which allows actors to make informed decision. Much of the premise of regulation is to compel disclosure to reduce the problem of informational asymmetry, in which one actor has information that the other does not. As such, enforcing transparency provisions (or violations or deceptions) thereof may be the single most important part of any privacy legislation. Indeed, the Federal Trade Commission is already empowered with this capability.

Sen. Grassley: Often times, comprehensive regulations end up just benefiting the large, entrenched entities that have teams of lawyers to ensure compliance. Should small businesses be treated differently in any federal data privacy framework? And if so, how?

Layton: It is absolutely the case the regulation has benefited the large, entrenched entities to the detriment of innovators.[5] My testimony details the perverse outcomes of the GDPR, helping big business and hurting small business. Moreover, most privacy legislation proposals have been designed with giant firms in mind, making it inappropriate for small- and medium-sized enterprises. The solution for a common framework is to pursue as trust-based approach with standards.

Sen. Grassley: If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just "check the box" of regulatory compliance?

Layton: Congress should ensure safe harbors for entities to develop and test privacy-enhancing innovation and to protect law-abiding firms that are doing right by their customers. Congress can also explore incentives for privacy enhancing innovation, which I describe on page 11 of my testimony.[6]

Sen. Grassley: How do we best craft a federal data privacy law that keeps pace with our ever-evolving tech and data landscape? And can we do that without giving unfettered discretion to the regulators?

Layton: Multistakeholder governance and soft law are the best solutions to these two challenges. Consider how the Organization for Cooperation and Economic Development has developed standard for artificial intelligence.[7] See further Hagemann, Ryan and Skees, Jennifer and Thierer, Adam D., Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future (February 5, 2018). Forthcoming - Colorado Technology Law Journal . Available at SSRN: https://ssrn.com/abstract=3118539

Questions From Sen. Mazie Hirono (D-HI)

Sen. Hirono: In your written testimony, you claim that "[i]f the GDPR were adopted in the U.S., it would likely violate the First Amendment, as the requirements for data processing are so onerous that they would be found to limit expression."

Please explain what you mean by this.

Layton: The data of websites—their words, pictures, and codes—are speech. The First Amendment clearly states, "Congress shall make no law . . . abridging the freedom of speech, or of the press." If the government adopts so many regulations for operating websites that it leads to the shuttering of websites, or the lessening of websites, then the regulation can be construed as abridging the freedom of speech. The case has already been exemplified with the more than

1,000 US news outlets that no longer serve the EU because of the cost and complexity of the GDPR.[8]

Here the case of *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974) is instructive. The Supreme Court overturned a Florida state law requiring newspapers to allow equal space in their newspapers to political candidates in the case of a political editorial or endorsement content. In effect the state law was making the operation of newspaper so expensive that it abridged speech; the newspaper had to buy extra ink and paper to comply with the law. It is not so different when compelling a company to hire the services of a web design firm, to purchase software, or to hire an employee with specialized experience. All of these serve to increase the cost of operation to fulfill a government requirement. The costs are so onerous such that the newspaper must reduce content or go out of business to comply, hence this shows the abridgement of speech. The court held that while the statute does not "prevent [newspapers] from saying anything [they] wish," it "exacts a penalty on content.' Because newspapers are economically finite enterprises, "editors may conclude that the safe course is to avoid controversy," thereby chilling speech.

Jane Bambauer observes:

> When the scope of First Amendment coverage is ambiguous, courts should analyze the government's motive for regulating. Second, it highlights and strengthens the strands of First Amendment theory that protect the right to create knowledge. Whenever the state regulates in order to interfere with the creation of knowledge, that regulation should draw First Amendment scrutiny. In combination, these claims show clearly why data must receive First Amendment protection. When the collection or distribution of data troubles law-makers, it does so because data has the potential to inform and to inspire new opinions. Data privacy laws regulate minds, not technology. Thus, for all practical purposes, and in every context relevant to privacy debates, data is speech.[9]

Similarly, the CCPA appears to compel speech both in requiring a firm to have an 800 number and to post it in a conspicuous place on the home page in addition to other CCPA information.

