Why Stronger Privacy Regulations Do Not Spur Increased Internet Use

BY ALAN MCQUINN AND DANIEL CASTRO | JULY 2018

Data protection regulations are often falsely described as means to increase consumer trust, and therefore technology adoption and use. Policymakers should be wary of those making this claim without evidence.

Over the last two decades, it has become the conventional wisdom in tech policy circles that stronger privacy regulations increase consumer trust, and higher levels of consumer trust will lead to more technology use. Few observers who should know better have challenged this assumption, and now many who influence policy simply assert it without question. However, there is little evidence to suggest that beyond some minimum baseline of consumer protection, stronger privacy regulations increase trust, adoption, or use. On the contrary, additional regulation restricts the supply of digital technologies by raising costs and reducing revenues for companies to invest in new products and services. In short, the conventional wisdom about the connection between regulation and trust is wrong. Policymakers should reject proposals purporting to increase trust through greater regulation of the digital economy if they come at the expense of innovation and consumer welfare.

Most activities—from bicycling to mountain climbing—involve some level of risk. Often, the individuals engaged in these pursuits cannot control all of the risks themselves. This is where trust comes in. For example, bicyclists may trust that their helmets work properly, and mountain climbers may trust that their ropes will not break. In the context of technology, trust is the level of certainty an individual has in the risk, or lack thereof, involved in using a given technology based on their experiences and expectations. The likelihood that individuals will use a particular technology is a function of the value they perceive in using the technology and their level of trust. For example, most consumers generally trust the Internet—they believe it is safe and will not cause them harm—and they get substantial value out of going online, so they choose to use the technology.

Policies to increase trust can take different forms, from educational campaigns to teach the public about the safety of a new technology to regulations designed to prevent unsafe products from entering the market.[1] By improving trust, policies may, under certain conditions, spur more demand for technologies. For example, strict aviation safety regulations combined with a strong overall track record have helped create an environment in which more people feel comfortable with air travel. But regulations to increase trust almost always come at a cost. For example, regulations could make vehicles even safer, but not without making them more expensive—thus leading to potentially less overall driving. The challenge for regulators is to find the optimum level between trust and cost.

Many policymakers have called for policies to increase consumer trust in digital technologies and platforms, justifying increased regulation on the grounds that it will boost digital adoption. For example, in the United States, the Clinton, Bush, and Obama administrations each cited the importance of building trust in boosting adoption and use of the Internet, e-government applications, and the Internet of Things, respectively.[2] The European Union has also invoked increasing trust as a justification for numerous data protection regulations, including its new General Data Protection Regulation (GDPR).[3] And most privacy advocates have justified their calls for stricter privacy laws on the grounds that they boost trust, which in turn boosts usage.

If increasing trust were really the goal of most proponents of stronger privacy regulations, they would be advocating for other policy options that would improve trust and spur digital technology usage. But the focus of most privacy advocates is on creating rules regardless of the cost, and many have realized it is more persuasive to argue that restrictive privacy rules not only have no cost, but actually produce vast benefits because they bolster user trust, which ultimately leads more people to use the technology.

However, as we show, the relationship between regulation and trust and between regulation and usage, is not linear—more regulation does not lead to more use. In fact, beyond a reasonable baseline of regulation—something the United States appears to have—most proposals to increase privacy rules do little to increase trust and use.

Likewise, the relationship between privacy regulation and usage is also not linear: More regulation does not always lead to more innovation. Instead, the relationship appears to be best modeled as an inverted U: where too little regulation limits usage, but too much regulation raises the cost or reduces the relative quality of digital technologies, thereby negatively impacting the number of people who use them. Indeed, past a certain point, stronger data protection regulations usually have the unintended consequence of decreasing the supply of technology. For example, one reason there are relatively few high-quality, ad-supported websites and apps for children is Congress has enacted strict privacy laws that limit the viability of these services.[4] Thus, the net impact of strong privacy regulations for consumers is likely to be negative.

This relationship suggests there is an optimal level of regulation—a Goldilocks level—that is neither too weak nor too strong. Aggressive regulatory policies, such as those deployed in

GDPR, will likely do little to nothing to increase trust, but will limit digital innovation and raise costs, thereby reducing use relative to more balanced rules. It is time, therefore, to end the spurious claims that more privacy regulation is pro-innovation and pro-consumer.

CLAIMS THAT INCREASED TRUST IN THE INTERNET BOOSTS USAGE

Policymakers around the world have argued that additional Internet regulation will increase trust and greater trust will encourage more people to use Internet applications. Rather than evidence, however, virtually all these claims are supported by false assumptions and wishful thinking.

In the United States, this argument has been cited, without evidence, by administrations and federal agencies. The Clinton administration cited trust as an important factor in the use of the Internet in two of its reports: "A Framework for Global Electronic Commerce" and "Defending America's Cyberspace."[5] The George W. Bush administration cited trust as a necessary component to get more citizens to use the administration's e-government applications.[6] The Obama administration cited trust as an essential component in many of its proposals. In support of its Consumer Privacy Bill of Rights in 2012, a White House report stated:

> Trust is essential to maintaining the social and economic benefits that networked technologies bring to the United States and the rest of the world… Privacy protections are critical to maintaining consumer trust in networked technologies.[7]

Other Obama administration officials made similar assertions. For example, Lawrence Strickling, the administrator of the National Telecommunication Information Administration (NTIA), said "Preserving consumer trust is essential to the sustainability and continued growth of the Internet economy."[8]

Officials in the European Union have made similar claims to justify many EU data protection initiatives, such as GDPR and restrictions on cross-border data flows. For example, in 2017, Andrus Ansip, the vice president of the European Commission's Digital Single Market wrote, "It's very simple: without clear rules on privacy in electronic communication services—or ePrivacy—there will be no trust. Without trust, people will not use digital services."[9] Similarly, Paul Timmers, the director of the Digital Society, Trust, and Cybersecurity at the Commission said trust is the "most important currency" of the digital age.[10] In 2016, the European Commission claimed that new rules to promote customer trust through better protection and enforcement would boost e-commerce.[11] And, in 2018, the European Commission endorsed provisions for data flows and data protection in its trade agreements, which say "The protection of personal data and privacy… contribute to trust in the digital economy and to the development of trade."[12]

The international community has also bought into this conventional wisdom, which is reflected in how it approaches rules and resolutions for the global Internet. The Organisation for Economic Co-Operation and Development (OECD) released a report saying, "Trust is fundamental to the functioning of the digital economy; without it,

individuals, firms and governments won't use digital technologies, and an important source of potential growth and social progress will be left unexploited."[13] The World Bank's Digital Dividends report states, with no citations or other support, that, "Protecting personal data online is key for the data driven economy, since it will increase trust in the Internet, and greater trust will foster more use."[14] Similarly, in 2016, the United Nations Human Right Council passed a proposal to promote the protection of human rights on the Internet, in which it described "building confidence and trust in the Internet" as "an enabler for development and innovation."[15]

Not surprisingly, most consumer privacy advocacy organizations, including Trust in Digital Life and the Online Trust Alliance, have worked to propagate this claim and relied on it to justify calls for more stringent privacy and data regulations.[16] For example, in testimony before the European Parliament in 2012, Electronic Privacy Information Center President Marc Rotenberg said, "Trust exists where data protection is established and enforced."[17] The Future of Privacy Forum has argued that a trust framework of privacy and cybersecurity rules is necessary to facilitate the adoption of various technologies, such as education technologies and drone technologies.[18]

This argument offers policymakers the proverbial free lunch: The more regulations they create, the more economic benefits they will reap. What policymaker can resist this siren song?

Many privacy groups understand that policymakers will be less likely to support stronger data protection rules if the rules harm the digital economy. These privacy advocates are offering policymakers the proverbial free lunch: The more regulations they create, the larger the economic benefits they will reap. Few policymakers can resist this siren song for strong regulations. As a result, privacy advocates and policymakers alike turn to this argument. For example, Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, has argued, "privacy breeds innovation."[19] Similarly, the Center for Democracy and Technology has argued that stronger privacy protections are necessary to promote health information technology (IT) adoption, writing:

> Although some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT may bring, we argue that the opposite is true: enhanced privacy and security built into health IT systems will bolster the public trust and confidence that are critical to the rapid adoption of health IT and realization of its benefits.[20]

HOW DO PRIVACY AND TRUST RELATE TO TECHNOLOGY ADOPTION AND USE?

At some level, trust does play a role in digital technology adoption and use. Research suggests that trust is an important component of any relationship that involves social uncertainty or risk, playing a role in the adoption of a technology, establishment of a business relationship, or the use of a service.[21] While the exact impact is hard to determine, numerous studies have shown levels of trust impact consumers' adoption of various technologies, from e-commerce to autonomous vehicles.[22] However, the research is at best ambiguous about the extent of the relationship between privacy and trust, and trust and actual use of a technology. What evidence that does exist is grounded in digital technology adoption and usage rates, academic studies, and public polling.

Many advocates and officials look to low Internet-application adoption and usage rates as an argument for regulation. For example, a 2017 OECD report argued the reason there is lower adoption and use of various digital technologies is consumers do not trust the technology.[23] It rightly notes that e-commerce remains "below its potential," as only 57 percent of Internet users in OECD countries report buying goods online, while 90 percent of Internet users report using email, and 80 percent report using the Internet for obtaining information on goods and services.[24] It also points to relatively low adoption rates of other digital technologies, such as e-government services, cloud computing, and radio frequency identification. However, the report then attributes these lower rates to a lack of trust in online services and growing concerns about risks associated with those services, which are a "serious barrier for the adoption of digital technologies."[25] The report cites consumer surveys that show users have increasing privacy and security concerns to back up this assertion, but it does not provide any evidence of whether these concerns actually affect levels of consumer trust or consumer adoption and use. Clearly there are a wide array of factors determining digital adoption and use, including levels of education and income, access to payment systems, maturity, and ease of use of the technology, as well as the value proposition. The report makes no attempt to control for these and other factors to justify its claim that the lower rates of adoption are a result of lower levels of trust.

