Statement before the National Telecommunications and Information Administration
Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780-8780-01

Consumer Privacy

Roslyn Layton, PhD
Visiting Fellow

November 9, 2018

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce, 1401 Constitution Avenue NW
Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

To whom it may concern:

I applaud the leadership of NTIA to conduct this inquiry, its open effort to solicit feedback from stakeholders, and its commitment to ensuring principles that promote both privacy and prosperity. This initiative seeks the golden mean of consumer privacy that provides "high levels of protection for individuals, while giving organizations legal clarity and flexibility to innovate."

These comments reflect my academic and policy research in comparative international data protection regulation and privacy policy. Please see my related comments submitted to the Federal Trade Commission (FTC) on market solutions for online consumer privacy[1] and an accounting of the unintended outcomes of the European Union's General Data Protection Regulation.[2] The EU's policy has not created greater trust online, nor has it "leveled the playing field", as was promised. Many small and medium sized business have shuttered operations in the EU or have closed altogether. Given the cost and complexity of the GDPR, thousands of American media companies are no longer accessible in the EU. Fortunately, the US can leapfrog the misguided regulation of the EU, China, and California with a policy that legitimately empowers consumers, not self-interested authorities and litigants.

This comment highlights important policy points which are supplemental and important to the effectiveness of NTIA's proposed principles. They include

Realistic conceptions of consumers and their responsibilities
How consumer education should supplement the principles
Policies to promote innovation in privacy enhancing technologies
Policy considerations to resource the FTC and the consumer protection functions of government.

Please note that the comments reflect my own views. Thank you for the opportunity to participate.

Sincerely,

Roslyn Layton, PhD
Visiting Fellow
American Enterprise Institute
1789 Massachusetts Avenue NW
Washington, DC 20036

Comments

NTIA Developing the Administration's Approach to Consumer Privacy Consumer Privacy

Realistic conceptions of consumers and their responsibilities

From a monolithic view of consumers to a realistic view of diverse individuals with contextual preferences. The current policy process on consumer privacy has been open and inclusive, surfacing the views of many stakeholders. While there is a understanding of different kinds of firms and organizations which collect data (large Silicon Valley platforms, Fortune 1000 firms, data brokers, small and medium-sized internet companies, public sector agencies, startups, non-profit organizations, individual blogs, websites etc.), the people who use these digital products and services are lumped into single box such as "consumers" or "users". Nevertheless, consumers have multiple parameters by which they can be described including age, gender, race, occupation, education, location, affiliation and so on.

Conceptualizing consumers as a monolithic group as if they all want the same regulation is wrong. This presumption can lead to misguided policy which ultimately fails to achieve its stated goals, or to which firms and consumers find workarounds. Users of online services are highly diverse, have different preferences, and make individual, contextualized decisions based upon how they perceive the transaction with their data. Research tools deployed among hundreds of millions of users shows that privacy preferences change minute to minute depending on the site visited, the user's goal, and the user's desire for security and speed.[3] Users interpret privacy within a context, and many don't object to sharing information per se, only to sharing that is inappropriate based on the context.[4]

While there is a benefit to a single, comprehensive standard, policymakers should realize that not all "consumers" are the same. The point is underscored by a leading data broker's categorization of consumers by "lifestage", affluence, and use of digital technologies.[5] American households are further categorized into 70 segments and 21 groups based on similar demographic, socio-economic and consumer behavior.[6] Hispanic consumers can be categorized into 55 specific buying groups.[7] Understandably some regulatory advocates are opposed to such tools, even though they have been integrated in the American economy for decades, and prior to that, were conducted via analog means.

The point is merely that a data broker's description of "consumers" is a more accurate reflection than the current policy discourse. As such, it is worthwhile for policymakers to try to understand the diversity of consumers before making policy. Consumer education plays an important role to fill the gap between what regulatory advocates want and what different consumers prefer. As such, it makes sense for NTIA to propose a baseline set of principles and to allow consumers to supplement their preferences with informed choices.

