Statement 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

The 10 Problems of the GDPR

The US can learn from the EU's mistakes and leapfrog its policy

Roslyn Layton
Visiting Scholar

March 12, 2019

Chairman Graham, Ranking Member Feinstein, and Members of the Committee, thank you for the opportunity to discuss the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). It is an honor. I am heartened by your bipartisanship on this important issue. This testimony reflects my own views and research.

My testimony is informed by working at Denmark's Center for Media and Information Technologies at Aalborg University where we conduct research on privacy and security technologies. 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.

Today I will identify the 10 key problems with the GDPR, which, if not addressed, will plague the CCPA. I will discuss evidence-based solutions for online privacy and data protection. These include privacy enhancing technologies, consumer education, and standard setting. Finally, I will address why a strong federal standard supports a national digital economy, protects Americans' rights, and is supported by the Constitution.

The 10 Problems with the GDPR

Here are the 10 key problems with the GDPR, and, if not properly amended, these will also plague the CCPA.

1. The GDPR strengthens the largest players.
2. The GDPR weakens small- and medium-sized firms.
3. The GDPR is cost prohibitive for many firms.
4. The GDPR silences free speech and expression.
5. The GDPR threatens innovation and research.
6. The GDPR increases cybersecurity risk.
7. The GDPR and the CCPA create risks for identity theft and online fraud.
8. The GDPR has not created greater trust online.
9. The GDPR and the CCPA use the pretense of customer control to increase the power of government.
10. The GDPR and the CCPA fail to meaningfully incorporate the role of privacy enhancing innovation and consumer education in data protection.

To analyze a policy like the GDPR, we must set aside the political pronouncements and evaluate its real-world effects.

The GDPR has strengthened the largest players. Since the implementation of the GDPR, Google, Facebook, and Amazon have increased their market share in the EU.[2] Three things have happened. [3] (1) The high cost of GDPR compliance is an advantage for large firms which have larger budgets to pay for software upgrades and privacy professionals. (2) Companies have stopped using competing tracking tools to Google and Facebook, giving a greater share of the market to the established players. (3) Users are less likely to try new platforms and tools, sticking instead with the "devil they know" in the incumbent players.

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."[4] Indeed larger firms may welcome the GDPR because it can insulate them from competition.

The GDPR has weakened small- and medium-sized firms. Small ad tech competitors have lost about one-third of their market share. The data show that the EU has not fostered an environment in which small- and medium-sized companies grow.

Despite some years of notice about the GDPR's coming implementation, only 20 percent of EU companies, primarily the large firms, are digitized.[5] There is little to no data that show that small- to medium-sized companies are growing in the EU because of the regulation.[6] The European Commission's digital scoreboard reports show a consistent lag in the small to medium enterprise segment, particularly to modernize their websites and market outside their own EU countries.[7] 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.[8]

Many American retailers, game companies, and service providers no longer operate in the EU. The Williams-Sonoma and Pottery Barn websites are dark.[9] 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.[10] Drawbridge, an identity-management company from San Mateo, California, exited the EU and sold off its ad-tracking business because of the GDPR.[11] 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.[12]

Valve, an award-winning video game company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance.[13] 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.[14] California-based Gravity Interactive no longer offers games in the EU and refunded its European customers.[15]

The Las Vegas–based Brent Ozar Unlimited, which offers a range of information technology and software support services, stopped serving the EU.[16] 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.[17] 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.[18] Even the Association of National Advertisers website is not available in the EU.[19]

The regulation has hurt the European venture capital market which funds startups. 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.[20]

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.[21] Even so, the GDPR has also made it difficult for European startups. Consider the case of Momio, a social network for children started to offer an alternative to Facebook.

Momio is an online social network designed and operated exclusively for children age 5–15 with one million users across the Nordic region and Netherlands, Germany, and Poland.[22] Launched in 2013, it operates a flagship version and Momio Lite, which does not process any personal data. The Lite version does not allow posting of text or images. Parental consent is required for users under the age of 13. Kids access the platform via a mobile device and interact with avatars they individually create. The platform is funded by partnerships with kid-friendly content and media companies. The platform is grounded in concepts of digital life skills with a focus on digital use, safety, security, emotional intelligence, communication, and literacy. As explained in an email by the company's CEO Mikael Jensen, "…as far as I know, the GDPR legislative work has not involved parents and children in the development of the law when it comes to child protection. GDPR has not made it easier to be a child on digital platforms, but on the contrary, more difficult."[23]

