Statement before the Federal Trade Commission
On Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions for Online Privacy

ONLINE SUBMISSION

ROSLYN LAYTON, Ph.D.
Visiting Scholar

August 20, 2018

August 20, 2018

The Honorable Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Mr. Simons:

Thank you for your leadership to hold these hearing on competition and consumer protection in the 21st century. It is entirely appropriate that as a new chairman in a new administration that you conduct this inquiry to determine whether and how "broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy."

My comments reflect my empirical research in questions of international internet policy conducted at the American Enterprise Institute in Washington, DC, and the Center for Communication, Media and Information Technologies at Aalborg University in Copenhagen, Denmark. The findings are my own and do not necessarily reflect the views of the institutions with which I am affiliated.

The comments are organized in the following sections.

1. How market solutions promote online privacy
2. The role of privacy enhancing technologies (PETs) in promoting online privacy
3. The role of consumer education in promoting online privacy
4. Additional policy considerations for online privacy

Thank you for the opportunity to participate in these hearings. A general discussion on competition is submitted under separate cover.

Sincerely,

Roslyn Layton, Ph.D.
Visiting Scholar
American Enterprise Institute
1789 Massachusetts Avenue NW
Washington, DC 20036

How Market Solutions Promote Online Privacy

Overview the FTC's role to maintain a competitive market. The FTC has demonstrated an ongoing commitment to online privacy. The main authority for privacy enforcement in the US is 15 USC § 45, which charges the Federal Trade Commission (FTC) with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[1] In matters of privacy, the FTC's role is to enforce privacy promises made in the marketplace.

The FTC has considerable power to police online privacy. It can order firms to cease and desist unfair trade practices. Its ability to penalize companies that harm consumers through unfair and deceptive practices formed a means of effective privacy protection. Indeed, the FTC has launched an investigation into whether Facebook violated its 2011 consent decree.[2]

Whereas the EU's General Data Protection Regulation assumes that any data collection is suspect, the FTC focuses its enforcement efforts on sensitive information that should be protected against unwarranted disclosure. This helps avoid imposing costly and draconian compliance mandates on entities that are not a priori threats to personal privacy, such as personal blogs, nonprofit organizations, or informational websites. The FTC's approach seeks to allocate scarce regulatory resources to prevent the greatest threats to online privacy. To be sure, if a small entity behaves in an unfair or deceptive way, it can be prosecuted, but the FTC does not assume that every entity wants to harm online users. Additional laws form the foundation on which the FTC carries out this charge including the Privacy Act of 1974,[3] the Gramm-Leach-Bliley Act,[4] the Fair Credit Reporting Act,[5] and the Children's Online Privacy Protection Act.[6]

The FTC took up some 200 privacy cases in 2017 alone.[7] In addition to its numerous enforcements on unfair and deceptive practices related to online privacy and education resources about online privacy, the FTC has hosted three consecutive annual conferences in which it attempts to solicit state of the art research in the field.[8] These conferences have grown in quality and depth, are vital, and should continue. Importantly, the FTC maintains an open door to receive research in the field at any time.[9]

Theories of Online Privacy. Online privacy can be seen from two competing paradigms. One model is that of rational choice, in which the individual weighs the cost and benefits of privacy and decides. The other view paints users as being at the mercy of external factors that determine whether they reveal or conceals themselves. The former tends to support solutions and technologies that empower consumers to make their own choices and suggests that firms, valuing their customers, will take proactive steps to steward their experience. The latter holds that privacy tools are inevitably unreliable and that firms take predatory advantage of users. According to this view, regulation is needed to keep firms in check and to protect consumers. Empirical tests of the two models show that consumers are not inevitably predisposed to making bad choice or failing to act in a privacy enhancing matter.[10] Research from 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.[11] As such, the opt-in regime is not empirically demonstrated as superior means of protecting the user's privacy. The point is merely that privacy is not a binary choice. There are many means and modes to secure, and its importance varies depending on the user and the situation. As such, policymakers should tread carefully before applying draconian regulations that may satisfy the most vocal privacy advocates but reduce benefits and utility for millions of consumers.

The Economics of Online Platforms. An understanding of online privacy needs to incorporate the study of online platforms, which is a fancy way to say a two-sided (or multisided) market. Platforms have existed for millennia, for example the village market that was a place where merchants met villagers or buyers.[12] Today's platforms are characterized by networks effects; that is, how increasing the size of one side of the market affects the other. Platform operators frequently incentivize different market sides to grow the size of the platform.

A key difference of today's platforms versus traditional retailers is that interaction between the various sides of the market is facilitated by the platform (Airbnb, Uber, etc.) allow the platform to collect significantly more information about the other parties. For example, a grocery store could film a shopper's visit and then study the store, the products viewed, and finally which products purchased. In years past, offline market researchers would survey shoppers about their experience. However, a shopping tour online is studied and recorded more efficiently, allowing the platform, for example Amazon, to make improvements to the platform, remarket to the customer, and provide the shopper with a range of information (past purchases, similar items, ratings, refunds, etc).

The platforms can collect and sort this information to facilitate the matching between the various parties, for example ratings of Uber riders and drivers. Publishing such information helps the parties make informed trades. The situation could also give rise to information asymmetry in that some parties have information about the others but not vice versa. However, having perfect information is probably impossible and likely undesirable.