Responsibilities of consumers. The leading textbook of the field "Economic Education for Consumers" details the notions of consumer expectations as well as consumer responsibilities.[8] They include the following concepts:

1. Responsibility to be an educated consumer, including responsibility to gather and evaluate information before making a decision
2. Responsibility to use products and services safely
3. Responsibility to use information to make choices
4. Responsibility to choose carefully
5. Responsibility to express opinion about a product, as well as report improper business practices. This can be communicated to the community, firm, and/or authorities.

In addition, consumers have the freedom to consume in a responsible manner by selecting products and services that conform to their values as well as seek redress from injury by unfair, deceptive, and defective products and services.

Role of Consumer Education in Online Privacy. Consumer education is by no means a panacea. Indeed an academic review of the range of methods and approaches employed for financial literacy education notes shortcomings in their effectiveness.[9] On the other hand, the value of education to improve outcomes in personal health is well-documented.[10] However financial literacy may be more effective in imparting "rules of thumb", for example, knowing the value of diversification in an investment portfolio is more important than knowing the litany of financial instruments.[11]

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, conferences, and so on. There is no policymaker directing the discussion, but it grows by consumer demand.

There is no reason why there could not be a similar field for the consumption of online services, which describes the contours of online privacy and how users could select different technologies to manage their privacy. The difference is that consumer electronics education is essentially funded by advertising placed by the providers of phones, devices, appliances, and so forth. In general, online platforms do not advertise as such, so there is a policy opportunity to see how such resources can be developed in the marketplace. Consumer education on privacy could help consumers understand the principles of consent and control and exercise their associated freedoms.

Public Choice Explanation for the Lack of Consumer Education on Privacy. The academic discipline of public choice uses economics to investigate problems in political science. It could help explain why consumer education on privacy is lacking, aside from one possible explanation that consumers are not interested to learn about privacy and therefore do not demand such information. A public choice theorization would likely recognize that while the notion of consumer education has implicit valence, industry and regulators may have incentives to de-emphasize education. Indeed, if consumers are empowered to make informed choices, they have less need of regulatory supervision. Similarly, consumers making informed choices also affects industry; it has a powerful effect to drive consumers from one firm to another.

The GDPR is suspect in that among its 173 provisions the role and importance of consumer education is

never discussed.[12] This is a serious oversight particularly when the EU's official cybersecurity research institute noted the primacy of consumer education to create privacy, accountability, and trust.[13] Nor is consumer education discussed in the context of the California Consumer Privacy Act. This is likely because the real objective for these regulations is not empower consumers but to strengthen the data protection and compliance business, specifically to give jobs to data protection officers, regulators, and litigators.

The assumption of the European and Californian rules is that regulatory authorities have more information than consumers and firms and therefore know better how to order transactions in the marketplace.[14] All the same, the these regulations impose massive new responsibilities on data protection agencies without a concurrent increase in training or funding.[15] Data regulators must wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."[16] Furthermore, these regulations widen the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.[17] There are certainly many talented individuals among these ranks, but the mastery of information communication technologies varies considerably among these professionals.

Public choice theory also suggests that the data regulators' preferences are not necessarily aligned with the "public interest," or what is best for consumer welfare in the long run. Increasing user knowledge and the quality of data protection technology could legitimately make people better off, but it could also render regulators less important. While data regulators will not necessarily reject policies that improve user knowledge and technology design, it is in their interest to promote inputs that increase their own resources and legitimacy in conducting compliance and adjudication.[18]

Surveys demonstrate that many users fail to practice basic privacy-enhancing behaviors.[19] This situation is ripe for improvement and represents a classic example of how consumer education can improve outcomes better, more quickly, and at a lower cost than regulation. Indeed, the first principle of consumer education in data protection, buyer beware, is the same first principle for how citizens should protect themselves in cyberthreats in Michael Chertoff's new book on cybersecurity: "Be mindful of what data you transmit and what you connect to your own network."[20] He also recommends practicing cyber hygiene, taking advantage of layered cybersecurity technology, and outsmarting scams with a phone call.