Sen. Hirono: Do you have the same concern about the California Consumer Privacy Act?

Layton: Yes.

Sen. Hirono: In your written testimony, you called for greater privacy education for consumers. Right now, users are largely left to their own devices to wade through lengthy privacy policies that are often written in dense, legal language. A 2008 study found that it would take the average American 76 days to read the privacy policies of the websites they visit.

How do you think this problem can be improved? What types of privacy education do you have in mind?

Layton: I support the effort to make privacy policies shorter, clearer, and more customer centric. Even with improved policies, there is still a role for consumers to be educated. I discuss this on p. 12 in a testimony I gave.[10]

Questions from Sen. Ben Sasse (R-NE)

Sen. Sasse: Aside from situations in which compliance costs lead to higher product prices and foregone spending on research and development, in what ways is CCPA affecting Americans outside of California?

Layton: Additional impacts were described in a recent Senate hearing,[11] including reduced effectiveness of online products and services (for example, homeowners suffering reduced capability to property estimate the value and price for a home sale).

Sen. Sasse: Which types of sites, apps, and platforms are able to provide different user experiences between California and the rest of the country in a manner that is technologically feasible and cost-effective? Which are not?

Layton: Google has the best ability to tailor its experience individually to each individual user; indeed, this may well be its competitive differentiator—its combination of human and machine learning to make each search inquiry relevant for the user. Facebook and Amazon also engage in personalization. This capability requires the deployment of a sophisticated set of web analytic, behavioral, multivariate, and other tools. The platforms have many proprietary tools to do this. Competing platforms may license tools from individual web analytics providers. Ironically those tools that could enable customization and differentiate based on location are being hammered by the General Data Protection Regulation (GDPR). This is precisely what is going on when describing how and why the GDPR has benefited Google, Facebook, and Amazon, which have their own proprietary tracking tools, but the competing ad tech tools have been kicked off content websites.[12]

Sen. Sasse: What is a principles way we can think about the possibility of federal preemption in the data privacy context? When is not appropriate to let states regulate as they wish, even if we disagree with their policy choices? In what situations should we be comfortable with letting one state drive nationwide policy as a practical matter?

Layton: California's imposition of privacy rules for the internet, a service that transcends state boundaries, triggers constitutional concerns for interstate commerce and supremacy. Notably Article I of the Constitution regulates commerce among the states. It also notes that no preference should be given to any state's regulation and that all state laws are subject to revision and control of Congress. The purpose of these rules was to maintain the single national market of the United States, and it turned out to be essential for the US to commercialize the internet.

It could be appropriate for California to regulate privacy if it could certify that the particular internet communication both originated and terminated within the state, but this would likely require California authorities to engage in deep-packet inspection.

Sen. Sasse: To what extent has GDPR deprived European users from accessing particular types of content on the internet?

Layton: The most impacted content has been news. The number of news outlets has been drastically reduced. See my response to Sen. Hirono.

Sen. Sasse: Which aspects of GDPR, CCPA, and proposed aspects of potential federal legislation most worry you in terms of protecting incumbents in particular markets and creating major barriers to entry for new firms?

Layton: See next question.

Sen. Sasse: Which aspects of GDPR, CCPA, and proposed aspects of potential federal legislation most worry you in terms of harming innovation? How much should we worry about regulation hampering innovation in the West and giving China a competitive advantage in the development of new technology such as artificial intelligence?

Layton: Please see the response to Chairman Graham.

China is already ahead for many reasons. Notably, we have lost a decade fighting over internet regulation, being distracted by elitist issues. China has selected national champions and blocks US competitors. Please see my testimony to the Senate Commerce Committee on Internet Governance directly addressing this issue.[13]

Sen. Sasse: In terms of the different proposals for giving the Federal Trade Commission new rulemaking authority, how should we think about balancing between ensuring flexibility to adapt a regulatory framework to fit emerging technologies and avoiding delegation of what should be lawmaking authority properly exercised by Congress to a "fourth branch" of government?