Platforms provide many benefits to users, particularly in minimizing search costs. However, this may also give rise to so-called lock-in effect, when it becomes costly for the user to leave the service, for example how users tend to focus on the top Google search results on the page, even though the search engine may deliver thousands of possible answers to the query. To break lock in, consumers must find other ways to search, frequently requiring an incentive to do so. This is where free offers, flexible pricing, and zero rating of internet data may be helpful.

The internet is an "experience good," which means that its value cannot be ascertained until it is consumed. In markets with heterogeneous products, consumers with different preferences and information make it costly, if not impossible, for consumers to identify the attributes of the products or assess the fit vis-à-vis their preferences before the products have been consumed.[13] Similarly, the provider cannot accurately match the offer to the consumer without some amount of trial and error. This process of the user switching, learning, and adjusting comprises a user's "search costs." The larger the search costs, the smaller the expected benefit of the second product over the first, and the less likely it is that the consumer will try to find a better match, even though there is definitely a better one out there. Thus, high search costs lead to suppliers having some market power over their existing customers—even though there are many different variants of the product available. Thus, regulators should keep in mind that free data may be helpful to reduce the user's search costs to find alternative applications and to lower entrance barriers for entrant applications.[14]

Data are unlike traditional goods and services in that they are frequently non-excludable and non-rivalrous, making the traditional application of economics and property rights slightly challenging. However, this represents an opportunity for the evolution of markets. We should encourage and expect market solutions to emerge.[15] Indeed, some regulation and regulatory norms, for example price controls which require that consumers pay the full cost of broadband, may have deterred this market development.

The study of platforms can be further extended to whether it creates bottlenecks for content providers and merchants and whether these actors have other means to reach ends users and how effective they are. Moreover, the entire digital market is characterized by regulatory discrimination as traditional content and communications providers must compete under obsolete legacy regulation whereas the new software platforms have no such obligations. It is a key debate within the internet policy field whether antiquated regulation should be applied to the software platforms or whether after long last, policies for broadcast, cable, and telecom providers can be modernized so that they are granted the same freedoms of permission-less innovation as the software platforms. In 2014 Congress undertook a bona fide effort to update the Communications Act, which governs the sector, scuttled unfortunately by an Federal Communication Commission (FCC) effort to reregulate the telecom sector; the effort should be revisited as soon as possible.[16]

Market Responses Offer Swift Feedback to Firms and Preserve Consumer Sovereignty, Frequently More Effectively Than Regulation. There has long been a tension between market and regulatory responses to problems when it comes to privacy. Consider that in response to telemarketing, consumers started to deploy technologies to uncover the identity of callers. Many privacy activists decried these efforts, saying that the technologies violated the privacy rights of the callers. However, today the prevailing view is that those on the receiving end of the call have the right to be informed of who is calling.[17]

This view underpins consumers' ethos to robocalls today, the leading consumer complaint at both the FCC and FTC. However, regulation to combat robocalls has likely increased rather than reduced the problem. Unwanted automated calls have exploded to more than two billion per month. Considerable resources are spent by regulatory agencies in processing complaints. The fastest way to stop the problem is through technology, allowing networks and users to employ techniques to block unwanted calls.

Policymakers took a different path to address the problem through the 1991 Telephone Consumer Protection Act (TCPA). But robocall perpetrators easily escape regulation by moving offshore or shifting technology to evade regulators. Unwittingly, the TCPA has given rise to a class-action lawsuit industry, driving thousands of suits per year, ensnaring unsuspecting actors that attempt to adhere to TCPA but unwittingly end up violating it. Given that the TCPA regulates speech, it is increasingly scrutinized under the First Amendment.[18]

The tension between the seeming right to privacy and the right to be informed is also implicated by the General Data Protection Regulation (GDPR).[19] A key example is WHOIS, the query and response protocol used to identify those who register domain names, now masked by the GDPR. Law enforcement, cybersecurity professionals and researchers, and trademark and intellectual property rights holders have a vital interest in the transparency of WHOIS.[20] "The publicly available data that is used to inform threat intelligence networks, find bad actors, and block them from accessing networks will no longer be available under the GDPR," notes AEI's Shane Tews.[21]

On the internet, browser and cloud-based ad blocking technologies have been used by millions of users globally to reduce exposure to unwanted ads, reduce the cost of mobile subscriptions, and increase privacy, security, energy efficiency, and usability to speed the running of mobile apps and websites.[22] Blocking technologies have arguably been more effective than regulations such as the EU's ePrivacy Directive (Cookie Law")[23] to signal to advertisers to improve the design, quality, and delivery of advertisers; the Internet Advertising Bureau adopted the Light, Encrypted, Ad Choice, Supported, and Non-Invasive (LEAN) program for advertising as a result.[24] The EU's Cookie Law, which creates a pop-up the first time a person visits an EU-based website, costs businesses $2.3 billion annually in lost sales and productivity with no meaningful improvement for users' privacy or experience.[25]

User response to Facebook is also instructive in the fake of the Cambridge Analytica revelation. The tech media paints a picture of a mass exodus against Facebook, but the data tell another story. Daily active users (DAU) on Facebook in US and Canada have held steady for the past year in spite of the press coverage.[26] It appears that millions of US Facebook users either do not know or are not concerned about the Cambridge Analytic scandal.