Many researchers have analyzed the relationship between trust and technology adoption or use, discovering many factors that affect individuals' levels of trust in a technology and their intention to use it.[26] Indeed, trust is a multidimensional construct. One of these factors that researchers have analyzed is perceived privacy and security, and several studies have confirmed that the perceived privacy and security of a service influences the perceived trustworthiness of that service.[27] This effect is often pronounced in early studies of adoption of online services, which showed that perceived problems of privacy and security of the Internet had a negative effect on trust online.[28] Indeed, it was not uncommon in the early days of e-commerce for individuals to avoid using it because they did not trust their credit card information to be secure. This may be the case, as Cho et al. suggests, because maturity plays a role in establishing trust for any technology.[29] Indeed, privacy concerns about technologies do fade over time as the public interacts more with them and as technology developers make systems more secure.[30]

Some research does suggest that implementing privacy protections can boost adoption of services that gather data, although the findings are mixed. For example, Culnan and Armstrong found that telling consumers about the use of fair information principles boosted the trust of users, increasing the willingness of those with privacy concerns to have their information used by an organization.[31] Similarly, in 2002, Pavlou found that websites can improve trust in e-commerce by encrypting transactions, installing firewalls, using authentication mechanisms, and ensuring privacy seals and disclosures.[32] However, more recent research suggests this is not always the case. In 2016, Ben-Shahar and Chilton analyzed how participants would behave based on the privacy policy of a dating app, where one policy explained the app would collect highly sensitive information, such as sexual

history, and sell that information to third-party advertisers. The authors found that consumers' willingness to share this information was the same, regardless of what the privacy policy said and whether the participants had read it.

Importantly, the body of trust research has several limitations that make it difficult to assess what factors play a role in increasing trust. First, across dozens of studies of consumer trust and technology adoption and use, there are numerous definitions of trust that are often contradictory and confusing.[33] Some define trust as a positive value, in which users ascribe beneficial traits to a firm or technology, such as benevolence, credibility, ability, integrity, and honesty.[34] Others describe it as a neutral action, attitude, or intention by the individual towards the technology. (As mentioned in the introduction, we define trust as the level of certainty an individual has in the risk, or lack thereof, of using a given technology based on their experiences and expectations.) Second, there is no widely accepted measurement of trust. In a 2011 analysis of over 171 papers published over a 48-year period, there were over 129 different measures of trust.[35] Third, many studies focus narrowly on one actor in the relationship, not considering all parties involved, such as the consumer, the party to be trusted, the technology, and the broader environment.[36] Fourth, few studies are empirical, and the ones that are have limited models that ignore important components in the trust relationship.[37]

The third source of evidence that privacy advocates and government officials have often based their claims on is polling that reports decreasing levels of trust and perceived privacy for technologies and institutions in both the public and private sector. For example, in 1998, the U.S. Department of Commerce cited a *Business Week*/Harris poll that found three-quarters of Internet users would use online services more if privacy were guaranteed.[38]

Polling data that shows decreasing levels of trust and rising levels of perceived privacy and security concerns are often cited by advocates of more-restrictive regulation. For example, according to two Eurobarometer surveys, 43 percent of Europeans were worried that online banking would result in the misuse of personal data in 2015—up from 37 percent in 2013.[39] In a 2014 Gallup survey, few U.S. respondents trusted online businesses to keep personal information secure.[40] Indeed, this survey showed that only 2 percent of Americans expressed trust in social networking websites, and only 6 percent trusted online retailers.[41] Despite their apparent reservations, 62 percent of U.S. adults reported using social media websites and 47 percent reported shopping online that same year.[42] Similarly, in 2014, Pew Research found that only 26 percent of respondents were confident email providers were keeping their information safe, while 14 percent were confident in search engine providers, 10 percent in social media providers, and only 6 percent in online advertisers.[43] And following the Facebook privacy scandal involving Cambridge Analytica, a 2018 survey of U.S. adults by market research firm HarrisX found that the majority of Americans do not trust tech companies on data privacy.[44]

However, there are many problems with the surveys and their interpretations. a number of these polls ask biased questions. For example, many attempted to confirm the preconceived notion held by the pollster or poll sponsor that people do not trust technologies because of

their lack of security or privacy protections (See Box 1).[45] Indeed, it is common for such survey questions to "lead the witness," presuppose an answer to a question, or fail to reflect the reality of how services work or companies share data. For example, a 2010 Gallup survey of 1,019 U.S. adults asked respondents whether "invasion of privacy" was worth it to "allow people free access to websites."[46] Based on this framing, which assumed peoples' privacy was being "invaded," it is not surprising only 35 percent answered affirmatively.

BOX 1: EXPLORING HOW PUBLIC SURVEYS CAN GET PRIVACY WRONG

A 2016 Pew Research survey set up six hypothetical scenarios about different technologies—including office surveillance cameras, health data, retail loyalty cards, auto insurance, social media, and smart thermostats—and asked respondents whether the tradeoff they were offered for sharing their personal information was acceptable.[47] For example, see the following question on Pew's survey regarding smart home devices:

> "A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room."[48]

In this question, the consumer benefit (i.e., saving money) is only described as being "potential," while the alleged loss of privacy (i.e., the company knowing which room a person is sleeping in) is definite. Nor does the scenario mention that one reason for data collection is to help all customers cut energy use, and thereby reduce pollution. In this scenario, there is very little incentive for a user to participate.[49] Moreover, the tradeoff set up in the question does not reflect the reality of how smart thermostat companies actually share data. Based on Pew's description, many respondents might believe they are required to share information about when they are home or what they are doing inside their home. However, all the major smart thermostat companies—Nest, Honeywell, and Ecobee—have strict privacy policies for how they use and share consumer data to protect it from misuse, including using it only for de-identified, macro-level analytics.[50]

A more appropriate question would be:

> A company has created an inexpensive thermostat sensor for your home that would measure your temperature zone, in addition to your family's movements around the house, and help you use less energy—thereby saving you money and helping cut pollution and emissions that cause global warming. It is programmable remotely in return for collecting data about some of the basic activities that take place in your house, such as when people are there and when they move from room to room. The device uses this anonymized data to help you compare your energy use to other similar homes.

These academic studies and public surveys usually fail to uncover consumers' actual preferences because they do not ask respondents to confront the cost consequences of their choices. As a result, while people say privacy is an important factor in their decision-

making, in practice, this is largely not the case. This phenomenon, demonstrated in a number of studies, is often called the "Privacy Paradox," wherein consumers confronted by a privacy concern choose to share their data when data protections are seen as too costly or ineffective.[51] This phenomenon has been demonstrated in many studies. Acquisti and Grossklags showed through survey evidence that consumers possess disparate privacy tastes, and even with sufficient evidence to make privacy-sensitive decisions, often choose to make long-term privacy tradeoffs for short-term benefits.[52] For example, Preibusch et al. surveyed German participants buying DVDs from two online stores—one with a privacy-invasive questionnaire and one without—and found that even when the prices were the same, neither store sold more DVDs than the other.[53] But when offered a very modest discount in exchange for completing the questionnaire, the majority of participants chose to buy from the cheaper, privacy-invasive firm.[54] In this study, most individuals found the perceived value of the exchange to be higher than the perceived risk. Similarly, Happ et al. conducted a study that revealed that over a third of respondents would readily give up their personal passwords for work or school accounts for a bar of chocolate, despite the risks of doing so.[55] Moreover, Athey et al. found that consumers, despite having privacy concerns with sharing contact information, were willing to give up their friends' contact information in exchange for merely a small incentive: pizza.[56]

Academic studies and polling surveys usually fail to uncover consumers' actual preferences because they do not ask respondents to confront the cost consequences of their choices.

Thus, whenever respondents are asked via surveys to confront these choices, answers better reflect actual preferences. In a survey from 2014, 55 percent of U.S. participants responded "agree" or "strongly agree" with the statement, "I am willing to share some information about myself with companies in order to use online services for free."[57] Similarly, a Eurobarometer survey found that, while just over half of individuals were concerned about privacy, 71 percent said that sharing information was "increasingly part of modern life" and that they accept the tradeoff between information sharing and free or higher-quality digital services.[58]

Furthermore, privacy preferences vary significantly between individuals and are contingent on cultural norms and standards that may change over time. Alan Westin, the late professor of Public Law and Government Emeritus at Columbia University, performed several foundational surveys that helped form an understanding of the American public's attitude toward privacy.[59] In his research, he found three general groups of people with different stances toward privacy values. The first group represented a small fraction of people called "privacy fundamentalists," who place such a high premium on their privacy that they are almost always unwilling to share their information under any condition. This group represents about 20 to 25 percent of the population.[60] The second group was called the "privacy unconcerned"—which represents about 20 percent of the United States—has little concern for privacy.[61] The final group, called the "privacy pragmatists," was the largest, with roughly 55 to 65 percent of the population.[62] Westin explains, the "[p]ragmatists favor voluntary standards over legislation and government enforcement," and are willing to make trade-offs around sharing their data, especially if expanded use of

the data is beneficial to society.[63] Most consumers are willing to trade their data in exchange for direct or indirect benefits to themselves or society at large.

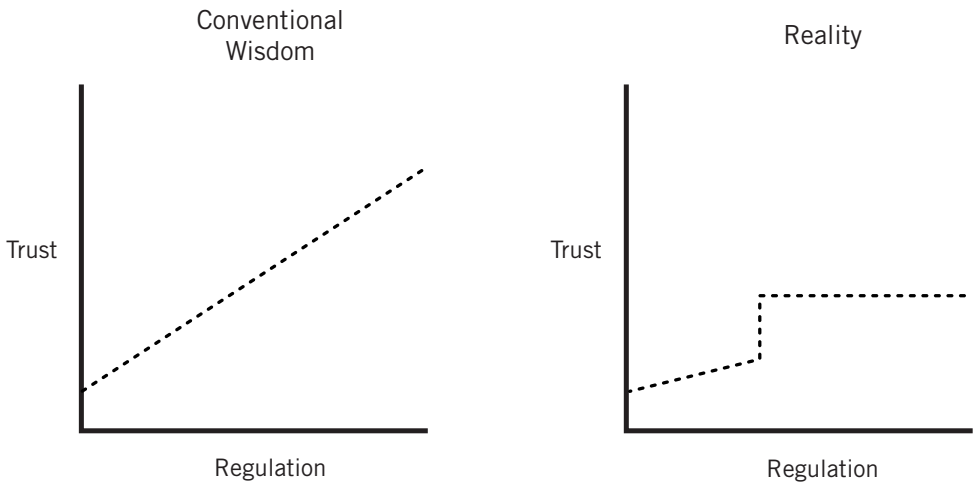
Trust and privacy are complicated topics, and the evidence does not suggest increasing privacy protections will necessarily increase trust. The question remains: What is the relationship between data protection regulations and increasing trust?