Layton: It is correct that we should be wary of overreach by administrative agencies. The mention of the "fourth branch" describes how a class of unelected bureaucrats exert an outsized influences on the lives of Americans and the economy. Indeed the FTC itself was censured for exceeding its statutory authority and was branded the national nanny. Notably the FTC was then required by operate by Magnuson-Moss rulemaking which imposes a significantly higher bar than the Administrative Procedure Act. As we saw with the 2015 FCC's foray into online privacy rules, an agency can invent privacy rules without any record of harm to achieved advocates preferred social or policy outcomes.[14]

does not discount knowledge of FTC. Very narrowly tailored. Worthy to ask FTC for more information before giving them rulemaking capability.

Sen. Sasse: Do you foresee any situations in which data portability requirements actually enhance some firms' abilities to build more data-rich profiles of individual users?

Layton: The value of data portability is overestimated as a policy instrument for innovation. It is highly unlikely to expect data portability to create a knock-off search engine or social network. Innovators and investors are looking for solutions that are better and different. Some academic background is in order. One should not conflate "number portability" with data portability; the former respects a specific, identical service. The efficacy of data portability depend on whether services are substitutes or complements.[15] Moreover platforms such as search engines, social networks, and marketplaces have different kind of dynamics, e.g. the degree to which a new user creates a network effects and economies of scale. For example, users on search engines don't engage with each other as they do on social networks. Data ported from a marketplace does not necessarily map to a social network.

Sen. Sasse: Do you foresee any situations in which opt-in requirements actually increase the amount and types of data that firms collect from individual users?

Layton: Yes, this has been the experience of Do Not Track.[16]

Sen. Sasse: To what extent do you think privacy policies and user agreements are drafted deliberately to dissuade users from closely reading them?

Layton: While one can imagine such a motivation and outcome, for most startups they use privacy policies that are templates or purchase software systems that offer compliance to leading regimes. Ideally the proper framework will allow platforms to engage meaningfully with users about the tradeoffs of securing data.

Questions from Sen. Cory Booker (D-NJ)

Sen. Booker: Marginalized communities, and specifically communities of color, face a disproportionate degree of surveillance and privacy abuses. This has been the case since the Lantern Laws in eighteenth-century New York City (requiring African Americans to carry candle lanterns with them if they walked unaccompanied in the city after sunset) up through the stop-and-frisk initiatives of more recent years.

There are echoes of this tradition today in the digital realm as marginalized communities suffer real harm from digital discrimination. For example, in recent years we have seen many instances of housing discrimination and digital redlining, employment discrimination through digital profiling and targeted advertising, exploitation of low tech literacy through misleading notice and choice practices, discriminatory government surveillance and policing practices,

and voter suppression and misinformation targeting African Americans and other minorities.

I am concerned that—rather than eliminating the bias from our society—data collection, machine learning, and data sharing may actually augment many of the kinds of abuses we fought so hard to eliminate in the Civil Rights Movement. We need privacy legislation that is centered around civil rights.

In your view, is a private right of action critical to protecting the civil rights of individuals affected by data collection and disclosure practices?

Layton: The statement above suggests that people are subject to abuse because of being economically disadvantaged. If that is the case, then the answer is to improve people's economic situation through enterprise. Some have observed that the residents of New Jersey face systematic discrimination by the state government abridging individuals' rights and freedoms, and this has worsened in the past decade.[17] Indeed Newark is the third most needy city in the USA as measured by poverty, food insecurity, and homelessness.[18] These indicators suggest reasons why marginalized communities persist in New Jersey, notably because of rent control and similar regulation making land use inefficient. The state's wage controls discourage hiring, a regulation which falls hardest on the poor and minorities. Similarly, the inputs for running a home or business are unnaturally expensive because of state regulation whether electricity, telecommunications, occupational licensing, insurance, etc. It is notable that many residents of New Jersey (ranked 47th for economic freedom) are fleeing to Florida, the leading state for economic freedom.[19] While better weather is one reason, the high cost of living and the lack of jobs account for more of the migration.