For all the castigation against the company for so-called fake news, the platform has gained give million DAU since the 2016 election. While Europe lost three million DAUs last quarter (the first time a decline has been recorded in two years, a likely outcome of the GDPR), DAU increased in last quarter in the rest of the world. This is not to say that there are not concerns about the platform. Indeed, a recent poll reports that two-thirds of older Americans (age 53–72), the demographic that reliably votes in all elections, want tech companies to be regulated like big banks, even though respondents overall have some doubts about whether governments can successfully regulate such firms.[27] But it does suggest that policymakers need to be careful about generalizing about all Facebook users and adopting policies predicated on an incorrect understanding of its diverse users.

Privacy advocates would likely describe most Facebook users as suffering from a "privacy paradox" (understanding the value of privacy but failing to practice privacy enhancing behaviors), but the reality may be more likely that users accept the trade-offs. Many users get value from Facebook; they like having their family and friends, photo albums, and messaging all in one place. Like how advertising supported analog television, radio, and print, they understand that advertising and data collection

underpin the platform and make the valuable services possible. Naturally, they expect to be treated well but do not necessarily expect that there will never mistakes or problems. Indeed, users may be more interested to see how Facebook responds to situations by making improvements to the platform, rather than quitting outright. This may be related to Facebook having a resilient "brand personality" in that users understand that it is an imperfect and evolving platform. Indeed, Facebook experienced an increase in engagement from US users following the Cambridge Analytica revelation, as users went online to change their privacy settings.[28]

However, many US users quit Facebook. A recent Hill Holliday survey of Generation Z (those born from 1994 and after) shows that so-called digital natives, which are estimated to comprise 40 percent of US consumers by 2020 and of whom more than 90 percent use social media platforms, found that more than one-half switch off social media for extended periods and one-third canceled their social media accounts.[29] Users cited time wasting as the reason for quitting twice as often as a concern about privacy. While service providers may not like high rates of churn experienced among social media platforms,[30] it reveals a competitive market in which consumers find it easy to leave and desire experience other platforms with different features.

Additionally, reports suggest that some forms of user engagement are declining.[31] This could be related to Facebook changing its model to emphasize posts from family and friends over news.

The most significant market response was the company losing $119 billion following its second quarter financial results, the biggest market value drop for a company on a single day in US history.[32] This amount is roughly 10 times the maximum fine that authorities could apply on the company under EU's GDPR. Facebook's shareholders have demanded leadership changes[33] and have lodged lawsuits against the company.[34]

As for the discontent that remains, AEI's Mark Jamison observes,

> Users are upset because they're surprised and dismayed by revelations about how tech companies use people's data. They feel they lost something that was rightfully theirs. Social media companies should meet this disillusionment head on. Accept the public outcry as a mandate for change before governments overstep. Engage with users openly. Tell them what has been going on and what is currently going on in ways that respect their time and intelligence. And remind people about the true relationship between the tech company and user.[35]

Some companies have turned crises into opportunity. Consider Tylenol, the most popular over-the-counter product in 1982, used by 100 million and accounting for 20 percent of Johnson & Johnson's revenue. Following the revelation that its product was with cyanide, the company immediately recalled all its products and demonstrated that it prioritized safety over profit.[36] Rather than blame the company for the default, which killed seven people, public opinion leaned to the view that the firm was victim of a crime. Indeed, the case of who and how the tampering occurred is still unknown to this day. Following the incident, the firm worked with the Food and Drug Administration to introduce innovations to reduce the ability to tamper with medicines such as foil seals and gelatin-coated "caplets."[37] Thereafter, Congress passed legislation to make it illegal to tamper with consumers products and the Food and Drug Administration–established tamper-proof guidelines. The company has long enjoyed the ranking of the most respected pharmaceutical company.[38]

The story offers a few lessons for the digital space. While these efforts have significantly reduced the probability of tampering, it still happens. For actors that are intent on doing bad things to harm others, rules and regulations are not necessarily a deterrent. Ultimately, technology innovation performs the lion's share of consumer protection, and policy needs to be flexible to allow solutions to emerge. Industry and regulators can work collaboratively to solve problems, but it should not be assumed that regulators inherently have the best solutions or even the right information. As the next section describes, dozens of technological means can improve online privacy. If regulators demand one approach above others, they risk making the wrong choice and deterring a range of solutions, which can bring better outcomes for consumers.

Market Solutions Comprise Three of the Four Crucial Inputs to Creating Trust Online. The European Union Agency for Network and Information Security (ENISA) produced an official report about how to create trust online, noting that trust is a function of four key inputs, the knowledge of the end user, the level and type of technology, business practices, and institutions (the laws and policies that govern the system).[39] The ideal policy incorporates all elements and offers a flexible balance that allows privacy enhancing innovation to emerge. Policies that incorporate only some of the elements or overemphasize some elements to the exclusion of others are not optimal and potentially harmful.

Unfortunately, in the promulgation of the GDPR, the EU did not incorporate the advice of its official research institute, notably the importance of consumer education and innovation in privacy-enhancing technologies.[40] After a decade of GDPR-type regulations across the EU, consumers report only a marginal increase in trust online. As of 2017 only 22 percent of Europeans shop outside their own country (a paltry increase of 10 percent in a decade), suggesting that the European Commission's Digital Single Market goals are still elusive.[41] Moreover, only 20 percent of EU companies are highly digitized.[42] These are primarily large firms. Small- to medium-sized companies invest little to modernize their business and market to other EU countries. The US should not make the same mistakes as the EU in failing to investigate the empirical research and failing to test whether their policies are achieving their promises.