HOW REGULATIONS AFFECT CONSUMER TRUST AND ADOPTION

Privacy researcher Helen Nissenbaum wrote that consumers care about trust online because it "brings about valued ends."[64] Indeed, as we have shown, many policymakers, international organizations, and consumer privacy advocates argue that increased regulation over the digital economy leads to more trust, more trust leads to more willingness for consumers to use technology, and, therefore, more regulation will increase digital technology usage. In this framing, the relationships between trust and regulation—as well as regulation and technology adoption and usage—are linear: More regulation leads to more trust, and more trust means more adoption and use. Therefore, stricter privacy regulations will boost adoption and use—regardless of the baseline levels of regulation that already exist. However, as discussed below, there is little evidence to suggest the relationship between these factors is linear.

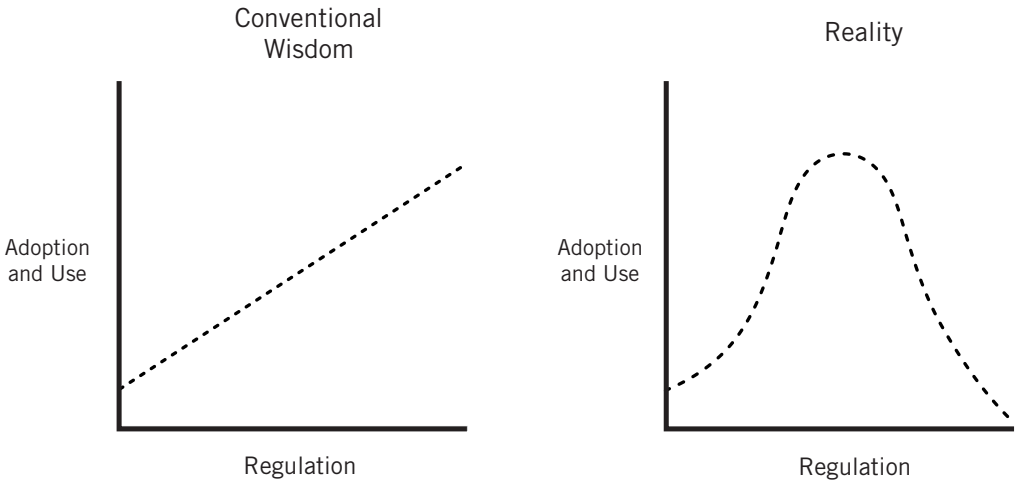
To continue the analogy from above, mandating that bicycle helmets be able to withstand a three-meter fall onto an anvil—the current standard is two meters—would be unlikely to increase trust in cycling because the existing standard already protects against most common accidents.[65] Indeed, there is likely some level of regulation beyond which further protection has little effect on trust. Therefore, the relationship between regulation and trust is a stepwise function: No regulation means very little trust, and some reasonable baseline level of regulation increases trust, but trust does not measurably increase beyond that baseline level (see figure 1). In other words, with no regulations, helmet manufacturers may make helmets that crumble from only the slightest of impacts, which would lead to little to no trust in the product. Yet increasing the standard from a two-meter to a three-meter anvil fall has little effect on trust.

Figure 1: Linear versus stepwise relationship for trust and regulation.



But how does regulation affect actual technology adoption and use? If bicycle helmets have no safety standards and thus offer little to no protection, individuals may not use them or may choose to not ride bicycles altogether. However, simply increasing the regulation to their highest level would have diminishing returns for their adoption and use. This is because cost plays a more significant role than many advocates and policymakers may realize or want to admit. If creating helmets with a three-meter standard is significantly more expensive than for a two-meter standard, many riders may not be able to afford the new helmets and as a result some may not ride bicycles. Therefore, rather than describe the relationship between regulation and digital technology adoption and usage as linear, it is best described as an inverted U-curve (figure 2).

Figure 2: Linear versus inverted-U relationship between regulation and technology adoption and use.



This brings us to digital regulation. The core questions are whether the relationship between digital regulation and trust is linear or stepwise, and whether the same is true for digital regulation and consumers' willingness to use a certain technology. In other words, will strong data protection legislation lead to even more trust among Internet users than a light-touch regulatory regime, and will that trust translate into increased adoption and usage or will it be the equivalent of the three-meter helmet standard, wherein a baseline level of trust is enough.

To analyze these relationships, we compared consumer trust and technology adoption and usage data from consumer surveys across a range of countries with varying levels of regulation. Our goal was to answer three questions: To what extent does regulation have an impact on consumer trust of the Internet? To what extent does regulation have an impact on consumers' willingness to adopt the Internet? And to what extent does regulation have an impact on actual usage rates of Internet applications?

As previously mentioned, academic studies have found a relationship between trust and the willingness to adopt a technology: Greater levels of trust in a product or service mean people are more likely to use it. However, we were not able to find a study that analyzes this effect in depth; whether this relationship is linear, stepwise, an inverted-U, or

something else entirely; or how these effects differ across cultures. It is likely that trust does have some positive net effect on consumers' willingness to adopt and use a technology, but we do not know the true extent of that effect.

Does Digital Regulation Increase Trust?

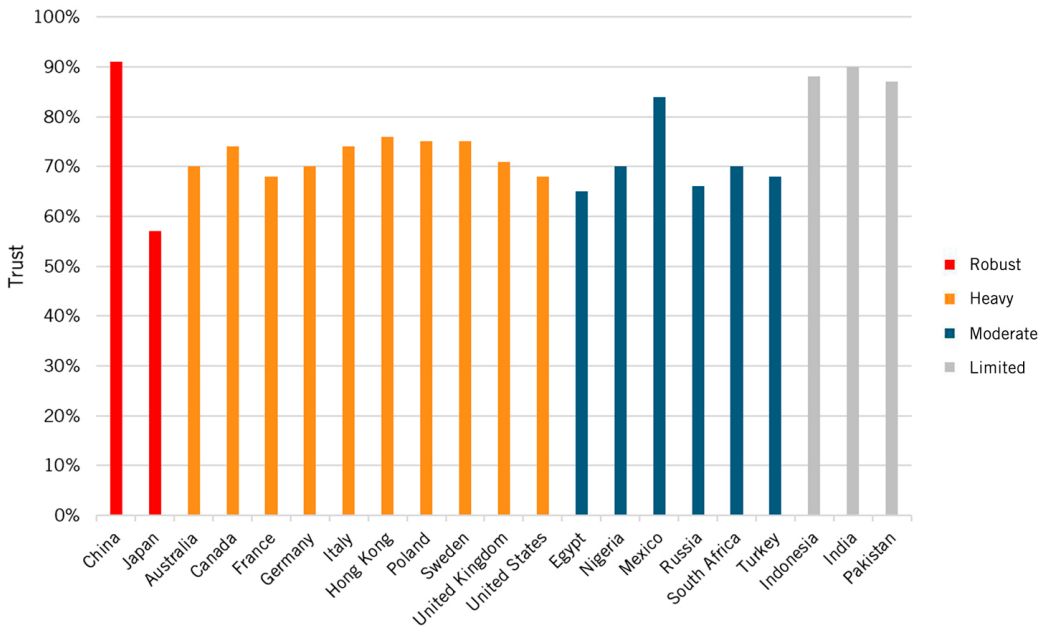
We first analyzed whether stronger digital regulations lead to increased consumer trust by comparing levels of trust across several different countries whose strengths of both data protection and enforcement varied. If the relationship is linear, then countries with the strictest protection regimes would also have the highest levels of trust among their citizens.

It is striking that for all the efforts the European Commission and individual EU nations put into digital regulation that trust levels are largely the same as in the United States, a country with fewer strict digital regulations.

We compared levels of trust from consumer surveys across 21 countries with different levels of data protection regulations.[66] For levels of trust, we used survey data from the Centre for International Governance Innovation (CIGI), a nonpartisan think tank, and Ipsos, an independent market research company, which conducted four surveys on behalf of the United Nations Conference on Trade and Development in 2014, 2016, 2017, and 2018 on roughly 24,000 Internet users each year from 24 different countries.[67] The survey questions they asked varied year to year, but focused heavily on privacy concerns and trust. In both the 2017 and 2018 surveys, CIGI asked respondents to what extent they trusted the Internet.[68]

For levels of data protection regulation, we used ratings made by DLA Piper, a global law firm with expertise in privacy regulations.[69] The firm ranks the strength of data protection regulations in each country as robust, heavy, moderate, or limited (Appendix 1): DLA Piper finds that countries like China and Japan have robust data protection regulations and enforcement; Australia, much of Europe, the United States, and a few others have heavy data protection regulations and enforcement; countries like Mexico, Nigeria, and South Africa have moderate data protection regulations; and India, Indonesia, and Pakistan have only limited data protection regulations.

Figure 3: Levels of trust in the Internet by country and level of regulation.



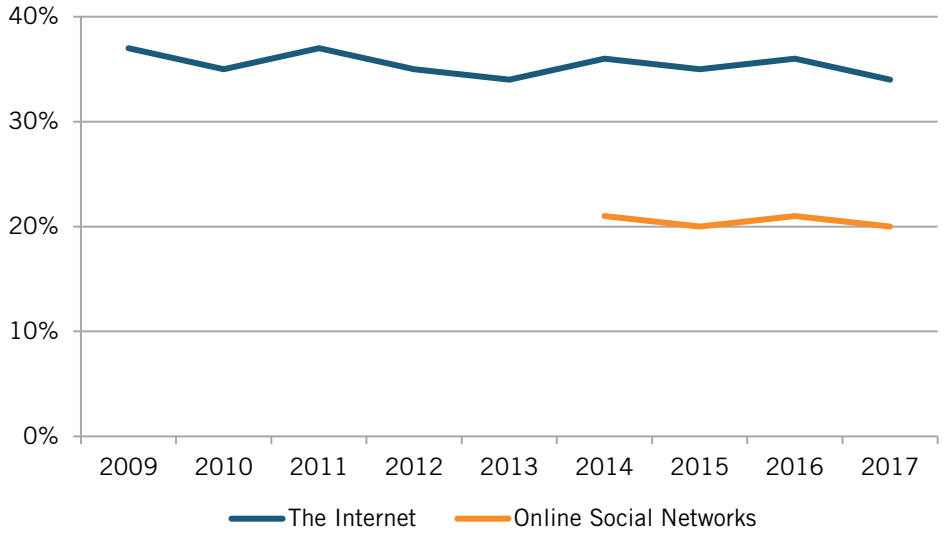
If the trust-regulation relationship were linear, countries with stronger privacy protections would have lower levels of privacy concerns and higher levels of trust. However, strong privacy regulations do not have a positive relationship with trust in Internet businesses and digital services. In the 2018 survey, the level of trust in the Internet was relatively flat across most countries with moderate to heavy regulations (figure 3).[70] In fact, among many of the countries with heavy levels of regulation, the group of individuals who either said they strongly agreed or somewhat agreed that they had trust in the Internet was similar. For example, heavy regulatory countries like United Kingdom (71 percent of respondents), France (68 percent), and the United States (68 percent) had similar levels of trust to moderately regulated countries like Nigeria and South Africa (70 percent of respondents each). Of course, even within each of these categories, countries and regions differ in their approaches to data protection, such as the European Union and the United States. However, it is still striking that for all the efforts the European Commission and individual EU nations have put into data protection regulation, trust levels are largely the same as in the United States.