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.[20] 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.[21]

A private right of action does not necessarily protect people. It has been well-documented how the litigation industry disproportionately rewards lawyers and litigation financiers over consumers.[22] However, consumer education to address what the question describes as "low-tech literacy" could be helpful. See page 12 of my testimony to the Federal Trade Commission (FTC) in which I describe how the FTC's existing privacy education resources can be leveraged, examples of curricula, and education distribution models.[23] The testimony highlights the scholarship of New Jersey's Seton Hall University to "train the trainer" on teaching privacy.

Sen. Booker: How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?

Layton: The FTC has made a detailed report on this issue.[24] There are a formidable set of laws already that protect against harmful discrimination, notably the Fair Credit Reporting Act and Equal Opportunity Laws. Indeed, there is a risk that regulation that reduces the amount of information for decision-making could create worse outcomes by increasing prices across the board to compensate for inaccuracies. This adverse outcome was found in a study of home loans in the San Francisco Bay Area in which counties that had the strictest privacy settings ended up paying more for mortgages and defaulting at a higher rate because the banks could not accurately match the applicant to the appropriate loan.[25]

Rather than restrict firms in their ability to use data, policy should encourage firms to improve the accuracy of their tools. Policy could also support improving the readability of disclosures on business practices and consumer education about how online platforms work (discussed in another QFR), so that consumers can make better decisions about the online platforms they use.

Importantly, the FTC report notes the importance of harnessing data practices for the betterment of the disadvantaged.

> Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap. . . . Therefore, to the extent that companies today misunderstand members of low-income, disadvantaged, or vulnerable populations, big data analytics combined with a competitive market may well resolve these misunderstandings rather than perpetuate them. In particular, a company's failure to communicate premium offers to eligible consumers presents a prime business opportunity for a competitor with a better algorithm. To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals.[26]

Improving the FTC's enforcement capabilities overall, notably with removing common carrier and nonprofit exemptions, increasing the FTC's budget and headcount for online privacy investigations and enforcement, and allowing the FTC to levy civil penalties, would be helpful in this regard.

Sen. Booker: Significant amounts of data about us are gathered by companies most people have never heard of. Do we need a registry of data brokers, similar to what Vermont established last year?

Layton: No.

Sen. Booker: The tech journalist Kashmir Hill recently wrote a widely circulated article on her efforts to leave behind the "big five" tech companies—Facebook, Google, Apple, Microsoft, and Amazon. Using a VPN, she blocked all of the IP addresses associated with each company and then chronicled how her life changed. She experimented first by blocking individual companies, and then, at the end of the series, she blocked all five at once. Ms. Hill found that—to varying degrees—she could not get away. Repeatedly, her efforts to intentionally block one company created unpredictable ripple effects for engaging with other, seemingly unrelated, companies and services. Ms. Hill's article spoke to how pervasive these companies are and how much data they capture about us when we're not even (knowingly) using their services.[27]

How would you respond to the following argument? "If people are uncomfortable with the data practices of certain tech companies, they simply shouldn't use their services."

Layton: Hill's article describes the many benefits and improved efficiencies consumers have realized as a result of online products and services, benefits consumers have received largely through declining costs. Indeed, Hill's experience intimates how much one would need to spend to purchase physical books, magazine and newspaper subscriptions, and vinyl records if there were not advertising-supported digital alternatives; the downsides of maintaining a paper address book over an online database; the limits of the plain old telephone network versus a modern smartphone, and so forth. Indeed Facebook alone is estimated to offer at least $48 of value which consumers would otherwise have to spend out of pocket. Indeed Hill described her life without Google, Facebook, Amazon, Apple, and Microsoft as "hell."