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.[43] 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.[44] 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.[45]

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 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.[46]

ENISA's 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.[47] 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 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.[48] 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.[49] 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.[50] 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[51] 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.[52] 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.[53] 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.[54]

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.[55] 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.[56] Moreover, regulation can crowd out efforts to create new and better systems.[57] For example, under the GDPR firms must employ privacy professionals, reducing revenue for engineers who can design and deploy privacy professionals.

Description of PETs. Following is a brief overview of examples of PETs. This represents just a sliver of a vast and growing field that needs to be properly evaluated considering policymaking on online privacy. Many of the technologies emerge from the cybersecurity domain, which endeavors to protect hardware, software, and data from theft, disruption, and misdirection. Additional technologies not discussed include privacy enhanced data mining, computations, intervenability, and information retrieval.

Encryption. *Encryption is a process of encoding information that only authorized parties can access it. While it does not prevent interference with data transmission, it can deny access to unauthorized parties. Encryption allows users to protect the privacy and integrity of their information, so that it cannot be viewed by others. The Secure Socket Layer and Transport Layer Security are cryptopgraphic protocols that provide security for communications over computer networks.*

Encryption is particularly important in the cloud storage setting in which many documents are gathered. Such environments entail risk from identity thieves, possible illicit and unlawful review of documents by cloud providers, and even government surveillance.[58] As such, firms compete on providing secure storage environments.

A related tool is the digital signature, a mathematical, cryptographic means to preserve the integrity of messages, verify a known sender, and ensure that the sender cannot deny having sent the message (non-repudiation). Digital signatures are used for software distribution, financial transactions, and software to minimize forgery and tampering.

Data Minimization. *Data minimization is the notion of using the least possible amount of information to make the service or application applicable to the user. This can be as simple as the service not requesting information of the user that is not relevant to the transaction. Users can also deploy tools such as the Privacy Eraser, which deletes browsing history, caches, cookies, entered data, forms, passwords, and other sensitive information.[59] Some browsers support "private browsing" so that data are not stored on the computer. Messaging services such as Snapchat and Firechat create only minimal information, which is automatically deleted.[60]*

Authentication. *Authentication is the process of confirming the veracity of data and identity. This is a means to protect users and systems from unauthorized users and uses of services. It can involve multiple factors, layered approaches, and continuous verification.*

Attribute-Based Access Control. *Attribute-based access control (ABAC) is a dynamic, context-aware and risk-intelligent method of access granted based on the use of specific policies and attributes (e.g., if, then). For example, ABAC can be used to determine whether a person is of a minimum age of 18 before purchasing alcohol or that a rider on public transportation is eligible for the senior citizen discount. Such methods eliminate the introduction of unnecessary personal information. They can also be used to generate a verified token for the consumption of services without compromising personal information. Examples of ABAC include Goethe University's Privacy-ABCs, IBM's Idemix, and Microsoft's U-Prove.*

Anonymization. *Anonymity is the notion of wanting others to see one's action, but not one's identity. Anonymization of communication takes place by concealing the identity of the user and other personal information. Instead, they are replaced by non-traceable options. For example, the user can engaged with an anonymous one-time email address or random internet protocol (IP) address.[61] Anonymization is typically used for emails, web browsing, IP telephony, chat, etc.*

Anonymous credentials allow a user to consume a service without revealing personal identify. For example, a car rental provider need not know the identity or name of the customer, only that the customer is of minimum legal age and has a driver license, car insurance, and a method of payment.

The notion of privacy on its face seems to contradict the business of personalization and derivative services (e.g., loyalty programs). Indeed, many consumers like firms to personalize services to them, for example the shop owners who recognize frequent customers and say hello upon their entering the store and personalized online communications. Services for health and fitness, financial planning, and personal shopping are predicated on customers' unique personal attributes and would be undesirable, even harmful, if they were based on generalized information (e.g., making health recommendations to children based upon information for adults). On the other hand, there are efforts to design privacy-aware loyalty program using anonymization techniques.[62] The point is that the government should not mandate one method or another but allow providers and consumers to gravitate to those models to which they prefer.

Part of the value of the US approach to date is that the regulation of privacy is predicated on the sensitivity of information. Unlike the European approach, which considers all data collection suspect and all data collectors nefarious, the US has defined regulations for knowingly sensitive domains such as health, finance, and children. This is prudent and fiscally responsible approach to focus expertise and resources to known risks.

Service-Level Agreements and Tools to Enable Transparency and Choice. *Many firms are increasingly transparent about how they manage data and provide options for users to decide how personal data are to be managed. Greater software sophistication and user-centric design allows consumers choice to select and specify how data can be managed and transferred, whether they can be shared with third parties and under which conditions, how and when data should be deleted and so on. Moreover, users can audit or change these conditions at will. Users need not rely on companies' promises; independent transaction logs can verify that requested conditions have been fulfilled.*[63]

Consider Ghostery, the privacy and security mobile browser and extension app that detects and blocks third-party data-tracking technologies. Its seven million users manage privacy with downloadable transparency tools and many active in policy discussion.[64]

These are but a few examples of promising technologies that can promote privacy and drive competition among firms. As described in the next section, coupling privacy enhancing innovation with consumer education is an effective means to empower consumers to drive the optimal privacy outcomes.