The GDPR has proved cost prohibitive for many firms. To do business in the EU today, the average firm of 500 employees must spend about $3 million to comply with the GDPR.[24] Thousands of US firms have decided it is not worthwhile and have exited.[25] 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[26]), 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.[27] The direct welfare loss is estimated be about €260 per European citizen.[28] 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[29] and one-third of annual e-commerce revenue in the US.[30]

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.[31] Some advertisers report being shut out from exchanges.[32] 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.[33]

The GDPR has silenced free speech and expression. Since the GDPR went into effect, over 1,000 news sites have gone dark in the EU.[34] EU residents have been unable to access Tribune Media, whose flagship newspapers include the *Los Angeles Times*, the *Chicago Tribune*, *New York Daily News*, the *Hartford Courant* (America's longest running newspaper since 1764), the *Orlando Sentinel*, and the *Baltimore Sun*.[35] Nor can they access more than 60 newspapers of Lee Enterprises covering news across 20 US states.[36] Blocked media is a problem not only for the one million Americans who live in the EU who can no longer read news and information about their hometowns but also for Europeans who wish to learn more about the US from direct sources rather than the state-owned media, which dominate the press and broadcasting in most EU countries.

No longer visible in the EU are more than 1,000 American news and media outlets, in addition to many sites for ecommerce, games, information technology, and other services.[37] This is concerning because the EU is the destination of about two-thirds of America's exports of digital media, goods, and services.[38]

GDPR compliance is so costly and cumbersome that these entities self-censor rather than risk violating the GDPR. If the GDPR were adopted in the US, it would likely violate the First Amendment, as the requirements for data processing are so onerous that they would be found to limit expression. A related issue with the GDPR is the Right to be Forgotten (RTBF), the notion that information has a finite life and that after a certain period, the information's life is "spent" and can be deleted from the public domain. The EU asserts that the GDPR applies to data controllers anywhere in the world if they process a European citizen's data. Similarly, RTBF proponents such as France's data protection authority (DPA) attempt to force the global removal of public information in the name of data protection. For example, the French DPA has ordered Google to delete certain search results in France, and it believes that the company must therefore delete them for all countries' search engines. Google has appealed this holding to the European Court of Justice. The European Commission, Ireland, and Greece support the company in its appeal, arguing that RTBF stretches the meaning of data protection too far.[39]

Indeed, the GDPR's asserted jurisdiction outside the EU may itself be illegal—at least where the US is concerned.[40] The GDPR is likely unenforceable under US common law, which rejects foreign rulings when they are contrary to American policy.[41] The SPEECH Act, passed in 2010, supplies strong protections for First Amendment freedoms in the context of libel suits brought in foreign jurisdictions.[42]

The GDPR threatens innovation and research. Many GDPR requirements are fundamentally incompatible with big data, artificial intelligence, blockchain, and machine learning, especially those that require data processors to disclose the purpose of data processing, minimize their use of data, and automate decision-making.[43] For technology developers, engineers, and entrepreneurs, the GDPR creates uncertainty not only in the text of the law and its adjudication but also in that requirements and tenets of the GDPR conflict with the operation of machine learning and artificial intelligence.[44]

Some of the most important recent scientific advances have been the result of processing various sets of information in inventive ways—ways that neither subjects nor controllers anticipated, let alone requested. Consider the definitive study on whether using mobile phones causes brain cancer.[45] The Danish Cancer Society analyzed 358,403 Danish mobile subscribers by processing Social Security numbers, mobile phone numbers, and the National Cancer Registry, which records every incidence of cancer by Social Security number.[46] The study, the most comprehensive investigation of its kind ever conducted, proves that using mobile phones is not correlated with brain cancer. But the users' information was not collected for the express purpose of such a study. Therefore, it is possible that, had the GDPR been in effect at the time of the study, consent from the population whose data was analyzed would not have been available, and the GDPR's purpose-specification requirement would have therefore made it impossible to conduct the study. Going forward, it is possible, if not likely, that valuable research will not be conducted because of the GDPR.