In point of fact, many people do not use the services of the Big Five. Remarkably, 20 percent of the American population does not use the internet primarlily because they do not believe the Internet to be valuable. However internet policy has long described the importance to connect the unconnected,[28] which ostensibly will allow them to enjoy the services of the Big Five. Indeed, connecting everyone to the internet, regardless of an individual's preference to do so, is a pillar of the Democratic Party.[29]

In any event, the facts show that users quit and switch services frequently. Hill Holliday's survey of Generation Z (those born since 1994) shows that so-called digital natives, who are estimated

to comprise 40 percent of US consumers by 2020 and of whom more than 90 percent use social media platforms, found that more than one-half had switched off social media for extended periods and one-third had canceled their social media accounts.[30] Users cited time wasting as the reason for quitting twice as often as a concern about privacy. While service providers do not like the high rates of churn on their platforms,[31] they are indicative of a competitive market in which consumers find it easy to leave and try other platforms with different features.

Sen. Booker: What does providing consent mean in a world where it's extremely difficult to avoid certain companies?

Layton: At least 20 percent of the US population is not online and therefore "avoids" certain companies. It is not consent that is necessarily the problem, but rather enforcement against violation of deceptive practices. These are issues that the FTC already has authority and capability to address with existing laws today.

Sen. Booker: Given that California has enacted its own privacy legislation that will take effect next year, much of the discussion at the hearing centered on how a federal data privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy statutes do not include provisions to overrule stricter protections under state law.[32] These preemption provisions are the exception rather than the rule and became more prevalent starting in the 1990s in statutes like the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.

In your view, should a federal data privacy law preempt state data privacy laws? Why?

In your view, should a federal data privacy law implement the requirements of the California Consumer Privacy Act as a floor? If not, please explain the most significant change you would suggest.

Layton:
The internet transcends state boundaries, and state level privacy laws frustrate the single national market our Constitution sought to create. State level internet privacy laws likely violate interstate commerce. Leading California privacy lawyers described the California Consumer Privacy Act (CCPA) as a hodge podge of provisions pasted together in a week and not justified to be adopted nationwide. Thankfully the federal government exists to protect citizens from the vicissitudes of zealous state actors. Therefore, it is necessary and proper that federal law preempts state law.

It is telling that the agencies of California government both at the state and local level have not voluntarily adopted the CCPA, which they tout as some magical, blissful standard. If their hope is to condition consumers to the California standard, there is no reason why the state government should not meet the same expectation demanded of companies, nonprofits, and other

institutions. Government collects significant personal and sensitive data, and unlike the marketplace where there are alternatives for many platforms and services, the government is the only choice for certain kinds of service, such as identification cards, driver's licenses, and so on. This regulatory asymmetry is indicative that the CCPA may an effort on the part of the California Attorney General to grab the power of litigation to ensure payouts to his state over the residents of other states. Preemption is also important to ensure that if there is litigation against internet platforms, that the payouts are enjoyed by all Americans, not just Californians.

Please see earlier responses which address this question.

Sen. Booker: The specific wording of a proposed preemption provision will invite considerable debate in Congress and, ultimately, will still require courts to interpret and clarify the provision's scope. The preemption language in, for example, the amendments to the Fair Credit Reporting Act was included as part of a heavily negotiated process in which consumers received a package of new rights in exchange for certain preemption provisions.[33] Rather than centering the federal privacy bill debate on the existence of a preemption provision, shouldn't our starting point be: "Preemption in exchange for what?" In other words, what basic consumer protections should industry stakeholders be willing to provide in exchange for preemption? Do the requirements of the California Consumer Privacy Act represent a good floor for negotiating preemption? Should the Federal Trade Commission have notice-and-comment rulemaking authority to aid in the statute's interpretation and to clarify which types of state laws are preempted? Or, alternatively, is case-by-case adjudication of multiple state privacy laws preferable? Would rulemaking authority obviate the need for Congress to solve each and every preemption issue in drafting the text?

Layton:
The interstate commerce and supremacy clauses of the Constitution are clear, and a federal policy of preemption is supported amply by case law. This need not invite debate and judicial challenge. However, the reality is that self-interested litigators challenge Constitutionally supported legislation, but this is not an excuse to avoid the proper policy preemption. Moreover this is no reason to reward the FTC with additional rulemaking powers. The FTC's existing ability to prosecute deceptive acts is sufficient, albeit with an increased budget for enforcement and the ability to level civil penalties for violation.