Interestingly, the countries with limited levels of digital regulation showed higher levels of trust than their more regulated counterparts. For example, 90 percent of respondents in India and 87 percent of respondents in Pakistan trusted or somewhat trusted the Internet. In addition, countries with the most robust data protections showed mixed results, with China showing the highest levels of trust (91 percent of respondents) and Japan showing the lowest (57 percent). Given this odd result, we decided to investigate the relationship further by performing a correlation analysis between trust, regulation, and GDP per capita (Appendix B). We found a strong positive relationship between poor countries and high levels of trust, while more wealthy countries tended to have more regulations and lower levels of trust. For example, China and Japan—countries with robust levels of data protection—have significantly different levels of trust based on their GDP per capita, with the poorer China having the highest levels of trust in the Internet and the richer Japan having the lowest. Therefore, it is likely that Internet trust concerns are primarily a "rich man's disease" that affects wealthier nations.

Unfortunately, because CIGI only asked about trust in two surveys, we were unable to track trust over time across different countries—particularly in instances before and after a country increased the strength of its digital regulations. However, we can look at trust over time in the European Union, which has some of the strongest data protection regulations—especially after the implementation of GDPR. The biannual Eurobarometer survey, which interviews 100 individuals from each EU country on a variety of topics, has been tracking European trust in the Internet since 2009 (see figure 4).[71] Interestingly, European trust in the Internet remained flat from 2009 through 2017, despite the European Union strengthening its ePrivacy regulations in 2009 (implementation of which occurred over the subsequent few years) and significantly changing its privacy rules, such as the court decision that established the right to be forgotten in 2014.[72] Similarly, European trust in social networks, which the Eurobarometer started measuring in 2014, has also

remained flat, albeit low. It will be interesting to review these results from 2018 and 2019 to see whether the implementation of GDPR affects trust levels.

Figure 4: Eurobarometer results for percentage of individuals that place trust in the Internet, 2009 to 2017.



The evidence suggests strong data protection regulations have little to no positive effect on trust when compared with other countries with moderate or limited levels of digital regulation. This is perhaps because people interpret heavy regulations as signs the government is telling its citizens the technology cannot be trusted. This is clearly the message that European Commission and EU national privacy regulators have been sending to EU citizens: Cyberspace is so fraught with risks and dangers that only incredibly restrictive regulation can provide protection from serious harm. It is no wonder European consumers do not appear to have more trust in the Internet than citizens in other nations with less-strict privacy regulations.

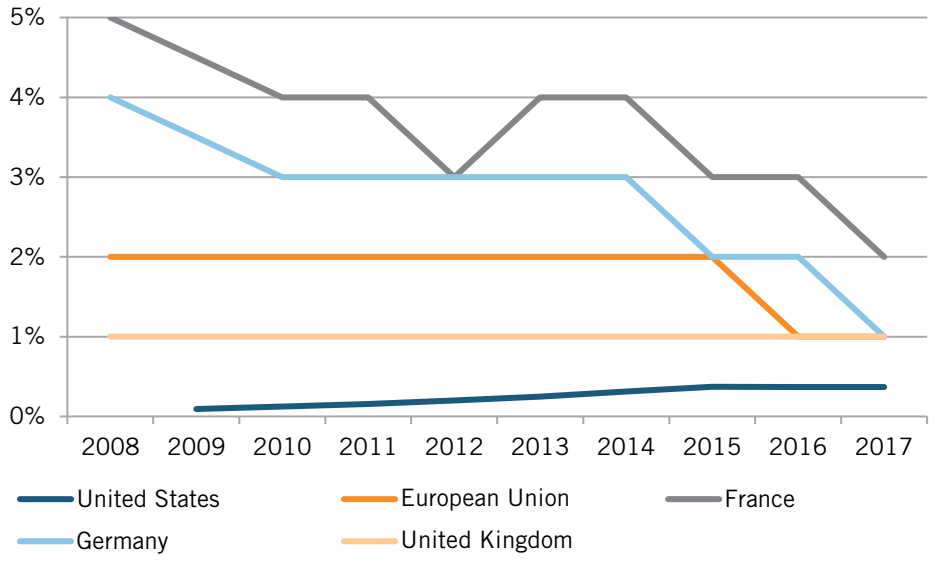
While we estimate the relationship between digital regulation and trust is stepwise (see bicycle helmet discussion above), there is not enough data or evidence at this time to conclusively make that determination.

Does Digital Regulation Increase Willingness to Adopt Internet Applications?

Much of the evidence that advocates and policymakers cite when arguing for stricter digital regulations is based on surveys that focus on privacy and security concerns across a variety of different Internet applications, such as e-commerce, social media, and online banking. But the question remains: Does digital regulation actually improve individuals' willingness to adopt (rather than simply use) Internet applications? Indeed, there are very few surveys that ask non-users why they are not adopting technology. This lack of evidence makes it difficult to determine whether trust or privacy concerns actually translate into a lower willingness to adopt.

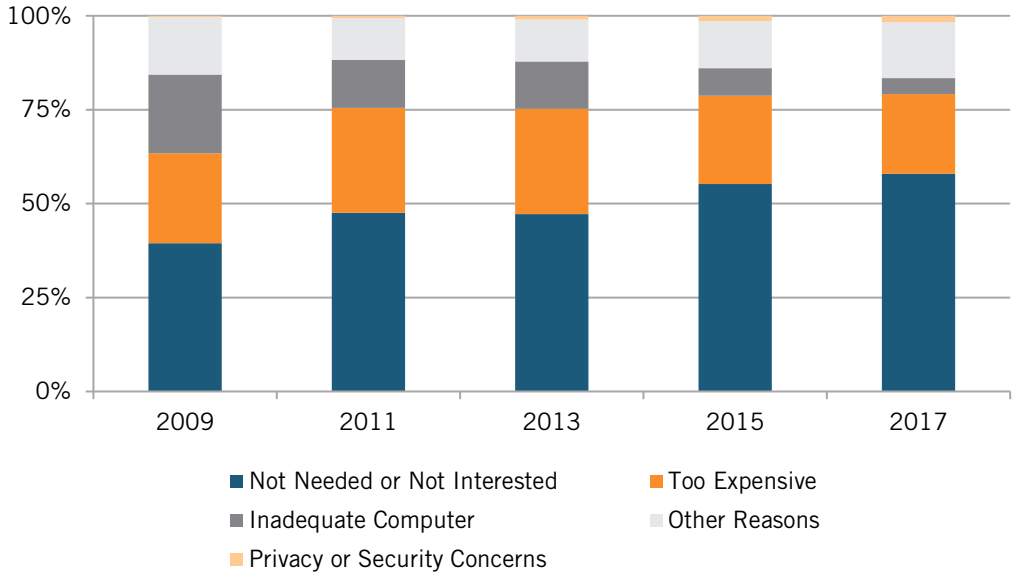
Several surveys have asked about whether a lack of trust is a barrier for consumers to get Internet access. From 2008 to 2017, Eurostat asked European households that did not have Internet access why this was the case.[73] The survey found that the share of overall European households that cited privacy or security concerns as the reason they did not have Internet access declined, decreasing from just 2 percent in 2008 to 1 percent in 2017 (see figure 5).[74] Individual countries also saw decreases in the total percentage of households that cited privacy and security concerns as their reason for not having Internet access. For example, both France and Germany saw a 3-percentage point decrease from 2008 to 2017.[75] These concerns trend downward over time, even as the population of people without Internet access decreases. It is unlikely that making regulations stricter, such as through the passage of the GDPR, would cause this small group of individuals—likely privacy fundamentalists—to change their minds and get Internet access.

Figure 5: Percentage of total EU and US households that cite privacy and security concerns as the reason they do not have Internet, 2008 to 2017.[76]



In the United States, the percentage of households that do not go online because of privacy or security concerns is even lower. National Telecommunications and Information Administration (NTIA) surveys found that the proportion of households that say privacy and security concerns are their main barrier to adopting the Internet at home has been less than 0.5 percent for the past decade—it was 0.1 percent in 2009 and 0.4 percent in 2017. During this period, Internet adoption at home grew from roughly 60 percent to 72 percent of households.[77] Indeed, U.S consumers consistently cite privacy and security concerns as one of the least important reasons they have not adopted Internet access at home (figure 6).

Figure 6: Reasons cited by US households for choosing not to have Internet access at home 2009 to 2017.[78]



Overall, survey evidence does not suggest increased regulation leads to a greater willingness to adopt, as countries with higher regulatory strength, such as Germany and France, also have higher percentages of people who claim to avoid using such technologies due to privacy or security concerns. If data protection regulations had a linear relationship with Internet adoption, European respondents would likely have lower levels of privacy or security concerns than their U.S. counterparts due to having stricter privacy laws. However, most European and U.S. respondents without Internet access who do not subscribe for other reasons, such as a lack of perceived need, insufficient skills, or cost concerns.[79]

BOX 2: PRIVACY AND TRUST CONCERNS ARE PUSHING CONSUMERS TO CHANGE THEIR BEHAVIOR

While few people consider security and privacy concerns a large-enough barrier to prevent them from adopting technologies altogether, surveys do find consumers that are already using an Internet application are changing their behavior to mitigate perceived trust and privacy concerns. The 2018 CIGI survey found that many respondents had made behavior changes in the previous year.[80] But most of these behavioral changes appear to be related to concerns about security, rather than privacy.