Consumers need to practice the same kind of vigilance and personal responsibility in cybersecurity as they do in the data protection domain. Outsourcing the job to bureaucrats will not cut it, as the user can be a vulnerability point. Consider warnings and labels on food and chemicals; while regulation can mandate that disclosures be made, if users do not recognize the meaning of expiration dates or consumption warnings, then disclosure has little impact.

How consumer education should supplement NTIA's principles

Transparency. The principle that "organizations should be **transparent** about how they collect, use, share, and store users' personal information" is laudable. Indeed, the FTC has been extremely deft to use transparency rules to bring actions against actors which threaten and/or harm consumers. The agency has levied significant fines and collects compensation for users. The history of enforcement serves as an important deterrent as well as a roadmap for firms.[21] The bottom line for policymakers is

that the FTC has proven its capability to police privacy and security, and transparency requirements are powerful tools to protect privacy.

However imposing transparency requirements is not without costs to consumers. The GDPR is driving disclosure overkill. Indeed, European requirements have become so onerous that many consumers have stopped using websites with cookie disclosures.[22] Opera, the popular browser, has developed technology to block the disclosure dialogues that plague users every time they visit a website in EU. Indeed, technologies and users can find innovative ways to go around regulations they don't like.[23]

Policymakers should not believe that automatically making consent more explicit makes consumers more informed. If the user fundamentally does not understand to what she agrees or the underlying transaction, no amount of disclosure, however detailed or granular, empowers the user. This is the gap that consumer education can fill.

When producers and consumers do not have perfect information, this discrepancy can give rise to inefficiency or abuse. Peer-to-peer platforms have resolved many of these problems of informational asymmetry through information sharing. Consider how the ability to evaluate drivers and riders is an essential part of ridesharing apps. Before Uber, neither the taxi company nor the regulator was interested to publish real-time information about the quality of drivers or cars, as it could impugn the deficiency of regulator. Ratings and peer reviews are essential in the digital economy. Indeed, some health regulators use Yelp ratings to help inform how they deploy their inspection resources.[24]

Consumer education could be vital to demystify the "black box" of many internet platforms, which for many consumers is a system in which they can observe the inputs and outputs but have little to no insight to its internal workings. It is only when consumers have enough education about the tools they can use that they can begin to "exercise **control** over the personal information they provide to organizations."

Preliminary ideas about promoting consumer education in privacy. My submission to the FTC describes some of the leading privacy education programs beginning on page 15.[25] Firms could support these organizations financially to spread the information and as an example of their commitment to principles. Following are additional ideas to consider to embedding consumer education for privacy into the marketplace.

- Leverage the FTC's educational website, materials and knowledge into the public domain https://www.consumer.ftc.gov/topics/privacy-identity-online-security. Firms could link to the FTC from their websites.
- Firms can develop their own educational platforms for privacy and engage and encourage customers to learn.
- Firms could offer rewards/discounts for customers to take online privacy training.
- Firms could supplement disclosures with consumer-centric tools (videos, cartoons etc.) to explain how their products and services, incorporate data.
- A task force of FTC, industry and consumers could promote consumer education for privacy.

Policies to promote innovation in privacy enhancing technologies

These following principles should be supplemented with technical guidelines from NIST; privacy enhancing technologies; safe harbors to protect product development, experimentation, and lawful operations; and a series of incentives for innovation.

1. The collection, use, storage and sharing of personal data should be **reasonably minimized** in a manner proportional to the scope of privacy risks.
2. Organizations should employ **security** safeguards to protect the data that they collect, store, use, or share.
3. Users should be able to reasonably **access and correct** personal data they have provided.
4. Organizations should take steps to **manage the risk** of disclosure or harmful uses of personal data.
5. Organizations should be **accountable** for the use of personal data that has been collected, maintained or used by its systems.