Notes

[1] See Roslyn Layton, "Congress Investigated Whether Privacy Rules Can Protect Consumers Without Killing Small Business," Forbes, March 26, 2019, https://www.forbes.com/sites/roslynlayton/2019/03/26/congress-investigates-whether-privacy-rules-can-protect-consumers-without-killing-small-business/#18a389c74459; and Evan Engstrom, "Small Business Perspectives on a Federal Data Privacy Framework," testimony before the Senate Commerce, Science & Transportation Committee Subcommittee on Manufacturing, Trade, and Consumer Protection, March 26, 2019, https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf.

[2] See Eric Goldman, "An Introduction to the California Consumer Privacy Act (CCPA) (July 9, 2018)," Santa Clara University, https://ssrn.com/abstract=3211013 or http://dx.doi.org/10.2139/ssrn.3211013.

[3] Engstrom, "Small Business Perspectives on a Federal Data Privacy Framework."

[4]Scroll to 1 hour 10 minutes in video to see the comments of Pam Dixon. http://www.aei.org/events/perspectives-on-data-privacy-from-the-federal-trade-commission-and-department-of-justice/

[5] *Economist,* "Should the Tech Giants Be More Heavily Regulated?," April–May 2018. The follow-up mention was at Open Future, "On Servile DC Journalists, Helping Free-Trade's Losers and Elections in Lebanon," https://www.economist.com/blogs/openfuture/2018/05/open-future.

[6] Roslyn Layton, "The 10 Problems of the GDPR: The US Can Learn from the EU's Mistakes and Leapfrog Its Policy," testimony before the Senate Judiciary Committee, March 12, 2019, https://www.judiciary.senate.gov/download/03/12/2019/layton-testimony.

[7] http://www.oecd.org/going-digital/ai/oecd-initiatives/

[8] NiemanLab, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

[9] Jane Bambauer, "Is Data Speech?," *Standford Law Review*, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/01/66_Stan._L_Rev_57_Bambauer.pdf.

[10] Roslyn Layton, testimony before the Federal Trade Commission, August 20, 2018, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf.

[11] Roslyn Layton, "Congress Investigates Whether Privacy Rules Can Protect Consumers Without Killing Small Business," Forbes, March 26, 2019, https://www.forbes.com/sites/roslynlayton/2019/03/26/congress-investigates-whether-privacy-rules-can-protect-consumers-without-killing-small-business/#24fc77014459.

[12] Shan Wang, "European News Sites Are Among the Worst Offenders When It Comes to Third-Party Cookies and Content," NiemanLab, http://www.niemanlab.org/2018/05/european-news-sites-are-among-the-worst-offenders-when-it-comes-to-third-party-cookies-and-content/; Shan Wang, "Has the GDPR Law Actually Gotten European News Outlets to Cut Down on Rampant Third-Party Cookies and Content on Their Sites? It Seems So.," NiemanLab, http://www.niemanlab.org/2018/08/has-the-gdpr-law-actually-gotten-european-news-outlets-to-cut-down-on-rampant-third-party-cookies-and-content-on-their-sites-it-seems-so/; and NiemanLab, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/?relatedstory.

[13] Roslyn Layton, "The Internet and Digital Communications: Examining the Impact of Global Internet Governance," testimony before the Senate Committee on Commerce, Science and Transportation, July 31, 2018, https://www.commerce.senate.gov/public/index.cfm/hearings?Id=00505D23-78EC-4C8C-8C18-11770654D27A&Statement_id=04BDF976-CF46-49BA-AD8C-221901DB7F00.

[14] https://ecfsapi.fcc.gov/file/60002081035.pdf

[15] Inge Graef, Sih Yuliana Wahyuningtyas, and Peggy Valcke, "Assessing Data Access Issues in Online Platforms," *Telecommunications Policy* 39, no. 5 (June 2015): 375–87, doi:10.1016/j.telpol.2014.12.001.