Global respondents to the survey described several of these changes:

- 43 percent avoided opening emails
- 36 percent avoided certain Internet websites
- 30 percent avoided certain web applications
- 28 percent reduced the amount of personal information they share online
- 12 percent made fewer online purchases
- 10 percent closed their social media accounts
- 7 percent used the Internet less often

Does Digital Regulation Increase People's Use of Internet Applications?

To better ascertain the relationship between regulation and Internet usage, we analyzed the usage rates of the United States and Europe around the introduction of a new privacy law to see whether the implementation of strong data protection rules spurred more people to use the technology. We primarily looked at usage rates for three different technology applications: Using the Internet (generally), using social media, and shopping online. We used data from the Pew Research Center and NTIA for U.S. usage rates, and data from Eurostat and the International Telecommunications Union (ITU) for European rates.[81] Because data was not available for earlier implementations of European data-privacy initiatives (specifically data protection regulations established in 1995 and 2002), we opted to focus on a modification to the Directive on Privacy and Electronic Communications, also known as the ePrivacy Directive, which was updated in 2009.[82] This regulation, often called the "Cookie Law," required all 28 EU member states to pass laws requiring users to give informed consent before Internet content providers could use browser cookies that collect, store, or process consumer data.

We compared the Internet usage rates between 2009 and 2012 of Europe to those of the United States, which did not adopt any new privacy rules for Internet services during that time. The data does not suggest that creating stronger EU privacy laws impacted Internet usage rates in relation to the baseline level of protections in the United States. The percentage of U.S. adults using the Internet increased from 76 percent in 2009 to 83 percent in 2012, a 7-percentage point change.[83] The rate of EU individuals using the Internet between the ages of 16 and 74 increased just 8-percentage points during the same period, from 67 percent to 75 percent.[84] Moreover, countries throughout Europe have implemented the law in varying ways and at different times. For example, Estonia and Italy implemented the law with two separate consent regimes.[85] Because the implementations of this law varied significantly between each European country, we selected two large European countries with varying implementations for closer analysis: France and the United Kingdom. France fully enacted the Cookie Law in November 2011, while the United Kingdom partially enacted the law in May 2011.[86]

Given that each country implemented the law in a different way, there is no evidence the law affected usage rates. When we compared the United States to France and the United Kingdom using data from the ITU, we found that the United States had a greater increase in the percentage of individuals using the Internet from 2011 to 2012. Indeed, the United States saw a 4-percentage point increase while France and the United Kingdom saw a 4-percentage point and a 2-percentage point increase, respectively.[87] Data from Eurostat and the Pew Research Center showed the same trend: The United States had a higher percentage increase of Internet users across similar groups from 2011 to 2012 compared with the European Union as a whole, and to France and the United Kingdom individually (Table 1).[88]

Table 1: Percentage of adult population that uses the Internet in the US, EU, France and UK from 2009 to 2017 (Pew Research and Eurostat).[89]

Year	United States	European Union	France	United Kingdom
2009	76	67	73	84
2010	76	71	77	85
2011	79	73	80	87
2012	83	75	83	89
2013	84	77	84	91
2014	84	80	86	92
2015	86	81	87	93
2016	88	84	88	95
2017	--	85	88	95

If American privacy regulations are supposed to be lacking in strength compared to the robust EU regime, and trust is key to improving usage, why are more Americans using social media than Europeans?

We also analyzed social media usage in Europe compared with the United States after the adoption of the Cookie Law. Data was only available from Eurostat from 2011 through 2017, so we could only observe this relationship after the law took effect.[90] There is again no evidence the law affected usage rates. The passage of the Cookie Law does not appear to have affected usage rates in the European Union and its member states when compared to the United States. After the law took effect in Europe, usage rates still lagged behind those of the United States for both France and the European Union as a whole. Indeed, between 2011 and 2016, France saw a 4-percentage point increase in usage and the European Union saw a 14-percentage point increase in usage, while the United States earned a 19-percentage point increase (Table 2).[91] Only the United Kingdom passed the United States' social media usage rates in 2017.[92] If U.S. privacy regulations are supposed to be lacking in strength compared to the robust EU data protections, and trust is key to improving usage, why are more Americans using social media than Europeans?

Table 2: Percentage of adult population that use the Internet for social media in the US, EU, France and UK from 2011 to 2017 (Pew Research and Eurostat).[93]

Year	United States	European Union	France	United Kingdom
2011	50	38	36	50
2012	53	--	--	--
2013	60	43	38	58
2014	62	46	39	60
2015	65	50	38	60
2016	69	52	40	69
2017	--	54	43	71

Finally, we analyzed the percentage of U.S. and EU respondents that made online purchases following the adoption of the Cookie Law. For this analysis, we gathered U.S. usage data from NTIA for 2011, 2013, and 2015; and EU data from Eurostat for 2009 to 2017.[94] There is no evidence that implementation of the law positively affected usage rates for e-commerce. The passage of the cookie law does not appear to have affected adoption rates in the European Union and its member states when compared to the United States. Indeed, we again see rates for the European Union and France lag behind those of the United States, which lag behind those of the United Kingdom. Between 2011 and 2017, France saw a 14-percentage point increase in e-commerce usage and the European Union saw a 15-percentage point increase in usage, while the United States enjoyed a 17-percentage point increase (See Table 3).[95] During this time, the United Kingdom saw only an 11-percentage point increase in e-commerce usage—although this rate was much higher at 82 percent of adults.

Table 3: Percentage of adult population that used the Internet to make a purchase in the US, EU, France and UK from 2009 to 2017 (NTIA and Eurostat).[96]

Year	United States	European Union	France	United Kingdom
2009	--	36	44	66
2010	--	40	54	67
2011	52	42	53	71
2012	--	44	57	73
2013	53	47	59	77
2014	--	50	62	79
2015	67	53	65	81
2016	--	55	66	83
2017	69	57	67	82

However, there are several caveats for these results. First, the Eurostat data does not account for individuals 74 or older (while the U.S. surveys do), even though they use technologies at a lower rate.[97] This may have artificially raised the EU usage rates. Moreover, usage rates tend to slow in growth as they get higher, and the United States started at higher percentages for most of these technologies. For example, as shown in Table 1, the United States had 76 percent of U.S. adults using the Internet in 2009 compared with 67 percent in the European Union.

In short, the data shows no evidence of a linear relationship between regulation and usage. It is more likely that overly strict regulations negatively affect usage by unnecessarily restricting how companies spend their resources in innovation, and thus reduce the supply of technology available for individuals to use.

THE EFFECTS OF DATA PROTECTION REGULATIONS ON INNOVATION

Even if strengthening data privacy rules beyond some baseline level does not increase trust, what would be wrong with enacting additional rules, given many privacy advocates assert privacy is a fundamental human right? In other words, returning to the prior analogy of bicycle helmet safety, if a three-meter fall standard would provide even a modicum of greater safety than the current two-meter standard, why not simply mandate the higher standard? The answer is the same for all regulatory decisions: to balance cost with benefits. A three-meter standard would increase the costs of helmets, thereby reducing consumer welfare by depriving them of money that could be spent on other things, and perhaps even hurt safety, as some consumers would forgo the purchase of these more expensive helmets and ride without one altogether. Moreover, some people who might otherwise have ridden a bicycle with a modestly priced helmet would choose not to ride at all if they had to pay more for a helmet.

Stringent data protection regulations are the digital equivalent of the three-meter helmet standard. Adding more rules raises compliance costs and reduces revenues for companies that provide online services. And higher costs with lower revenues reduces the investments companies can make to improve their online services. In addition, companies may try to compensate by raising costs for consumers, such as by switching from providing free services to charging for them. In short, additional regulation hurts consumer welfare, makes it more difficult for online companies—including start-ups—to monetize user engagement, and stunts the growth of digital adoption and usage.

Strict data regulations are not free. Companies have to devote resources to compliance which reduces the amount of money that can be invested in innovation.

Many studies have looked at the effects of data protection regulations on innovation. In this report, we highlight five factors affecting data protection regulations that can adversely impact innovation: high compliance costs, threat of high legal fees, reduced viability of free business models, increased uncertainty, and reduced access to data for innovation. Importantly, these factors do not just affect companies, but leave consumers worse off.

Raising Compliance Costs

Strict data protection regulations are not free. Companies must devote resources to compliance, which reduces the amount of money that can be invested in innovation. For example, a 2016 study found that GDPR requirements for public authorities and companies to process personal data could lead to an additional 75,000 jobs for privacy professionals—none of whom work for free.[98] These hires redirect funds from innovating on products to complying with regulations. Similarly, a 2013 report on Europe's proposed regulations for the "right to be forgotten"—the ability for individuals to request that search engines remove links from queries associated with their names if those results are irrelevant, inappropriate, or outdated—estimated these rules, which were eventually implemented, could cause a decrease of European GDP by between 1.5 and 3.9 percent, and a welfare loss of $4,566 (€ 3,812) per household.[99] Furthermore ,a 2014 report from ITIF found the European Union's ePrivacy Directive to regulate browser cookies cost European businesses an estimated $2.3 billion dollars annually.[100] Many privacy advocates simply wish away these costs by assuming they will all be borne out of reduced profits—as if that alone made

these higher costs acceptable. But some of these costs will also be passed on to customers and, to a lesser extent, suppliers, depending on the elasticity of each market. As previously discussed, there is little evidence consumers value additional privacy enough to pay for it.

Moreover, to pursue data protection, some countries have contemplated or created forced data localization rules on companies. While these laws are often designed to either force foreign companies to invest locally, or to protect domestic firms from competition, they come with significant costs.[101] A report from Leviathan Security estimates that such restrictions would force local companies to pay 30 to 60 percent more for their computing needs than if they could go outside the country's borders.[102] For example, the study estimates that if Brazil were to enact data localization as part of its "Internet Bill of Rights," local companies would have to pay an average of 54 percent more than the lowest worldwide price to use cloud services.[103]

Increasing Legal Risks

Increased legal risk and the threat of large fines for companies can leave consumers worse off. If regulatory agencies levy massive fines for actions that are unintentional or caused little to no harm, companies devote fewer resources to releasing safe, useful products and services for consumers, and more on legal fees and internal audits that ultimately slow down the pace of innovation. As a result, lawyers will trump computer scientists and engineers. For example, a 2017 Center for Data Innovation report argues that by both indirectly limiting how personal data gets used by firms and raising the legal risks of companies developing and using artificial intelligence (AI), the GDPR will have a negative impact on the development and use of AI in Europe.[104] Not only will these rules create a competitive disadvantage for European AI firms, it will undoubtedly restrict the available supply of products and services that use AI for European citizens.