Indeed, part of the promise of socialized medicine was the ability to tap the vast pools of data in public health databases to make advances in medicine. However, a privacy panic is threatening to derail some projects,[47] including Iceland's genome warehouse, the oldest and most complete genetic record in the world, which promises groundbreaking therapies for Alzheimer's disease and breast cancer.[48] While many regulatory advocates focus attention on Silicon Valley firms and call for greater regulation, their campaign is backfiring as users turn their ire toward governments and demand erasure of their data from national health care records and other government services, potentially frustrating the operating models of mandated social programs.[49] With the mantra of "if in doubt, opt out," about half a million Australians rejected the country's national electronic health record, causing the computer system to crash in July 2018.[50]

For centuries, European state churches have collected and published information on births, deaths, weddings, baptisms, and more. In Denmark and Sweden, these institutions retain the official register for this information. Because of the GDPR, many churches have stopped printing announcements in the bulletins for their local congregations unless they obtain consent first.[51] GDPR risks have also been identified with respect to convicted felons successfully removing information about their crimes from search engines,[52] the exchange of business cards,[53] the taking of pictures in public,[54] and disclosures of health and injury information in the trade of soccer players.[55]

The GDPR increases cybersecurity risks. A key unintended consequence of the GDPR is that it undermines the transparency of the international systems and architecture that organize the internet. The WHOIS query and response protocol for internet domain names, IP addresses, and autonomous systems is used by law enforcement, cybersecurity professionals and researchers, and trademark and intellectual property rights holders.[56] The Internet Corporation for Assigned Names and Numbers (ICANN) recently announced a Temporary Specification that allows registries and registrars to obscure WHOIS information they were previously required to make public, ostensibly to comply with the GDPR.[57] This could hinder efforts to combat unlawful activity online, including identity theft, cyberattacks, online espionage, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and other criminal behavior, and it is not even required by the GDPR.

The GDPR does not apply at all to nonpersonal information and states that disclosure of even personal information can be warranted for matters such as consumer protection, public safety, law enforcement, enforcement of rights, cybersecurity, and combating fraud. Moreover, the GDPR does not apply to domain names registered to US registrants by American registrars and registries. Nor does it apply to domain name registrants that are companies, businesses, or other legal entities, rather than "natural persons." All the same, actors including ICANN are practicing voluntary censorship because the GDPR's provisions are so vague and the potential penalties so high. GDPR proponents have likely contributed to the impression that the GDPR urges measures such as the Temporary Specification. For example, in her role in the Article 29 Working Party, the group that drove the promulgation of the GDPR, Andrea Jelinek said that the elimination and masking of WHOIS information is justified under the GDPR.[58]

The WHOIS problem can be described as the conflict between the individual's right to privacy and the public's right to know.[59] It can also be understood within the context of the problem of "privacy overreach,"[60] in which the drive to protect privacy becomes absolute, lacks balance with other rights, and unwittingly brings worse outcomes for privacy and data protection.[61] The situation harkens back to a key fallacy of privacy activists who attempted to block the rollout of caller ID because it violated the privacy rights of intrusive callers. Today, the receiver's right to know who is calling is prioritized over the caller's right to remain anonymous.[62] Similarly it is understood that the needs of public safety will supersede data protection, particularly in situations of danger to human life. Moreover, one should expect intellectual property to be in balance with data protection, not in conflict as it is under the GDPR. The pace of development of privacy and data protection law is significantly faster than that of other kinds of law, leading one scholar to suggest that it threatens to upend the balance with other fundamental rights.[63] This point is eloquently underscored by Richard Epstein in his critique of the idea of privacy rights established by the Warren Court. This progressive theory assumes that it is "always easy, if not inevitable, to expand the set of rights without adverse social consequences," but it never stops to consider that, when rights are expanded, correlative duties are imposed on others.[64]

I have noted the security fallout from the GDPR, but there are additional 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.[65] Eu-

ropean 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 the Senate for its leadership on this front.[66] I also support the role of cyber insurance to help firms assess and address security risks.[67]

The GDPR and the CCPA create risks for identity theft and online fraud. The GDPR and the CCPA purportedly give users the ability to control their data by facilitating user requests. However, they also give hackers and identity thieves the ability to steal data because there is no provision for user authentication. Companies now have to develop data pools to respond to user requests, creating a target-rich environment for cyber criminals. [68] This outcome is indicative both of the zeal of policymakers to regulate without thinking through the consequences (let alone consulting users to their preferences) and the general sloppiness of a law stitched together in a mere week, as was the case of the GDPR.

The GDPR has not created greater trust online. 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[69]—Europeans report no greater sense of trust online.[70] 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 has not helped them understand how their data are used.[71] 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.[72] Similarly, California has more privacy laws than any state, and yet its residents do not report feeling more private or safe.