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.[26] 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.[27] As early as 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.[28]

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 & Information (NTIA) Administration, the National Institute of Standards and Technology (NIST), 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.[29]

Indeed, principles proposed by NTIA generally align with President Barack Obama's 2012 Consumer Privacy Bill of Rights.[30] The 2012 proposal also supported using multi-stakeholder processes to develop enforceable codes of conduct through Section 5 of the FTC Act. Importantly, the Obama administration was adamant about the need for preemption of state laws that would contradict the national standard. It expected states to participate in multi-stakeholder processes and believed that states proposing more stringent requirements would diminish incentives for firms to adopt the codes of conduct. Moreover, the administration wanted Congress to codify forbearance from enforcement of state laws for companies already compliant with the FTC's codes of conduct.[31]

The European Union Agency for Network Security and Information (ENISA, now the Cybersecurity Agency) 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.[32] 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.

Consider how technology and innovation could create better outcomes that prescriptive regulation. The GDPR has extensive reporting, auditing, and compliance requirements, necessitating that enterprises hire data protection officers and that data protection authorities hire workers. These requirements will vastly increase the virtual paperwork created and stored in databases, itself a data protection risk. If the goal is to ensure that entities are practicing data protection, a better system could include audit on demand or even auditable systems, which are software that expose the relevant information to those users who are interested, like ratings used on peer-to-peer platforms.

It could be that because privacy by design technologies are nascent, policymakers are reluctant to describe them in further detail, though this also contradicts the implicit assumption that data supervisors know best. However, the GDPR-chosen approach of regulation creates path dependency and inevitable outcomes. It clearly puts the thumb on the scale in favor of regulation over innovation.

Such frameworks can have indirect effects in that firms, concerned about inadvertently violating many of the tenets of the regulation and facing steep fines, will choose not to innovate. The GDPR's Article 25 on privacy by design and by default offers little in the way of incentives. There is no safe harbor for data processors to experiment or to implement new privacy by design technologies, so firms risk significant fines if their technologies fail, even if they have an entrepreneurial willingness to employ improved technologies.

Moreover, the GDPR and similar regimes with a priori restrictions for purpose specification, data minimization, automated decisions, and special categories are fundamentally incompatible with big data, artificial intelligence, and machine learning.[33] Some of the most important scientific advances have been the result of processing disparate sets of information in inventive ways, ways that neither subjects nor controllers anticipated, let alone requested. Consider the definitive study on whether the use of mobile phones causes brain cancer.[34] 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.[35] The study is the most comprehensive investigation proving that using mobile phones is not correlated with brain cancer.

Indeed, part of the promise of socialized medicine was tapping the big data in public health databases. However, a privacy panic[36] is threatening to derail some projects, for example 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.[37] While many privacy advocates like to focus attention on Silicon Valley firms and calls for greater regulation, the campaign is backfiring as users turn their ire toward government, demanding erasure of their data from national health care records and other government services, potentially frustrating the operating models of mandated social programs.[38]

With the mantra of "if in doubt, opt out," about half a million Australians en masse rejected the country's national electronic health record, causing the computer system to crash.[39]

A review of the literature on the impacts of economic regulation in the information communications technology sector shows a detrimental impact of regulation on innovation.[40] Regulation can create a deadweight loss in the economy as resources are diverted to regulatory compliance and away from welfare-enhancing innovation. A study across all major industries from 1997 to 2010 found that less-regulated industries outperformed overregulated ones in output and productivity and grew 63 percent more. Overregulation increases barriers to entry for entrepreneurs, which slows economic growth.[41] Moreover, regulation can crowd out efforts to create new and better systems.[42] For example, under the GDPR firms must employ privacy professionals, reducing revenue for engineers who can design and deploy privacy professionals.