Reducing the Effectiveness of Online Advertising

Targeted advertising is beneficial to consumers and businesses alike, allowing firms to be more efficient with their resources and time while increasing the probability of making a sale—all while reducing the number of advertisements necessary to achieve that sale.[105] Consumers benefit by gaining more utility from relevant ads, such as by learning about products that are similar to past purchases offered at prices they can afford.[106] And overall economic welfare increases as companies become more efficient. As such, any data privacy rules that unduly limit targeted advertising would reduce both producer and consumer welfare.[107]

Data protection regulations can reduce the effectiveness of targeted advertisements, resulting in less revenue for websites, especially those offering free services. It is all too easy to forget that the vast array of online services available on the Internet—all sorts of apps, social networks, search engines, encyclopedias, rating systems, and much more—are free. In 2010, McKinsey Institute and IAB Europe estimated that the consumer surplus from ad-supported Internet sites (after discounting the "costs" of privacy and ads) was $44 billion per year in the United States and $95 billion per year in Europe.[108] (Consumer surplus is the difference between what consumers are willing to pay for a product or service

and what they actually pay). In 2011, Brynjolfsson and Oh estimated the surplus to be even larger: $564 billion.[109] Restrictive privacy laws like the GDPR will reduce the value of this surplus significantly.

Moreover, strict privacy regulations reduce the revenue digital companies can earn from online ads, thereby reducing the overall growth of the digital ecosystem. If digital ad revenue grew at the same rate in Europe as in the United States, then an additional 11.7 billion euros would have flowed into the EU digital ecosystem between 2012 and 2017.[110] For example, regulations that shift online services from an "opt-out" privacy system, in which consumers can choose to not have their data used by a company, to an "opt in" privacy system, in which companies can only use data after obtaining affirmative consent from users, will adversely affect advertising-based business models.[111] Perhaps the definitive study on this is from academics Ari Goldfarb and Catherine Tucker, who in 2010 found that the European Union's ePrivacy Directive limited how advertisers could collect and use information about consumers for targeted advertising, which negatively impacted the efficacy of online advertising.[112] The authors found that after the affirmative consent policy went into effect, the result was an average reduction in the effectiveness of the online ads by approximately 65 percent. This reduction occurred because websites had insufficient information about their users to make the ads relevant. Thus, click-through rates fell, reducing the amount advertisers would be willing to pay. The authors noted that if advertisers decreased their spending on online advertising based on this reduction in effectiveness, "revenue for online display advertising could fall by more than half from $8 billion to $2.8 billion." Therefore, this regulation reduced the available funding for online companies, limiting the capacity of existing companies to invest in innovation, and reducing the incentive for new companies to enter the market. Consumers lose in both cases.

Switching the Internet to a subscription-based model would result in reduced revenues and could decrease the quality, breadth, and variety of online content.

Reducing the effectiveness of advertising may result in some companies, particularly those with thin margins, switching to a fee-for-service or subscription business model, wherein customers would have to pay for services that used to be free.[113] While this change would mean slightly lower living standards for everyone who switches, many low- and middle-income individuals would simply lose access to beneficial services they could no longer afford. Moreover, because a subscription-based model would result in reduced revenues, it would also likely decrease the quality, breadth, and variety of content. The simple fact that many online services, such as search engines and social media websites, choose an ad-financed model suggests this form of revenue is more effective than subscription models at enabling them to earn enough revenue to continue innovating. Without this revenue source, many companies would have fewer resources to pay for high-quality content and services.

Increasing Market Uncertainty

Milberg et al. show that one of the largest drivers of data protection is policymakers' desire to address their citizens' "uncertainty avoidance" by reducing their fears (or perceived risks) of privacy violations.[114] Indeed, as we show above, the major argument policymakers make

for rules like GDPR is to increase consumer trust. However, Fuller argues data protection legislation, while potentially reducing this uncertainty for Internet users, significantly increases uncertainty for businesses.[115] Data protection laws can be vague and typically cede interpretation to privacy-enforcement authorities and judges, creating an environment in which entrepreneurs often do not know exactly how laws apply to their activities.[116] This ambiguity creates disincentives for innovation around new technologies and discourages market entry.

Because of differing levels of uncertainty, businesses in the United States have an easier time finding funding than their European counterparts. For example, Europe's ePrivacy Directive, which went into effect in 2002, led to a reduction in venture capital investment in European online advertising companies of around $249 million over the subsequent nine years.[117] Moreover, Lambrecht found that the European ePrivacy Directive led to a 58 to 75 percent decrease in venture capital investment in online news, online advertising, and cloud computing.[118] This lack of investment is one important reason why Europe has relatively fewer Internet start-ups than the United States.

Reducing Access to Data

Finally, stringent data protection laws can result in less access to data or constrain how it can be used—both of which limits innovation. One way that regulations do this is through "purpose specification" rules, which prohibit the reuse of data for purposes not compatible for with those for which it was first collected. For example, purpose specification in the GDPR will prevent companies from experimenting with new uses for existing data.[119] Similarly, the U.S. Federal Trade Commission released a report promoting purpose specification as it relates to the Internet of Things.[120] Moreover, some data regulations call for data retention limitations, wherein a company deletes valuable data to avoid hypothetical future harms that could arise from storing or using data for an extended period of time. While data retention policies are well-intentioned, many companies need access to historical data for new and interesting purposes that ultimately benefit the consumer. For example, Pinterest often uses historical data to both understand large-scale trends in their service and develop new product ideas.[121]

Similarly, restricting how companies can use information may prevent them from adopting new and beneficial technologies altogether. For example, Miller and Tucker reviewed state laws designed to promote increased privacy protection of hospital medical information in 2009, finding that the creation of these laws led to a reduction in the adoption of electronic health records (EHRs) because those laws prevented hospitals from easily exchanging patient information.[122] Indeed, EHRs can help reduce the costs of healthcare substantially.[123]

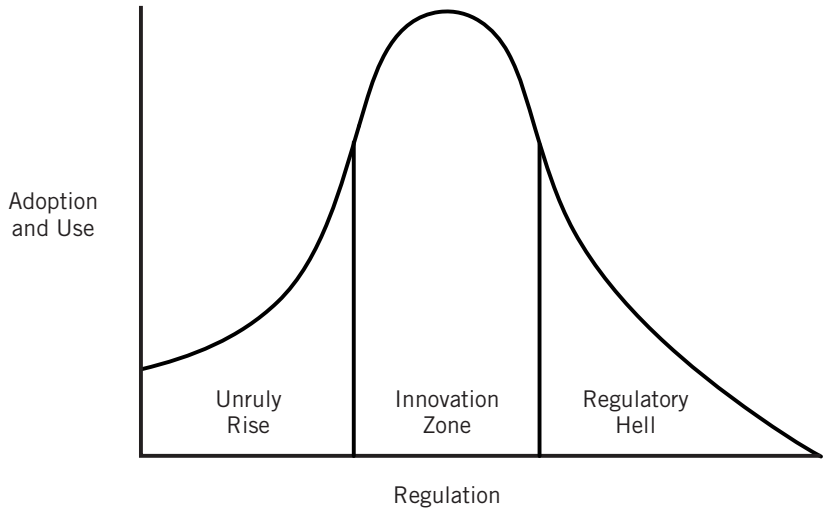
Policymakers Should Strive for a "Goldilocks Level" of Data Regulation

Given these negative effects, if one of the goals of data protection rules is to increase consumer adoption of online services, creating rules that are restrictive and difficult to comply with is not the best solution. While baseline protections may have a modest effect

in increasing the trust people place in digital technologies, strong data protections depress the private sector's ability to release new products and services, and reduces the breadth of free, ad-supported services. This reduction in supply of innovative products and services would deprive consumers of the rapidly developing services and technologies that characterize the Internet age.

Our analysis shows that the relationship between regulation and the adoption and use of online services is best described as an inverted U-curve (figure 7). In this diagram, regulation can be either government regulation or self-regulation by industry.[124] In the first stage, which we call the "Unruly Rise," light regulation can increase user adoption and use of Internet applications, although consumers may have low levels of trust because regulations do not add a sufficient baseline of protections. In the second state, the "Innovation Zone," a reasonable baseline of protections promotes both trust and innovation, thereby ensuring high levels of user adoption and use of Internet applications. However, if policymakers create overly restrictive rules, the use of online services will likely fall or grow more slowly than it would otherwise due to a reduction in supply caused by costly and revenue-limiting regulations. This represents the dangers of the third stage, which we call "Regulatory Hell," wherein overly-strict rules actually harm consumers by creating excessive burdens on digital innovation.

Figure 7: Inverted U-curve showing relationship between regulation and technology adoption and use.



This relationship suggests that there is an optimal level of regulation for the digital economy—a Goldilocks level—with rules that are neither too weak nor too strong. Too little regulation (government regulation or industry self-regulation) is problematic, as it does not provide baseline protections that encourage consumer trust. If nations do not protect against harmful misuse of personal data or hold companies to their privacy promises, some of the "privacy pragmatists" may choose to avoid using digital services, which would no longer have the customer base or data they need to continue to innovate. But overly restrictive regulations are not only unlikely to increase consumer trust, they actually reduce the ability of companies to innovate or provide free or low-cost services,

resulting in a reduced supply of technologies and constraining a nation's overall Internet ecosystem. Overly aggressive regulatory policies, such as the EU's GDPR, not only do little or nothing to increase trust, but reduce access to new and innovative services—leaving consumers worse off.

Policymakers need a mechanism to test for this Goldilocks level of optimal regulation. For example, returning to the bicycle analogy: If existing two-meter-fall helmets failed to protect many bicyclists, but three-meter-fall helmets did not, and they could be produced at a reasonable cost, then policymakers should change the standard to three meters to help avoid unnecessary injuries. However, if relatively few individuals are harmed by three-meter falls, the price of the new helmets pushes people to stop buying them altogether, or the change somehow outweighs the countervailing benefits of the cheaper helmets, then the more-restrictive standard is not useful.

Overly restrictive regulatory policies, such as Europe's GDPR, not only do little or nothing to increase trust, but reduce access to new and innovative services—leaving consumers worse off.