The GDPR and the CCPA use the pretense of consumer control to increase the power of government. Control is defined as the power to influence behavior. The European and California rules are a government power grab in the name of giving control to consumers. This can be demonstrated by studying the text of the laws themselves in which the discussion of consumers is mere pretense to the true objective: giving more power to government. The GDPR imposes 45 specific regulations on business practices and regulators with 35 obligations. California goes even further with 77 regulations on business practices and sweeping powers to the attorney general.

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.[73]

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.[74] In fact, there are 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.[75] 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.[76] Rather, the GDPR is about data protection or, more correctly, data governance.[77] 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.[78] 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[79] and its ability to compel information in court.[80] 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.

It is precisely when leaders feel voter confidence slipping that they look for a way to increase power, as such the GDPR is an attempt by European policymakers to solidify legitimacy for Brussels during a period of deep skepticism among voters. The GDPR can be examined in the context of a heightened pro v. anti-EU debate, fueled by a rise in Euroscepticism and nationalist parties which charge that European integration weakens national sovereignty.[81] Smarting from a disgruntled electorate and the Brexit bombshell,[82] pro-European coalitions support pan-European regulation such as the GDPR to legitimize the EU project. It should be noted that Eurosceptic political actors are not necessarily opposed to data protection regulation; they

merely prefer the primacy of national institutions over European ones, largely because of concerns that EU institutions and policies are subverting democracy.

In the case of the GDPR, there was no groundswell of public support calling for the enactment of greater data protection regulation. The GDPR was enacted during a period of voter "disengagement."[83] Participation in European Parliament elections has dwindled from 62 percent in 1979 to just 42 percent in 2014.[84] This environment of voter disengagement is conducive for the collective action of organized special interests to defeat a diffuse, disgruntled, and unorganized majority.[85] Relatively few Europeans are even aware of the GDPR. For example, a United Kingdom survey found that only 34 percent of respondents recognized the law, and even fewer knew what it covered.[86] Essentially, a relatively small group of GDPR advocates successfully implemented massive pan-European regulation without significant voter buy-in. Public opinion as measured by the Eurobarometer poll[87] suggests that most people would prefer a more nuanced approach to data protection over the sledgehammer of the GDPR, and that most would rather strengthen regulation at the nation-state level than at the EU.[88]

It does not appear that consumers are so empowered by the GDPR as litigants and non-profit organizations which the GDPR empowers with new rights to organize class actions,[89] lodge complaints,[90] and receive compensation[91] from fines levied on firms' annual revenue, as high as four percent of annual revenue.[92] Historically, Europe has largely eschewed "U.S.-style" class actions,[93] noting that they disproportionately reward lawyers and litigation financiers over consumers.[94] But policymakers have engineered the GDPR so that privacy activists can bring cases without overcoming legal barriers of standing and jurisdiction, which are traditional safeguards against the abuse of the legal system for private gain. A mere 7 hours after the GDPR was implemented, complaints requesting over $8 billion in damages and compensation had already been filed by professional litigants who helped craft the law.[95]

The GDPR and the CCPA fail to meaningfully incorporate the role of privacy enhancing innovation and consumer education in data protection. Without meaningful provisions to promote education or innovation, the GDPR and CCPA freeze the status quo in place, rewarding the largest players; punish small- and medium-sized enterprises; and trick people into thinking that they have more privacy when in fact they are being put at greater risk.

Bureaucratizing data protection does not create a *natural right of privacy*. Having ever more regulators and regulations to govern data does not make a person safer. Regulation freezes the status quo; it does not support the improvement of systems or user knowledge. Moreover, the EU and California rules *disintermediate* the vital connection between the user and online provider which provides feedback to help the platform evolve.

We have discussed the 10 problems. Now let's discuss policy elements which have been evidenced to provide superior outcomes than we have experienced with the GDPR: privacy enhancing technologies, consumer education, and standard setting.

The California and European rules miss two of the four *essential evidenced elements* to create

trust online. Neither policy incorporates the role of privacy enhancing technologies to improve the online system or the role of knowledge to help upgrade users' competence.