Momio: A Social Network for Kids Built with Privacy. *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.*[65] *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, literacy, and rights.*

The Role of Consumer Education in Promoting Online Privacy

Consumer education is tacit recognized as important, but it a fragmented field, frequently disconnected from policy. Canadian home economist and consumer studies educator Sue McGregor offers an authoritative academic review of the field of consumer education. [66] She describes consumer education as a means of protecting consumers as economic actors and empowering them with the political, ethical, and moral aspects of consumption (behavior) and consumerism (ideology) and observes that the concept has been extant for 120 years. A variety of theories explain the need for consumer education. For example, the market does not provide enough education, so information needs to be stimulated. Another view is that consumers demand "uncensored" information about the market. Another view posits that education is the path to consumer activism, so information is promoted by interested parties. Others define consumer education as a conceptual innovation. A modern view of consumer education describes it as a function of decision-making, personal resource management, and citizen participation in the policy process.

In recent decades the notion of consumer education has been likened to human right (1960s), a model of postindustrial economics, people no longer producing their own goods (1970s), the business paradigm of consumer as client (1980s), the public-private partnership for consumer

education, indeed a concept promoted in the 1996 Pitofsky report[67] (1990s), and in the 2000s, consumer education vis-à-vis globalization and the policy process. Most recently the field has incorporated complexity theory. Despite this evolution, consumer education remains a fragmented endeavor with certain areas getting significant attention, for example financial literacy and smoking cessation, while other important areas are not discussed. There is also the view of the politicization of consumer education, for example that centrally planned disclosure for nutrition information on food satisfies regulators' expectations but fails to be meaningfully adopted by consumers.[68] This suggests that for consumer education to be meaningful it needs to bottom-up or at least be holistic.

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, the many providers of phones, devices, appliances, and so on advertise in popular publications, host discussions, and so on. Online platforms do not advertise as such. A valuable policy research project could investigate how to stimulate a market for consumer education on privacy and some recommendations follow in this paper.

In any event, without consumer education on privacy it is difficult to expect all consumers to fully understand what to consent when agreeing to typical terms of services. The disclosures could be simplified and updated in more consumer-centric language and format.

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 its role. Indeed, if consumers are empowered to make informed choices, they have less need of regulators' supervision. Similarly, consumers making informed choices also affects industry; it has a powerful effect to drive consumers from one firm to another.

The European Union's GDPR is suspect in that among 173 provisions the role and importance of consumer education is never discussed. This is likely because the regulation is in part a make-work program for 75,000 new privacy officers and the employees of 62 data protection authorities. The GDPR assumes that regulatory authorities have more information than consumers and firms and therefore know better how to order transactions in the marketplace.[69] All the same, the GDPR imposes massive new responsibility on regulators without a concurrent increase in training or funding.[70] EU data

supervisors must wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."[71] Furthermore, the GDPR widens the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.[72] There are certainly many talented individuals among these ranks, but the mastery of information communication technologies varies considerably among these professionals, especially as each nation's data protection authority is constituted differently.

Public choice theory also suggests that the EU data supervisors' preferences are not necessarily aligned with the "public interest," or what is best for European 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 supervisors 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.[73]

A number of surveys demonstrate that many users fail to practice basic privacy-enhancing behaviors.[74] 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 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."[75] 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 the disclosure has little impact.

As such, the GDPR rests on a fallacy that making consent more explicit makes consumers more informed. The GDPR requires enterprises to make consent ever more detailed, burdensome, and granular without increasing the user's holistic knowledge of the transaction. This creates an increasing chasm between consumer empowerment and bureaucratic control. It is like speaking more loudly to a person who speaks another language in the hope that she will better understand.

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 would like impugn the failure 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.[76]

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.

Tapping the FTC's Consumer Education Resources. The FTC already has significant educational resources to help consumers protect themselves online in the privacy, identity and online security sections of its website.[77] It would be worthwhile to see how this information could be shared, syndicated, and amplified, for example through social media by users themselves. Even if no further policy was enacted at all, people could read the FTC section on protecting kids online and learn many things about being more responsible and protecting one's privacy. Essentially, the very restraint that parents are to apply to children, they should apply to themselves.

Moreover, there is nothing is to stop any privacy advocacy organization, philanthropic charity, school, trade association, or company from presenting a similar list or linking to the FTC's information. They do not have to ask permission; they do not need to wait for legislation. Information can be made available to consumers today.

The section on limiting unwanted calls and emails is quite detailed noting privacy choices for your personal financial information; stopping unsolicited mail, phone calls, and email; blocking unwanted calls; robocalls; the do not call registry; phone scams, telemarketing rules; and reducing spam on email and SMS. These include common sense tips such as using email filters, limiting exposure of one's email address, changing privacy settings, choosing unique email address, detecting and removing malware, and reporting spam.