My FTC submission goes into detail about types of privacy enhancing technologies (PETs) on page 8.[43] One approach is to focus on the minimization of data, the blocking the use of tracking tools, and the obscuring the user in the system, as we see with technologies for secure messaging, virtual private networks, anonymizing networks and anti-tracking tools for online browsing.[44]

On the other hand, a firm could consider taking the didactic, trust-based approach by disclosing and explaining how and why data is used. Customers who understand the role and use of the underlying data may grow more comfortable with it and use it even more. Privacy concerns can diminish with education and experience.[45] Similar to how people work with physicians and trusted advisors, there are valid reasons to enter data into systems so that both users and providers can make valid decisions. Indeed, some health platforms need intense data collection and sharing capabilities to deliver valuable healthcare support.[46] Consider the following tradeoff among cryptographic techniques,

> ". . . current PETs based on cryptographic techniques prevent unauthorized users from "viewing" the data, but typically reduce the efficiency of the algorithms by introducing storage and computational overhead that are often unacceptable. Whereas, PETs based on obfuscation techniques do not introduce computational overhead, but they reduce the accuracy (or utility) of the data hence are highly criticized by practitioners . . ."[47]

There is no one technology that addresses all the needs and challenges of data privacy and protection. As such, it is vital to encourage a range of technical solutions. It is important that policy encourages both bottom up and top down incentives. These can include grants,[48] awards,[49] and competitions.[50] Importantly, a national policy would include legal safe harbor for innovators so that they can experiment without punishment and so that enterprises can be confident that they are complying with the law.

Despite their benefits, there are significant barriers to the adoption of privacy enhancing technologies, not the least of which is complex regulation which makes it too difficult and uncertain for innovators to be sure they operate within the framework of the law. It is vital for American policymakers to stimulate innovative and creative capacity to improve current systems. Along with encouraging meaningful consumer education, innovation in privacy enhancing technology are the keys for the the US to leapfrog China and the European Union on data privacy and protection. The US will not lead if it merely copies the misguided California and European rules. It needs to make a superior framework.

Policy considerations to resource the FTC and the consumer protection functions of government

There is an important role for regulation to ensure privacy, but it is not as the GDPR mandates by imposing 45 requirements on the on the conduct of business and 35 associated requirements for regulators. At its core, consumer privacy is about securing fairness and equal treatment for all Americans. As such regulation should harmonize a rational set of privacy rules at the federal level which apply across all industries and technologies collecting personally identifiable information.

It is important to avoid the confusion and fragmentation which would result from 50 sets of rules. The residents of one state should not have a higher or lower standard than another, creating perverse incentives for firms and consumers to look for the least amount of friction to do business. Good regulation can also serve an important role to deter arbitrage and abuse by firms, politically-motivated state authorities, and self-interested litigants who abuse the law for pecuniary self-interest. Moreover, the harmonization of privacy rules at the federal level is vital to secure the proper funding and resourcing of the Federal Trade Commission and state level consumer protection authorities.

The legislative process should include an accounting of consumer protection resources at state and federal level to see how the expenditure can be strengthened and optimized. Precious consumer protection resources are currently squandered by duplicative agencies and redundant functions across federal and state authorities. Federal and state actors have worked cooperatively in the past and these relationships should be reviewed to highlight best practices and reduce overlap.

American taxpayers realize tremendous value from the FTC and its consumer protection and law enforcement functions, an agency that operates on a budget of roughly $300 million with 1140 employees.[51] Half of its budget is focused on consumer protection. Consider that it processes about 10 times as many robocall complaints as the Federal Communications Commission, the leading consumer complaint in the digital communications domain.[52] The FTC is clearly a workhorse of consumer protection and complaint adjudication, which is how most consumers know the agency. Indeed, the FTC's efficiency and effectiveness to deliver consumer protection could justify an increase to its budget and headcount. This could be achieved in part by incorporating lesser-performing federal consumer protection agencies into the FTC for greater effectiveness and savings.