The Role of Privacy Enhancing Technologies (PETs) in Promoting Online Privacy

Privacy regulation attempts to shape the market to deliver predetermined outcomes and requires government intervention to certify compliance. Innovation, on the other hand, can create better systems that never compromise a user's privacy. Extensive evidence shows that a flexible, innovation-based approach yields software and systems that are better designed to protect data and privacy and that empower enterprises to operate with data protection as a competitive parameters.[96] The International Association of Privacy Professionals' survey of privacy practices of 800 enterprises around the world found that traditionally less-regulated industries have more advanced privacy practices than highly regulated industries, which conform only to regulatory requirements.[97] Even in 2010, the International Conference of Data Protection and Privacy Commissioners resolved that efforts to promote privacy by design needed to be more deeply embedded in policy.[98]

The problem with regulating software technology is that it freezes a status quo instead of supporting the innovation that can lead to better, more consumer-centric systems. Indeed, the GDPR mandate of a single mode of data governance unwittingly creates an attack surface for cyber criminals. As such, we should encourage multi-stakeholder efforts of the National Telecommunications and Information Administration, the National Institute of Standards and Technology, and others to develop a scientific, evidence-based framework as the most salient approach to privacy and data protection in the 21st century. The focus on the scientific approach ensures the engineering trustworthiness of technology. Measurement science and system engineering principles can support the creation of frameworks, risk models, tools, and standards that protect privacy and civil liberties.[99]

The European Union Agency for Network and Information Security's (ENISA) related report "Privacy and Data Protection by Design" explains privacy-enhancing technologies including not only encryption but also protocols for anonymous communications, attribute-based credentials, and private search of databases in addition to a range of strategies of multiple practices that firms can employ.[100] It describes a large body of literature on privacy by design but also states that its implementation is weak and scattered. Indeed, privacy and data protection features are relatively new issues for engineers, designers, and product developers when implementing the desired functionality. To address this, ENISA has stewarded the discussion on how to develop a repository of such technologies.

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.[101] 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.[102]

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.[103] Outside of certain applications, the traditional health care industry is woefully inefficient; digital industries are eight 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 health care and government.[104]

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.[105] 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.

I commend the work by the National Institute of Standards and Technology to inform this effort.[106] 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.[107]

Consumer Control Requires Consumer Education

Consumer education is an important but fragmented field. It plays a role to help people consumer products and services safely and intelligently, like heath education and financial literacy. We need the same kind of training for our online lives.

It is instructive to consider the robust, vibrant market for information and education in the consumer electronics field, detailing the most minute and technical aspect of machines. For decades consumers have availed themselves to magazines, online discussions, rankings, reviews, how-to videos, and conferences on how to use these technologies, yet there is no policymaker directing the discussion; it grows by consumer demand.

There is no reason why there could not be similar resources for privacy education. There is a public policy role to support education in this space, including working with industry to disseminate the important information and challenge them to ensure their users take privacy trainings and tutorials. See p. 12 of my testimony to the FTC in which I describe how the FTC's existing privacy education resources can be leveraged, examples of curricula, and education distribution models.[108]

The US Can Leapfrog the GDPR and the CCPA with Technology-Based Standards for Data Protection

Policy should support the innovation of new and better privacy-enhancing technology. We can learn from the standard setting process undertaken at the FTC with COPPA. I applaud the work of Pam Dixon of the World Privacy Forum who has provided extensive analysis and documentation to the value of standard setting.[109] I quote liberally:

> "Much has been learned in the last 25 years about data protection and digital identity ecosystems. . . . However, baseline digital ecosystem governance principles are generally not as well-understood or known outside of certain contexts where they are often found in use, such as environmental, production, and law enforcement contexts.
>
> Nobel Laureate and economist Elinor Ostrom spent her entire career observing and analyzing governance of complex ecosystems, particularly the commons, or shared resources. Over the span of decades, she observed and distilled the most effective ways of managing complex ecosystems where stakeholders share resources ("common pool" resources). Identity—particularly digital identity—is one such common pool resource.
>
> In complex digital ecosystems, strict top-down ownership is a difficult position to uphold, as is demand for full individual control of data. However, mutually agreed governance of resources that are shared can work, and has proven to work. If we think of data—and identity data—as a shared resource, one in which multiple stakeholders have involvement with and an interest in, then we have a pathway to govern those systems as shared resource systems. . . .
>
> Ostrom set forth eight principles for governance of complex systems using shared resources. . . . They can also be applied in complex data and identity ecosystems where frameworks such as FIPs provide baseline principles to apply and implement. The Ostrom general principles are as follows:
>
> 1. Rules are devised and managed by resource users.
> 2. Compliance with rules is easy to monitor.
> 3. Rules are enforceable.
> 4. Sanctions are graduated.
> 5. Adjudication is available at low cost.
> 6. Monitors and other officials are accountable to users.
> 7. Institutions to regulate a given common-pool resource may need to be devised at multiple levels."