To accomplish an optimal regulatory balance for the digital economy, policymakers should use a three-part test to determine whether a particular regulation is the "right" one. First, each data protection regulation should be designed to address a substantial and quantifiable harm or injury that arises from the misuse of a technology. Harm here refers to the extent to which consumers are materially and negatively impacted by this misuse, which they could not have reasonably avoided themselves. Harms can come in several forms.[125] Autonomy violations result in harm for consumers when information they consider sensitive and would prefer to keep private becomes public through involuntary means. Discrimination occurs when personal information is used to deny a person access to something, such as employment, housing, loans, and other goods. Finally, economic harm occurs when a consumer suffers a financial loss or damage because of the misuse of their personal information. For example, if a company collects personally identifiable information about an individual's age and race, having this information does not in and of itself create a material harm. Using that data so the person is denied credit, however, may be a material harm and may violate laws designed to criminalize this form of discrimination. A harm-based standard is important because cultural norms and standards over what individuals consider privacy-invasive and what they are willing to share changes over time, and this type of regulatory principle will adjust with changing expectations.[126]

Second, data protection regulations should directly limit that harm. By narrowly tailoring regulations to address specific harms, regulators can send clear signals to companies about what behaviors are off-limits, while still allowing for experimentation and innovation. For example, in 2015, the Federal Trade Commission (FTC) penalized a company for a small technical violation of a consumer-protection statute that caused little or no harm to consumers.[127] By targeting that company without evidence that consumers were affected, the FTC pushed it to spend more resources on lawyers rather than on improving the product itself. Only by narrowly targeting regulations and enforcement actions to consumer harms can regulators create an optimum system of incentives that promotes desirable behavior and discourages undesirable behavior in the marketplace.[128]

Finally, the overall costs of the regulation on society should be less than the costs of the harm on society. For example, the FTC takes into account whether each of its regulations is "outweighed by any countervailing benefits to consumers or competition that the practice produces."[129] This is important because as countries move into a more data-enabled economy, robust, but privacy-protective uses of data will have significant social benefits, far beyond the benefits to individuals who share their data. From a cleaner environment and a safer transportation system to dramatically improved healthcare, the ability to use data will be critical to enabling societal progress.[130] By ensuring regulatory burdens are reasonable, policymakers can avoid many of the negative effects of regulations outlined in the previous section.

CONCLUSION

The conventional wisdom that government needs to facilitate trust to increase digital adoption has dominated technology policy debates for too long. Although unsupported by evidence, many repeat the claim ad nauseam, to the point where many policymakers accept it as fact without question. In reality, additional regulation does not seem to increase consumers' trust in online services, their willingness to adopt these services, or actual Internet usage. The conventional wisdom that regulations will increase adoption and use is incorrect.

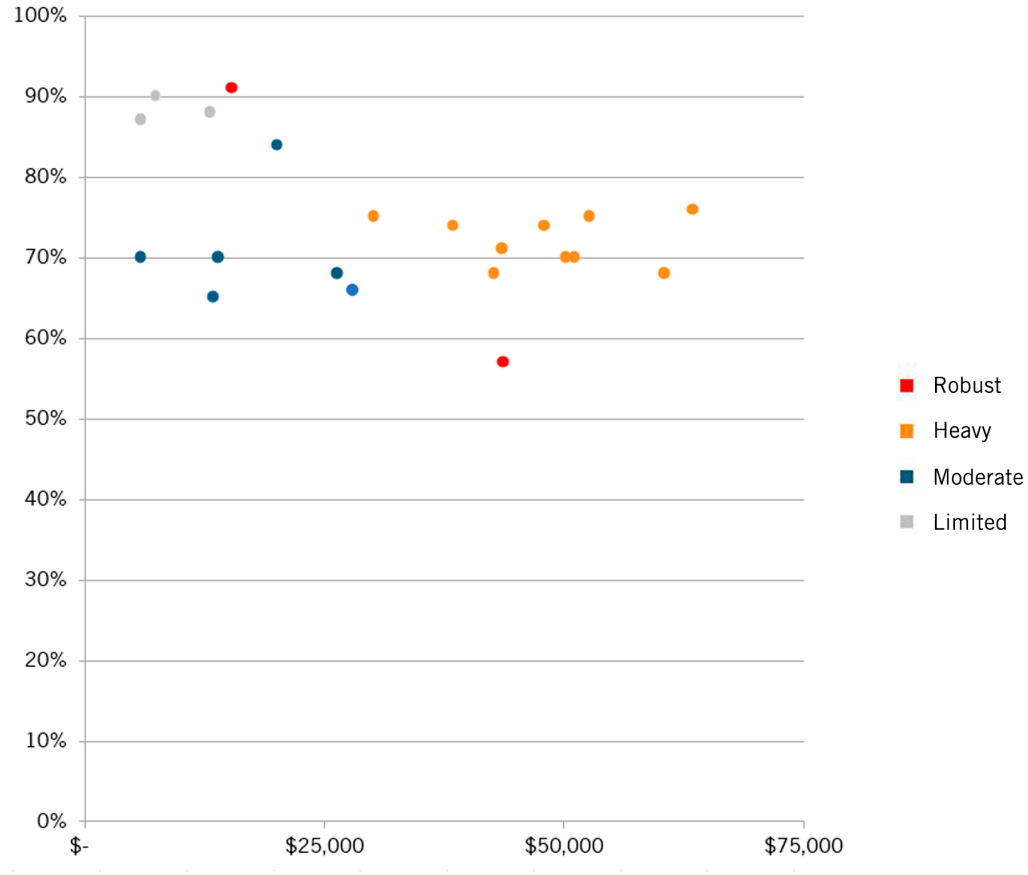
Instead, overly restrictive rules for the digital economy reduce innovation in ways that harm both businesses and consumers. By raising compliance costs, increasing legal risks, and reducing the effectiveness of online business models, these rules lead to a reduction in the supply of or demand for digital services. Therefore, policymakers should give extra scrutiny to trust-promoting reflexive regulations as they attempt to find the right balance between legitimate privacy and security concerns and innovation to increase overall consumer welfare. To do this, policymakers should pursue a three-part test for data protection regulations that targets specific, substantial harm, while weighing the regulation against its costs and countervailing benefits.

APPENDIX A: RELATIVE DATA PROTECTION REGIMES ACROSS SEVEN COUNTRIES.[131]

Country	Regulations	Regulatory Strength
China	While China does not have a specific data protection law, its constraints over the use of personal data are spread across several laws. China's cybersecurity protection law creates much more onerous protections than GDPR.	Robust
Japan	Japan's Act on the Protection of Personal Information (APPI) regulates privacy protection issues in Japan. It also has a central agency that supervises issues of privacy protection.	Robust
Australia	Australia has several federal and state laws that govern data protection, including the Federal Privacy Act and the Australian Privacy Principles.	Heavy
Canada	Canada has 28 federal, provincial, and territorial privacy laws. Among its federal rules, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private companies use personal data.	Heavy
France	Law No. 7817 on "Information Technology, Data Files, and Civil Liberty" is the principal law regulating data protection in France. Also subject to GDPR.	Heavy
Germany	Germany implemented the EU Data Protection Directive through its Federal Data Protection Act. It is also subject to GDPR.	Heavy
Italy	Italy implemented the EU Data Protection Directive through the Italian Data Protection Code. It is also subject to GDPR.	Heavy
Hong Kong	Hong Kong's Personal Data Ordinance (Cap. 486) regulates the collection and handling of personal data.	Heavy
Poland	Poland implemented the EU Data Protection Directive in the Personal Data Protection Act. It is also subject to GDPR.	Heavy
Sweden	Sweden implemented the EU Data Protection Directive through the Swedish Personal Data Act. It also has several sector-specific laws, such as the Patient Data Act and the Marketing Act. It is also subject to GDPR.	Heavy
United Kingdom	The United Kingdom implemented the EU Data Protection Directive through its Data Protection Act.	Heavy

United States	The United States has about 20 sector-specific or medium-specific national privacy or data security laws, and hundreds of such laws among its states and territories.	Heavy
Egypt	Egypt does not have a specific law that regulates the use of personal data, but it does have several laws and regulations that have provisions that address data protection. For example, the Egyptian Banking Law imposes protections for financial information.	Moderate
Nigeria	Nigeria does not have a comprehensive legislative framework on the protection of personal data. However, it does have a few industry-specific laws and regulations that provide limited protections.	Moderate
Mexico	Mexico has the Protection of Personal Data held by Private Parties Law (Ley Federal de Protección de Datos Personales en Posesión de los Particulares). This law only applies to private individuals or legal entities that process personal data, with several exemptions.	Moderate
Russia	Russia has provisions of data protection in its constitution, through international treaties, and within specific laws. For example, the Data Protection Act requires all personal data operators to store and process any personal data of Russian individuals within databases located in Russia.	Moderate
South Africa	In South Africa, the Protection of Personal Information Act (POPI) creates a regulatory framework for the processing of personal information. However, only certain portions of the act have been implemented.	Moderate
Turkey	Turkey has the Law on the Protection of Personal Data No. 6698, which governs data protection and is primarily based on the EU Directive 95/46/EC.	Moderate
Indonesia	In Indonesia, as of the date of this publication, there is no general law on data protection. However, there are certain regulations concerning the use of electronic data in the telecommunications and banking sectors.	Limited
India	There is no specific legislation on data protection in India. However, some laws contain specific provisions intended to protect electronic data.	Limited
Pakistan	There is no legislation regulating the protection of data in Pakistan.	Limited

APPENDIX B: ANALYSIS OF REGULATORY STRENGTH, TRUST, AND GDP PER CAPITA OF 21 NATIONS[132]



As this data shows, richer countries tend to have higher levels of digital regulation and moderate levels of trust. Examining only countries with moderate and heavy regulations, countries with stronger regulations may have slightly higher levels of trust, but this difference is not significant. This is especially the case if you ignore Mexico, an outlier country with moderate regulation and high levels of Internet trust. Indeed, because no rich country has moderate or limited levels of data protection regulations, it is difficult to truly ascertain the relationship between regulation and Internet trust.

Interestingly, the two countries with robust data protection regulations—China and Japan—have opposite levels of trust in the Internet. This is likely because there is a strong positive relationship between poor countries and higher levels of trust. Countries with limited data protections, and China, are some of the poorest countries per capita on the survey; while Japan and the countries with heavy regulations are the richest. Surely, the lesson to learn here is not that countries should decrease their wealth per capita to spur trust in the Internet. More likely, Internet users in these countries are more worried about other issues and are not preoccupied with concerns about online privacy.