The section on protecting kids online delves into cyberbullying, how parents can talk with kids, and basic security such as peer-to-peer file sharing, phishing, and downloading apps. Indeed, these pointers could easily be extended to adults. Some of these settings could be defaults for first-time adult users until they become more familiar. There are privacy-enhanced devices apps for children, so there is no reason why they cannot be designed for adults. Features include programmable limitation on services, emergency buttons, time management controls, filtering software applied to ensure that users do not share personal information or content. Just as parents develop rules for their kids, they should live by their own rules, limiting their use at family times, in the evening, etc. But they can also be more diligent about their behavior. Adults should be cautious in what they post, whether text, picture, or video. They should use "good judgment."

The OECD's International Cooperation on Consumer Education for Online Privacy. More than a decade ago various private and public organizations have outlined the role of consumer education in online privacy, but this thinking and educational assets have not been meaningfully incorporated into policy. Notably, the Organisation for Economic Co-operation and Development (OECD) published a study on Consumer Education for Digital Competence.[78] Key learning points include:

- Linking the concept of digital competence with critical thinking on technology and the media,
- Educating to provide a basis for developing an understanding of the structures and conceptual relationships understanding digital media (e.g., functioning of online market, e-commerce marketing techniques, and user tools),
- Learning the how and why of protecting personal information when using digital media,
- Using media to promote the education of digital competence in compelling ways (e.g., games, videos, blogs, and virtual worlds),
- Age-appropriate education,
- Implementing teacher training, and

- Strengthening multi-stakeholder cooperation to create educational partnerships.

The OECD also published a book to describe prevailing consumer education practices across the member nations, including the institutional frameworks and policy evaluation tools.[79]

Institute for Privacy Protection at Seton Hall University. Gaia Bernstein, director of the Institute for Privacy Protection and codirector of the Gibbons Institute of Law Science and Technology at Seton Hall University observes, "We can take action to regain control of our time, attention and social interactions."[80] The center offers training for teachers and other leaders about how to empower users to manage their privacy. The core curriculum is based on the concept of explaining the concept of privacy, digital footprints and reputation, ads and content choice, and online versus offline balance.[81]

Teaching Privacy Curriculum. For example, in the US, the "Teaching Privacy Curriculum" by Serge Egelman et al. offers interactive instruction on 10 principles of online privacy over three weeks in a university setting, a method that has also proved effective to educate and empower users to manage their privacy.[82]

Additional Policy Considerations for Online Privacy

Incentives to PETs. Americans can develop better privacy regimes through science, technology, and innovation. Policymakers should consider the role of incentives for design and experimentation with PETs. These can include partnerships for grants, prizes, award, and competitions. Importantly, any kind of privacy policy or legislation should include a legal safe harbor for PET innovation to ensure that innovators can innovate without punishment.

Consumers Enjoy and Expect a National Privacy Framework. To date, consumers have enjoyed common rules for privacy protection across the US with particular kinds of information being regulated because of their sensitivity. It is important that this standard be maintained with any new policy, regulation, or legislation. From the beginning, the US has been a de facto digital single market with a common language, currency, and policy. This has supported interstate commerce and the permission-less innovation for any startup to create a website, service, or application online. Some states in the show of symbolic politics are making up their own internet and privacy rules. These are dangerous and misguided efforts which will confuse consumers, possibly violate the Constitution and Communications Act, and frustrate interstate commerce.[83] Congress should preempt efforts by the states to pursue state level privacy policy.

Avoiding the Abuse of Privacy Class Action. My forthcoming paper for the Federalist Society details how various parties abuse data protection regulation as a form of political and economic rent-seeking.[84] The GDPR legislation was reverse engineered to exploit the standard European judicial jurisdictions and to allow litigants to bring users outside of the EU into lawsuits. Today, firms and data protection authorities now suffer the automation of complaints from bots and belligerent users, swelling the complaint channels with thousands, if not millions, of requests in a day. Moreover, litigants, under the blanket of nonprofit corporate status, are motivated to seek billions of dollars in damages by suing firms and keep the winnings on users' behalf. It is expected that lawsuits will take years to resolve, a cost borne by taxpayers to fund.

The US has a superior model in which the FTC can work with state attorneys general to make coordinated action where necessary. It is important that the US maintain the primacy of the FTC and ensure a common national standard for online privacy. If need be, Congress could strengthen the FTC's ability to apply civil penalties for privacy violations.

---

[1] 15 USC § 45 (2012).
[2] Federal Trade Commission, "Facebook, Inc.," November 29, 2011, https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.
[3] 5 USC § 552a.
[4] 15 USC §§ 6801-6809.
[5] 15 USC § 1681 et seq.
[6] 15 USC §§ 6501-6506.
[7] Federal Trade Commission, "Privacy & Data Security Update: 2017," January 2017–December 2017, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.
[8] Constitution Center, "PrivacyCon 2018," Federal Trade Commission, June 6, 2017, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018.
[9] See Constitution Center, "PrivacyCon 2018: Call for Presentations," Federal Trade Commission, June 6, 2017, https://www.ftc.gov/node/1223293. The FTC notes, "We invite you to send in your research to research@ftc.gov if you are interested in discussing your research with us or have further questions."
[10] Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," April 14, 2016, https://ssrn.com/abstract=2765097.
[11] 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.
[12] Bertin Martens, "An Economic Policy Perspective on Online Platforms," Joint Research Center, 2016, https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf.
[13] Phillip Nelson, "Information and Consumer Behavior," *Journal of Political Economy* 78, no. 2 (1970): 311–29.
[14] Roslyn Layton, "4 Questions Regulators Should Ask on Zero Rating and Free Data," American Enterprise Institute, September 27, 2016, http://www.aei.org/publication/4-questions-regulators-ask-zero-rating-free-data/. For a longer discussion see Bronwyn E. Howell and Roslyn Layton, "Evaluating the Consequences of Zero-Rating: Guidance for Regulators and Adjudicators" (The 44th Research Conference on Communication, Information and Internet Policy 2016, August 2016), https://ssrn.com/abstract=2757391.
[15] Nadezhda Purtova, "Property Rights in Personal Data: Learning from the American Discourse," *Computer Law and Security Review* 25.6 (2009): 507–21.
[16] Richard Bennett et al., "Comments on Communications Act Modernization," January 31, 2014,https://ssrn.com/abstract=2388723.
[17] See Justin "Gus" Hurwitz and Jamil N. Jaffer, "Modern Privacy Advocacy: An Approach at War with Privacy Itself?, Regulatory Transparency Project of the Federalist Society," June 12, 2018, https://regproject.org/paper/modern-privacy-advocacy-approach-war-privacy/.