The most striking difference between these recommendations and the GDPR and CCPA is that the users, not regulators, write the rules. Compliance is easy to monitor and not financially crushing to service providers. Monitors are accountable to users. The CCPA does not require any accountability to the California Attorney General. There are no transparency obligation or other valuable measures to ensure accountability.

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.[110] 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.[111] 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.

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.[112]. Unlike the GDPR, the US policy should not make it more expensive to do business, reduce consumer freedom, or inhibit innovation.

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.[113] 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] 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/.
https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324
https://www.bloomberg.com/opinion/articles/2018-07-20/google-s-mortal-enemy-does-it-a-95-billion-favor
https://www.bloomberg.com/opinion/articles/2018-06-25/google-and-facebook-turn-on-the-fake-riviera-charm

[3] Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy regulation and market structure." *Journal of Economics & Management Strategy* 24.1 (2015): 47-73.

[4] George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics* 2, no. 1 (1971): 3–21.

[5] 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.

[6] https://ec.europa.eu/digital-single-market/en/digital-scoreboard

[7] 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.

[8] 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.

[9] 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/.

[10] Jon Russel, "RIP Klout," TechCrunch, May 2018, https://techcrunch.com/2018/05/10/rip-klout/.

[11] 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/.
[12] 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.
[13] Steam, "Super Monday Night Combat," https://steamcommunity.com/app/104700/allnews/.
[14] 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.
[15] Warportal, "Important Notice Regarding European Region Access," http://blog.warpportal.com/?p=10892.
[16] Brent Ozar, "GDPR: Why We Stopped Selling Stuff to Europe," December 18, 2017, https://www.brent-ozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.
[17] 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.
[18] 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/.
[19] 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/.
[20] 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
[21] 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/.
[22] Momio, "About Momio," http://company.momio.me/about-us/
[23] Email from Mikael Jensen, March 6, 2019. Momio ApS, Lergravsvej 53, 2nd floor, 2300 Copenhagen S, Denmark
[24] International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018," 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.
[25] 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/.
[26] https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
[27] International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018."
[28] 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.
[29] Jonathan Spalter, "Broadband CapEx Investment Looking Up in 2017," USTelecom, July 25, 2018, https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017.
[30] US Census Bureau, "Quarterly Retail E-Commerce Sales 1st Quarter 2018," May 17, 2018, https://www2.census.gov/retail/releases/historical/ecomm/18q1.pdf.
[31] 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/.
[32] 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/.
[33] 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.
[34] 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/.
[35] Alanna Petroff, "LA Times Takes Down Website in Europe as Privacy Rules Bite," CNNMoney, May 25, 2018, https://money.cnn.com/2018/05/25/media/gdpr-news-websites-la-times-tronc/index.html.
[36] Renae Reints, "These Major U.S. News Sites Are Blocked in the EU," *Fortune*, August 9, 2018, http://fortune.com/2018/08/09/news-sites-blocked-gdpr/.