Conclusion

NTIA plays a valuable role in the interagency policy process by conducting this request for comment. This submission emphasized the importance of recognizing that consumers are individuals with unique preferences, not monolithic actors who all want the same thing. It emphasized the importance of consumer education and privacy enhancing technologies both to supplement NTIA's principles and to provide competitive advantages which will allow the US to leapfrog the data protection regimes of the EU and China. To be the world leader, the US must legitimately empower consumers and privacy enhancing innovation. It also described important policy considerations to ensure efficacy including a single national standard enforced by the FTC, the proper resourcing of the agency, and clarification of the roles between FTC, state and federal agencies to avoid duplication of enforcement and the waste of resources.

[1] Roslyn Layton, "Statement before the Federal Trade Commission On Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions for Online Privacy" (FTC, August 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf.

[2] Roslyn Layton and Julian McLendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," *The Federalist Society* (blog), October 29, 2018, https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.

[3] Scott Meyer, "The Next $50 Billion Will Come From . . . Putting Users First," Ghostery Inc. , https://www.slideshare.net/ghosterybrand/the-next-50-billion-will-come-fromputting-users-first.

[4] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009), https://www.sup.org/books/title/?id=8862.

[5] "Acxiom Personicx," accessed November 9, 2018, http://www.personicx.co.uk/personicx.html.

[6] "Consumer and Household Segmentation | Personicx," Acxiom, accessed November 9, 2018, https://www.acxiom.com/what-we-do/consumer-segmentation-personicx/.

[7] Ibid

[8] Roger LeRoy Miller and Alan D. Stafford, *Economic Education for Consumers* (Cengage Learning, 2009). p. 88

[9] Willis, Lauren E. "Evidence and ideology in assessing the effectiveness of financial literacy education." *San Diego L. Rev.* 46 (2009): 415

[10] Connell, David B., Ralph R. Turner, and Elaine F. Mason. "Summary of findings of the school health education evaluation: Health promotion effectiveness, implementation, and costs." *Journal of school health* 55.8 (1985): 316-321.

[11] Supra Willis

[12] Layton, Roslyn, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944358 or http://dx.doi.org/10.2139/ssrn.2944358

[13] Claude Castelluccia and more, "Privacy, Accountability and Trust – Challenges and Opportunities — ENISA," Report/Study, Enisa, February 18, 2011, https://www.enisa.europa.eu/publications/pat-study/.

[14] See generally F. A. Hayek, "Economics and Knowledge," 1937; and F.A. Hayek, "The Use of Knowledge in Society," 1945.

[15] Douglas Busvine, Julia Firoretti, and Mathieu Rosemain, "European Regulators: We're Not Ready for New Privacy Law," Reuters, May 8, 2018, https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.

[16] Colin J. Bennett and Charles Raab, "The Governance of Privacy: Policy Instruments in Global Perspective," 2006.

[17] Charles D. Raab and Ivan Szekely, "Data Protection Authorities and Information Technology," *Computer Law and Security Review* (forthcoming), https://ssrn.com/abstract=2994898.

[18] Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust," March 31, 2018, 14, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

[19] Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust."

[20] Michael Chertoff, "Exploding Data: Reclaiming Our Cyber Security in the Digital Age," *Atlantic Monthly Press*, 2018.

[21] "Privacy and Security Enforcement," Federal Trade Commission, July 22, 2013, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

[22] Daniel Castro and Alan McQuinn, The Economic Cost of the European Union's Cookie Notification Policy, ITIF, Nov. 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.

[23] Adam Thierer and Chand Reese. "Evasive Entrepreneurs and Permissionless Innovation. The Bridge. Sep 11, 2018 https://www.mercatus.org/bridge/commentary/evasive-entrepreneurs-and-permissionless-innovation

[24] Roslyn Layton, "How Sharing Economy Regulatory Models Could Resolve the Need for Title II Net Neutrality," AEI, June 26, 2017, http://www.aei.org/publication/sharing-economy-regulatory-models-resolve-need-title-ii-net-neutrality/; And Arun Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism* (*MIT Press*, 2016)

[25] https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf

[26] Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe," 2015.