[18] Hurwitz, Gus. Telemarketing, Technology, and the Regulation of Private Speech. 2018. Forthcoming Brooklyn Law Review.
[19] Shane Tews, "Privacy and Europe's data protection law: Problems and implications for the US". AEI.org May 8, 2018. http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/
[20] Shane Tews. "How European data protection law is upending the Domain Name System." American Enterprise Institute. February 26, 2018. https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/
[21] Supra Tews May 2018
[22] Roslyn Layton, "User Rights, Ad Blocking and Net Neutrality." Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management. Annual Report of the UN IGF Dynamic Coalition on Net Neutrality, 2016.
https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/17532/Net%20Neutrality%20Reloaded.pdf p. 183
[23] "Cookies - European Commission," EU, accessed August 20, 2018, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm#section_2.
[24] Interactive Advertising Bureau, "IAB Tech Lab Solutions," accessed August 20, 2018, https://www.iab.com/iab-tech-lab-solutions/.
[25] Daniel Castro and Alan McQuinn, "The Economic Cost of the European Union's Cookie Notification Policy," ,Information Technology and Innovation Foundation, November 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.
[26] Facebook, "Facebook Q2 2018 Results," https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q2-2018-Earnings-Presentation.pdf.
[27] HarrisX, "Inaugural Tech Media Telecom Pulse Survey 2018," April 2018, http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf.
[28] Daniel Turdiman, "Facebook Engagement Surge Post-Cambridge Analytica," Fast Company, April 24, 2018, https://www.fastcompany.com/40563518/why-facebooks-engagement-surged-after-cambridge-analytica.
[29] Hill Holliday, "Meet Gen Z: The Social Generation," last visited June 25, 2018, http://thinking.hhcc.com/?utm_campaign=Thought%20Leadership%20%E2%80%94%20Gen%20Z&utm_source=Press%20Release.
[30] Connie Hwong, "Why Churn Rate Matters: Which Social Media Platforms Are Losing Users?," Verto Analytics May 4, 2017, https://www.vertoanalytics.com/chart-week-social-media-networks-churn/.
[31] Ryan Erskine, "Facebook Engagement Plunging Over Last 18 Months," August 13, 2018, *Forbes*, https://www.forbes.com/sites/ryanerskine/2018/08/13/study-facebook-engagement-sharply-drops-50-over-last-18-months/#69c1de5794e8.
[32] Fred Imbert Francolla Gina, "Facebook's $100 Billion-plus Rout Is the Biggest Loss in Stock Market History," July 26, 2018, https://www.cnbc.com/2018/07/26/facebook-on-pace-for-biggest-one-day-loss-in-value-for-any-company-sin.html.
[33] Trillium Asset Management, "Facebook, Inc. — Independent Board Chairman (2019)," accessed August 20, 2018, http://www.trilliuminvest.com/shareholder-proposal/facebook-inc-independent-board-chairman-2019/.
[34] Owen Bowcott and Alex Hern, "Facebook and Cambridge Analytica Face Class Action Lawsuit," *Guardian*, April 10, 2018, https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.
[35] Mark Jamison, "Guest Post: How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?," Facebook Newsroom, accessed August 20, 2018, https://newsroom.fb.com/news/2018/08/guest-post-mark-jamison/.
[36] Department of Defense, "Case Study: The Johnson & Johnson Tylenol Crisis," accessed August 20, 2018, https://www.ou.edu/deptcomm/dodjcc/groups/02C2/Johnson%20&%20Johnson.htm.
[37] Howard Markel, "How the Tylenol Murders of 1982 Changed the Way We Consume Medication," *PBS NewsHour*, September 29, 2014, https://www.pbs.org/newshour/health/tylenol-murders-1982.
[38] Johnson & Johnson, "Johnson & Johnson Named a 2018 Fortune World's Most Admired Company," January 19, 2018, https://www.jnj.com/latest-news/johnson-johnson-named-a-2018-fortune-worlds-most-admired-company.