[37] 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.
[38] 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.
[39] IAPP, "European Commission Sides with Google in RTBF Case," accessed September 28, 2018, https://iapp.org/news/a/ec-sides-with-google-in-rtbf-case/.
[40] Kurt Wimmer, "Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?," *Syracuse Law Review* 68, no. 545 (2018), https://ssrn.com/abstract=3188974.
[41] Wimmer, "Free Expression and EU Privacy Regulation," 571.
[42] Wimmer, "Free Expression and EU Privacy Regulation," 572–73.
[43] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47 no. 995 (2017), https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.
[44] Joel Thayer and Bijan Madhani, "Can a Machine Learn Under the GDPR?," TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, December 16, 2018, https://ssrn.com/abstract=3141854.
[45] Patrizia Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study," *BMJ*, October 20, 2011, https://www.cancer.dk/dyn/resources/File/file/9/1859/1385432841/1_bmj_2011_pdf.pdf.
[46] Frei et al., "Use of Mobile Phones and Risk of Brain Tumours."
[47] Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology and Innovation Foundation, September 10, 2015, https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies.
[48] Jeremy Hsu, "Iceland's Giant Genome Project Points to Future of Medicine," IEEE Spectrum, March 25, 2015, https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/icelands-giant-genome-project-points-to-future-of-medicine.
[49] Bronwyn Howell, "Data Privacy Debacle Down Under: Is Australia's My Health Record Doomed?," AEIdeas, August 6, 2018, http://www.aei.org/publication/data-privacy-debacle-down-under-is-australias-my-health-record-doomed/.
[50] Howell, "Data Privacy Debacle Down Under."
[51] Version 2, "Minister: Krav om GDPR-samtykke til kirkeblade er absurd," September 11, 2018, https://www.version2.dk/artikel/minister-krav-gdpr-samtykke-kirkeblade-absurd-1086182; B.T., "Kirkeblade opgiver at bringe navne på døbte og døde," August 3, 2018, https://www.bt.dk/content/item/1203799; and Jens Peder Østergaard, "Konsekvens af EU-lov: Slut med at læse om døbte, gifte og døde," Viborg Stifts Folkeblade, May 22, 2018, https://viborg-folkeblad.dk/rundtomviborg/Konsekvens-af-EU-lov-Slut-med-at-laese-om-doebte-gifte-og-doede/artikel/376140.
[52] Daniel Castro, "The EU's Right to be Forgotten is Now Being Used to Protect Murderers," Center for Data Innovation, (September 21, 2018, https://www.datainnovation.org/2018/09/the-eus-right-to-be-forgotten-is-now-being-used-to-protect-murderers/. "According to the company (Google), almost one-fifth of the news articles it received requests to remove related to crime, and it removes roughly one-third of the right to be forgotten requests that it receives relating to news articles."
[53] Stephen White, "How Do Business Cards Sit with GDPR?," GDPR: Report, February 8, 2018, https://gdpr.report/news/2018/02/08/business-cards-sit-gdpr/.
[54] Kevin Sullivan, "What Photographers Need to Know About GDPR," PDNPulse, June 12, 2018, https://pdnpulse.pdnonline.com/2018/06/gdpr-how-bad-is-it-for-photographers.html; Soraya Sahhaddi Nelson, "New EU Data Protection Law Could Affect People Who Take Pictures with Their Phones," NPR, May 24, 2018, https://www.npr.org/2018/05/24/614195844/new-eu-data-protection-law-could-affect-people-who-take-pictures-with-their-phon?t=1538121870256.
[55] Thomas Idskov, "Mundkurv! Derfor holdes omfanget af FCK-spillers skade hemmelig," B.T., July 12, 2018, https://www.bt.dk/content/item/1197424.
[56] Shane Tews, "How European Data Protection Law Is Upending the Domain Name System," AEIdeas, February 26, 2018, https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/.

[57] Temporary Specification for gTLD Registration Data, ICANN, adopted May 17, 2018, https://www.icann.org/resources/pages/gtld-registration-data-specs-en.
[58] Letter from Andrea Jelinek, Chairperson of Article 29 Data Protection Working Party, to Göran Marby, President of ICANN, April 11, 2018, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf.
[59] Shane Tews, Privacy and Europe's Data Protection Law: Problems and Implications for the US, AEIdeas, May 8, 2018, http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/.
[60] See Justin "Gus" Hurwitz and Jamil N. Jaffer, "Modern Privacy Advocacy: An Approach at War with Privacy Itself?," Regulatory Transparency Project, June 12, 2018, https://regproject.org/paper/modern-privacy-advocacy-approach-war-privacy/.
[61] See Maja Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection," *Maastricht Journal of European and Comparative Law* 23 no. 812 (2016), http://journals.sagepub.com/doi/abs/10.1177/1023263X1602300505?journalCode=maaa.
[62] See Hurwitz and Jaffer, "Modern Privacy Advocacy," 179.
[63] See Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection," 180.
[64] Richard Epstein, "A Not Quite Contemporary View of Privacy," *Harvard Journal of Public Policy* 41 no. 95 (2018), http://www.harvard-jlpp.com/wp-content/uploads/2018/01/EpsteinPanel_FINAL.pdf.
[65] 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.
[66] https://www.cotton.senate.gov/?p=press_release&id=887
[67] Hurwitz, Justin (Gus), Cyberensuring Security (September 1, 2017). Connecticut Law Review, Vol. 49, No. 5, 2017. Available at SSRN: https://ssrn.com/abstract=3314400
[68] ANA, "The CCPA—Making Things Worse," March 4, 2019, https://www.ana.net/blogs/show/id/rr-blog-2019-01-The-CCPA-Making-Things-Worse.
[69] GDPR pop-up disclosures have become so intrusive that Europeans download pop-up blockers on their phones.
[70] 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.
[71] 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
[72] 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.
[73] Layton and Mclendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course."
[74] 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.
[75] 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).
[76] European Union, General Data Protection Regulation, note 18, https://gdpr-info.eu/.
[77] Evidon, "What Is the GDPR?," https://www.evidon.com/education-portal/videos/what-is-the-gdpr/.
[78] See Solove, "A Brief History of Information Privacy Law," 1-5, 1-6.
[79] See Solove, "A Brief History of Information Privacy Law," 7.
[80] See, for example, *Boyd v. United States*, 116 US 616 (1886).
[81] Euroscepticism as a Transnational and Pan-European Phenomenon 133 (John FitzGibbon, Benjamin Leruth, Nick Startin eds., 2016).
[82] *Id.* Euroscepticism is the notion that the European integration undermines the national sovereignty of its members states, that the EU lacks democratic legitimacy, is too bureaucratic, encourages high migration, and the perception that it is a neoliberal organization benefitting the elite at the expense of the working class—remains an obstacle to the goals some have for the European continent. *See also* Dalibor Rohac, *Europe's Pressure Points*, AEI, January 17, 2017, http://www.aei.org/feature/europes-pressure-points/.