[27] 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/.
[28] 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.
[29] 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.
[30] White House Office: http://www.whitehouse.gov, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 23, 2012, https://www.hsdl.org/?abstract&did=.
[31] Roslyn Layton, "A Look at the Growing Consensus on Online Privacy Legislation: What's Missing?," AEI, October 29, 2018, https://www.aei.org/publication/a-look-at-the-growing-consensus-on-online-privacy-legislation-whats-missing/.
[32] 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.
[33] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review 47, no. 4 (2017): 2.
[34] Patrizia Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study," BMJ 343 (October 20, 2011), https://www.cancer.dk/dyn/resources/File/file/9/1859/1385432841/1_bmj_2011_pdf.pdf.
[35] Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study.
[36] Information Technology et al., "The Sky Is Not Falling: Understanding the Privacy Panic Cycle," Information Technology and Innovation Foundation, September 10, 2015, https://itif.org/events/2015/09/10/sky-not-falling-understanding-privacy-panic-cycle.
[37] 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.
[38] Bronwyn Howell, "Data Privacy Debacle Down Under: Is Australia's My Health Record Doomed?," AEI, August 6, 2018, http://www.aei.org/publication/data-privacy-debacle-down-under-is-australias-my-health-record-doomed/.
[39] Howell, "Data Privacy Debacle Down Under."
[40] Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross," Information Technology and Innovation Foundation, June 2010, 18, http://www.itif.org/files/2011-impact-regulation-innovation.pdf.
[41] Antony Davies, "Regulation and Productivity," Mercatus Center, May 7, 2014, https://www.mercatus.org/publication/regulation-and-productivity.
[42] Patrick McLaughlin and Richard Williams, "The Consequences of Regulatory Accumulation and a Proposed Solution | Mercatus," Mercatus Center, February 11, 2014, http://mercatus.org/publication/consequences-regulatory-accumulation-and-proposed-solution.
[43] https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf
[44] Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies – A Review of Tools and Techniques," November 15, 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#fn10.
[45] Michael M. Harris, Greet Van Hoye, and Filip Lievens Privacy and Attitudes Towards Internet-Based Selection Systems: A Cross-Cultural Comparison, 11 INT'L J. SELECTION & ASSESSMENT 230 (2003); Donna L. Hoffman, Thomas P. Novak, and Marcos A. Peralta, Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web, 15 THE INFO. SOC'Y 129 (1999); Philip J. Reed, Emma S. Spiro, and Carter T. Butts, Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures, 59 SOCIAL SCI. RESEARCH 155 (2016).
[46] Fabian Prasser et al., "Data Integration for Future Medicine (DIFUTURE)," Methods of Information in Medicine 57, no. S 1 (May 2018): e57–65, https://doi.org/10.3414/ME17-02-0022.
[47] Ibid
[48] Gayle Swenson, "NIST Awards Grants to Improve Online Security and Privacy," Text, NIST, September 17, 2013, https://www.nist.gov/news-events/news/2013/09/nist-awards-grants-improve-online-security-and-privacy.

[49] "PET Awards," accessed November 9, 2018, https://petsymposium.org/award/winners.php.

[50] Brianna Vendetti, "Prize Competition Winners Announced!," Text, NIST, September 14, 2018, https://www.nist.gov/news-events/news/2018/09/prize-competition-winners-announced.

[51] "FTC Submits Annual Budget Request, Performance Plan and Performance Report to Congress," Federal Trade Commission, February 12, 2018, https://www.ftc.gov/news-events/press-releases/2018/02/ftc-submits-annual-budget-request-performance-plan-performance.

[52] Roslyn Layton, "The Politicization of Consumer Protection," *US News & World Report*, March 16, 2017, https://www.usnews.com/opinion/economic-intelligence/articles/2017-03-16/the-politicization-of-consumer-protection-at-the-fcc-hurts-consumers.