[16] Berin Michael Szoka, "The Paradox of Privacy Empowerment: The Unintended Consequences of 'Do Not Track,'" TPRC 41 (August 29, 2013), https://ssrn.com/abstract=2318146 or http://dx.doi.org/10.2139/ssrn.2318146.

[17] Freedom in the 50 States, "New Jersey—#47," https://www.freedominthe50states.org/overall/new-jersey.

[18] Annie O'Sullivan, "Newark Ranks 3rd, NYC Ranks 39th on Neediest Cities in the Country: Study," NBC, December 12, 2018, https://www.nbcnewyork.com/news/local/Newark-Ranks-3rd-Neediest-City-in-US-Homeless-Poverty-Hunger-Children-NYC-39th-Rochester-27th--502578902.html.

[19] Catey Hill, "3 Reasons So Many People Are Getting the Hell out of the Northeast," MarketWatch, January 31, 2019, https://www.marketwatch.com/story/3-reasons-so-many-people-are-getting-the-hell-out-of-the-northeast-2018-10-20.

[20] Bret Swanson. "Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation." Summary of Forthcoming Report. AEI. February 2019.

[21] http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm

[22] Martin Redish, *Wholesale Justice: Constitutional Democracy and the Problem of the Class Action Lawsuit* (Stanford Books, 2009), https://www.amazon.com/Wholesale-Justice-Constitutional-Democracy-Stanford/dp/0804752753.

[23] Roslyn Layton, statement before the Federal Trade Commission, August 20, 2018, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf.

[24] Federal Trade Commission, "Big Data: A Tool for Inclusion or Exclusion?," January 2016, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[25] Jin-Hyuk Kim and Liad Wagman, "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis," RAND Journal of Economics (2015). This is consistent with the more general phenomenon of risk-based lending markets. See Wendy Edelberg, "Risk-Based Pricing of Interest Rates for Consumer Loans," Journal of Monetary Economics 53, no. 8 (2006).

[26] Supra FTC.

[27] Kashmir Hill, "I Cut the 'Big Five' Tech Giants from My Life. It Was Hell," GIZMODO, February 7, 2019, https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

[28] John B. Horrigan, "Digital Readiness Gaps," Pew Research Center, September 20, 2016, https://www.pewinternet.org/wp-content/uploads/sites/9/2016/09/PI_2016.09.20_Digital-Readiness-Gaps_FINAL.pdf.

[29] See Democratic National Committee, "The 2016 Democratic Platform," https://democrats.org/about/party-platform/?source=homepage. "High-speed internet connectivity is not a luxury; it is a necessity for 21st century economic success, social mobility, education, health care, and public safety. Despite considerable progress and private investment in the last eight years to close the digital divide, there is more work to do. Democrats will finish the job of connecting every household in America to high-speed broadband, increase internet adoption, and help hook up anchor institutions so they can offer free WiFi to the public. We will take action to help America widely deploy 5G technology—the next generation wireless service that will not only bring faster internet connections to underserved areas, but will enable the Internet of Things and a host of transformative technologies."

[30] Hill Holliday, "Meet Gen Z: The Social Generation," http://thinking.hhcc.com/?utm_campaign=Thought%20Leadership%20%E2%80%94%20Gen%20Z&utm_source=Press%20Release (last visited June 25, 2018).

[31] Connie Hwong, "Why Churn Rate Matters: Which Social Media Platforms Are Losing Users?," Verto Analytics, May 4, 2017, https://www.vertoanalytics.com/chart-week-social-media-networks-churn/.

[32] The following statutes do not preempt stricter protections under state law: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Drivers' License Privacy Protection Act, and the Telemarketing Consumer Protection and Fraud Prevention Act.

[33] The 1996 and 2003 amendments included, for example, new obligations on businesses to ensure the accuracy of reports, increased civil and criminal penalties, remedial rights for identity theft victims, and the right to free annual credit reports.