[83] John Curtice, *How Deeply Does Britain's Euroscepticism Run?*, NATCEN (2016), http://www.bsa.natcen.ac.uk/media/39024/euroscepticism.pdf.
[84] Turnout 2014 - European Parliament, European Parliament, http://www.europarl.europa.eu/elections2014-results/en/turnout.html (accessed July 27, 2018).
[85] *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971).
[86] Kirsty Cooke, *Data Shows Awareness of GDPR Is Low amongst Consumers*, KANTAR, March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.
[87] European Commission, Public Opinion, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm.
[88] Roslyn Layton, *How the GDPR Compares to Best Practices for Privacy, Accountability and Trust*, SSRN Scholarly Paper, March 31, 2017, https://papers.ssrn.com/abstract=2944358.
[89] GDPR, Recital 142, Article 80.
[90] GDPR, Recital 141, Article 77.
[91] GDPR, Recital 143, Articles 78-79, 82.
[92] GDPR, Recital 143, Article 83.
[93] Lisa A. Rickard, *Consumers Are the Losers in EU's Collective Action Proposal*, POLITICO (Aug. 3, 2018), https://www.politico.eu/article/opinion-consumers-are-the-losers-in-eus-collective-action-proposal-european-commission-collective-action/.
[94] 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
[95] Roslyn Layton and Julian McLendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," Federalist Society, https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.
[96] Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe," 2015.
[97] International Association of Privacy Professionals, "IAPP-EY Annual Privacy Governance Report 2015," 2015, https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2015-2/.
[98] European Data Protection Supervisor, "International Conference of Data Protection and Privacy Commissioners," October 27, 2010, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf.
[99] Paul Hernandez, "Cybersecurity and Privacy Applications," National Institute of Standards and Technology, August 23, 2016, https://www.nist.gov/itl/applied-cybersecurity/cybersecurity-and-privacy-applications.
[100] European Union Agency for Network and Information Security, "Privacy and Data Protection by Design — ENISA," January 12, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
[101] 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.
[102] 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/.
[103] Bret Swanson. "Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation." Summary of Forthcoming Report. AEI. February 2019.
[104] English.gov.cn, "Internet Plus: Premier LI's New Tech Tool," March 13, 2015, http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm.
[105] 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
[106] 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.
[107] See Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings," 7.
[108] https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf

[109] Pam Dixon, "Digital Identity Ecosystems," World Privacy Forum, February 4, 2019, https://www.worldprivacyforum.org/2019/02/digital-identity-ecosystems/.
[110] 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/.
[111] CompTIA, "IT Industry Outlook 2018," January 2018, https://www.comptia.org/resources/it-industry-outlook-2018.
[112] Roslyn Layton, "FCC Privacy Regulation Will Limit Competition in a Market That Really Needs it: Online Advertising," AEIdeas, March 11, 2016, http://www.aei.org/publication/fcc-privacy-regulation-will-limit-competition-market-really-needs-online-advertising/.
[113] 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.