[39] European Union Agency for Network and Information Security, "Privacy, Accountability and Trust- Challenges and Opportunities," February 18, 2011, https://www.enisa.europa.eu/publications/pat-study.
[40] Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability and Trust," March 31, 2017, https://ssrn.com/abstract=2944358.
[41] European Commission Report, "Use of Internet Services," 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf.
[42] European Commission Report, "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.
[43] Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe," 2015.
[44] 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/.
[45] 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.
[46] 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.
[47] 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.
[48] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47, no. 4 (2017): 2.
[49] 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.
[50] Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study.
[51] 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.
[52] 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.
[53] 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/.
[54] Howell, "Data Privacy Debacle Down Under."
[55] 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.
[56] Antony Davies, "Regulation and Productivity," Mercatus Center, May 7, 2014, https://www.mercatus.org/publication/regulation-and-productivity.
[57] 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.
[58] Alan Henry, "The Best Cloud Storage Services That Protect Your Privacy," Lifehacker, accessed August 20, 2018, https://lifehacker.com/the-best-cloud-storage-services-that-protect-your-priva-729639300.
[59] "Privacy Eraser & Privacy Drive - Privacy & Security Software," accessed August 20, 2018, http://www.cybertronsoft.com/.
[60] Pardis Emami-Naeini and more, "Privacy Expectations and Preferences in an IoT World" (Privacycon, 2018), https://www.ftc.gov/system/files/documents/public_events/1223263/panel09_privacy_in_iot.pdf.
[61] Steven Englehardt, "I Never Signed Up for This! Privacy Implications of Email Tracking" (Privacycon, 2018), https://www.ftc.gov/system/files/documents/public_events/1223263/panel01_never_signed_up.pdf.
[62] Milica Milutinovic et al., "An Advanced, Privacy-Friendly Loyalty

System"; Marit Hansen et al., "Privacy and Identity
Management for Emerging Services and Technologies," June 17–21, 2013, 128–38,
https://link.springer.com/book/10.1007/978-3-642-55137-6.
[63] Giridhari Venkatadri et al., "Privacy Risks with Facebook's PII -Based Targeting," Privacycon, 2018,
https://www.ftc.gov/system/files/documents/public_events/1223263/panel05_privacy_risks_fb_pii.pdf.
[64] Ghostery, " The Purple Box," accessed August 20, 2018, https://www.ghostery.com/blog/.
[65] Momio, "About Momio," http://company.momio.me/about-us/
[66] Sue L. T. McGregor, "Framing Consumer Education Conceptual Innovations as Consumer Activism," *International Journal of Consumer Studies*, 2015,
http://www.consultmcgregor.com/documents/research/consumer_activism_published_ijcs.pdf.
[67] Federal Communication Commission, "Anticipating the 21 Century: Consumer Protection Policy in the New High-Tech, Global Marketplace" May 1996, https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf.
[68] S. Hieke and C. R. Taylor, "A Critical Review of the Literature on Nutritional Labeling," *Journal of Consumer Affairs* 46, no. 1 (2012): 120–56.
[69] See generally F. A. Hayek, "Economics and Knowledge," 1937; and F.A. Hayek, "The Use of Knowledge in Society," 1945.
[70] 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.
[71] Colin J. Bennett and Charles Raab, "The Governance of Privacy: Policy Instruments in Global Perspective," 2006.
[72] Charles D. Raab and Ivan Szekely, "Data Protection Authorities and Information Technology," *Computer Law and Security Review* (forthcoming), https://ssrn.com/abstract=2994898.
[73] 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.
[74] Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust."
[75] Michael Chertoff, "Exploding Data: Reclaiming Our Cyber Security in the Digital Age," *Atlantic Monthly Press*, 2018.
[76] 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)
[77] Federal Trade Commission, "Privacy, Identity & Online Security," https://www.consumer.ftc.gov/topics/privacy-identity-online-security
[78] Organisation for Economic Co-operation and Development, "Consumer Education Policy Recommendations of the OECD'S Committee on Consumer Policy," 2009, http://www.oecd.org/sti/consumer/44110333.pdf.
[79] Organisation for Economic Co-operation and Development, "Promoting Consumer Education: Trends, Policies and Good Practices — OECD," March 2009,
http://www.oecd.org/sti/consumer/promotingconsumereducationtrendspoliciesandgoodpractices.htm#howto.
[80] Gaia Bernstein, "About the Over-Users," accessed August 20, 2018, http://gaiabernstein.com/.
[81] Seton Hall, "Institute for Privacy Protection's School Outreach Program,"
https://law.shu.edu/about/news.cfm?customel_datapageid_6255=537438.
[82] Serge Egelman et al., "The Teaching Privacy Curriculum," 2016, 591–96.
[83] Roslyn Layton, "California: Avoid GDPR Insanity of Doing the Same Thing and Expecting a Different Outcome," *Forbes*, June 21, 2018, https://www.forbes.com/sites/roslynlayton/2018/06/21/california-avoid-gdpr-insanity-of-doing-the-same-thing-and-expecting-a-different-outcome/#57d158d35801.
[84] For a summary, see Roslyn Layton, "Privacy Regulation Insanity: Making the Same Rules and Expecting a Different Outcome," AEIdeas, June 21, 2018, http://www.aei.org/publication/privacy-regulation-insanity-making-the-same-rules-and-expecting-a-different-outcome/. This podcast features a discussion of these issues. GDPR and the Future of Internet Privacy. Federalist Society. July 9. 2018.
https://fedsoc.org/events/the-gdpr-and-the-future-of-internet-privacy