ENDNOTES

1. 42 U.S.C. §3604. For example, the Fair Housing Act enables users to place trust in rental managers because they cannot use user data to discriminate against renters based on race, religion, national origin, or age.
2. For examples, please see: William Clinton, "A Framework for Global Electronic Commerce," (The White House), accessed June 6, 2018, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html; "Implementing the President's Management Agenda for E-Government," (Executive office of the President of the United States, April 2003), accessed June 6, 2018, 37, https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_055959.pdf; Afua Bruce, Dan Correa, and Suhas Subramanyam, "Internet of Things: Examining Opportunities and Challenges," (The White House, August 30, 2016), accessed June 6, 2018, https://obamawhitehouse.archives.gov/blog/2016/08/30/internet-things-examining-opportunities-and-challenges.
3. "Commission Publishes Guidance on Upcoming New Data Protection Rules," *European Commission*, January 24, 2018, accessed June 6, 2018, http://europa.eu/rapid/press-release_IP-18-386_en.htm.
4. Daniel Castro, "Comments Before the Division of Advertising Practicing at the Federal Trade Commission," (the Information Technology and Innovation Foundation, September 22, 2012), accessed June 6, 2018, http://www2.itif.org/2012-ftc-coppa-filing.pdf.
5. William Clinton, "A Framework for Global Electronic Commerce," (the White House), accessed June 6, 2018, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html; "Defending America's Cyberspace," (the White House, 2000), accessed June 6, 2018, https://fas.org/irp/offdocs/pdd/CIP-plan.pdf.
6. "Implementing the President's Management Agenda for E-Government," (Executive office of the President of the United States, April 2003), National Academies, accessed June 6, 2018, 37, https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_055959.pdf. See performance metrics for trust reference.
7. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," (the White House, 2012), Journal of Privacy and Confidentiality, accessed June 6, 2018, 95, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc.
8. Lawrence Strickling, "The Importance of Trust on the Internet," *National Telecommunications and Information Administration,* January 28, 2011, accessed June 6, 2018, https://www2.ntia.doc.gov/node/752.
9. Andrus Ansip, "Online Privacy, Building Trust in the Digital Age," *European Commission*, September 5, 2017, accessed June 6, 2018, https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/online-privacy-building-trust-digital-age_en.
10. Andrew Keen, *How to Fix the Future*, (New York City, New York: First Grove Atlantic, 2018).
11. European Commission, "How Digital is Your Country? Europe Improves But Still Needs to Close Digital Gap," news release, March 3, 2017, accessed June 6, 2018, http://europa.eu/rapid/press-release_IP-17-347_en.htm
12. "Horizontal Provisions For Cross-border Data Flows and For Personal Data Protection," (European Commission, 2018), POLITICO, accessed June 6, 2018, https://www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf.
13. "OECD Digital Economy Outlook 2017," (OECD, 2017), OECD Publishing, Paris, accessed June 6, 2018, 33, http://dx.doi.org/10.1787/9789264276284-en.

14. "Digital Dividends," (World Bank, 2016), accessed June 6, 2018, 225, http://www.worldbank.org/en/publication/wdr2016.

15. Human Rights Council, "Agenda Item 3: Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development," United Nations, June 2014, accessed June 6, 2018, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

16. "Trust in Digital Life," *Trust In Digital Life*, accessed June 6, 2018, https://trustindigitallife.eu/; "About Us," *Online Trust Alliance*, June 6, 2018, https://otalliance.org/about-us.

17. Marc Rotenberg, "The Reform of the EU Data Protection Framework—Building Trust in a Digital and Global World," (Electronic Privacy Information Center, October 2012), accessed June 6, 2018, https://epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf.

18. Jules Polonetsky and Omer Tene," The Ethics of Student Privacy: Building Trust for Ed Tech," (Future of Privacy Forum, August 2016), accessed June 6, 2018, https://fpf.org/wp-content/uploads/2016/06/Ethics-of-Student-Privacy_Polonetsky-Tene.pdf; "Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft," (Future of Privacy Forum, August 2016), accessed June 6, 2018, https://fpf.org/wp-content/uploads/2016/08/Drones_and_Privacy_by_Design_FPF_Intel_PrecisionHawk.pdf.

19. Murad Hemmadi, "Greater Data Privacy 'Breeds Innovation,' Says Ont. Privacy Commissioner Ann Cavoukian," *Canadian Business*, June 17, 2014, accessed June 6, 2018, http://www.canadianbusiness.com/technology-news/ann-cavoukian-privacy-leads-to-innovation/.

20. Deven McGraw et al, "Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange," *Health Affairs*, Vol. 28, Number 2, March 2009, accessed June 6, 2018, http://shea.senate.ca.gov/sites/shea.senate.ca.gov/files/McGraw_Health.pdf.

21. Niklas Luhmann et al., *Trust and Power*, (Chichester: 1979); Mark Frolick and Lei-Da Chen. "Assessing M-Commerce Opportunities," Information Systems Management 21 (2): 53–61, 2004, accessed June 6, 2018, https://doi.org/10.1201/1078/44118.21.2.20040301/80422.8; Sirkka Jarvenpaa, Noam Tractinsky, and Michael Vitale, "Consumer Trust in an Internet Store," Information Technology and Management, November 2000, accessed June 6, 2018, 45-71, https://link.springer.com/article/10.1023/A:1019104520776; Roger Mayer et al, "An Integrative Model of Organizational Trust," the Academy of Management Review, 1995, Vol. 20, No. 3, accessed June 21, 2018, 709-734 http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=FE83A7DD8D17CC40D55C88CDCCAB73B3?doi=10.1.1.457.8429&rep=rep1&type=pdf.

22. Jong Kyu Choi and Yong Gu Ji, "Investigating the Importance of Trust on Adopting an Autonomous Vehicle," International Journal of Human–Computer Interaction October 3, 2015, 31, no. 10, , accessed June 6, 2018, 692–702, https://doi.org/10.1080/10447318.2015.1070549; Jarvenpaa, Tractinsky, and Vitale, "Consumer Trust in an Internet Store."

23. "OECD Digital Economy Outlook 2017."

24. Ibid.

25. Ibid.

26. David Gefen, "E-Commerce: The Role of Familiarity and Trust," Omega (28:6), 2000, accessed June 6, 2018, 725-73, https://doi.org/10.1016/S0305-0483(00)00021-9; Mary Culnan and Pamela Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science (10, 1), February 1999, accessed June 8, 2018, 104-115; David Gefen, Elena Karahanna, and Detmer Straub, "Trust and TAM in Online Shopping: An Integrated Model," MIS Quarterly, (27: 1), 2003, accessed June 8, 2018, https://pdfs.semanticscholar.org/1bd2/7a9c5434699f6cab538f0bbb414246f09b0e.pdf.

27. Shumaila Yousafzai, Gordon Foxall, John Pallister, "Multidimensional Role of Trust in Internet Banking Adoption," Service Industries Journal, Vol. 29, No. 5, May 2009, accessed June 12, 2018, 591-605, https://www.researchgate.net/profile/Gordon_Foxall/publication/247523936_Multidimensional_role_of_trust_in_Internet_banking_adoption/links/09e4150a577607590d000000/Multidimensional-role-of-trust-in-Internet-banking-adoption.pdf; Mary Eastlick, Sherry Lotz, and Patricia Warrington, "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," Journal of Business Research, Vol 59, Iss. 8, August 2006, accessed June 12, 2018, 877-886, https://www.sciencedirect.com/science/article/pii/S0148296306000713; France Belanger, Janine S Hiller, and Wanda J Smith. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," The Journal of Strategic Information Systems December 1, 2002, Vol. 11, no. 3, accessed June 10, 2018, 245–70. https://doi.org/10.1016/S0963-8687(02)00018-5.

28. S.E. Kruck et al, "Protecting Personal Privacy on the Internet," Information Management & Computer Security, 2002, Vol. 10 No. 2, accessed June 12, 2018, 77-84, https://www.researchgate.net/profile/S_E_Kruck/publication/220208198_Protecting_personal_privacy_on_the_Internet/links/54e688820cf277664ff5f6a5.pdf; B. Gavish and J.H. Gerdes , "Anonymous mechanisms in group decision support systems communication", Decision Support Systems, 1998, Vol. 23, accessed June 13, 2018, 297-328, https://dl.acm.org/citation.cfm?id=302105; Muhammad Usman Shah, Syeda Fatimee, Dr. Muhammad Sajjad, "Mobile Commerce Adoption: An Empirical Analysis of the Factors Affecting Consumer Intention to Use Mobile Commerce," J. Basic. Appl. Sci. Res., 2014, 4(4), accessed June 13, 2018, 80-88, https://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%204(4)80-88,%202014.pdf; Culnan and Armstrong, 1999; France Belanger, Janine Hiller, and Wanda Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," The Journal of Strategic Information Systems, December 2002, Vol 11, Issue 3-4, accessed June 13, 2018, 245-270, https://www.sciencedirect.com/science/article/pii/S0963868702000185.

29. D. Cho, H. J. Kwon, and H. y Lee, "Analysis of Trust in Internet and Mobile Commerce Adoption," In 40th Annual Hawaii International Conference on System Sciences, 2007, 50–50, accessed June 13, 2018, https://doi.org/10.1109/HICSS.2007.76.

30. Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," (the Information Technology and Innovation Foundation, September 2015), accessed June 11, 2018, http://www2.itif.org/2015-privacy-panic.pdf.

31. M. J. Culnan and P. K Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science (10, 1), February 1999, accessed June 10, 2018, 104-115, https://pubsonline.informs.org/doi/abs/10.1287/orsc.10.1.104.

32. P. A. Pavlou and D. Gefen, "Building Effective Online Auction Marketplaces with Institution-based Trust," Proceedings of the 23rd International Conference on Information Systems, Paper 2002 Proceedings, Paper 63, 2002, accessed June 10, 2018, 667-675, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.9167&rep=rep1&type=pdf.

33. R. Gulati and M. Sytch,, "The Dynamics of Trust", Academy of Management Review, 2008, Vol. 33, No. 1, accessed June 10, 2018, 276-8, http://www.academia.edu/9260493/Consumer_acceptance_of_internet_banking_the_influence_of_internet_trust.

34. Sirkka Jarvenpaa, Kathleen Knoll, and Dorothy Leidner "Is Anybody Out There? Antecedents of Trust in Global Virtual Teams," Journal of Management Information Systems (14:4), 1998, accessed June 10, 2018, 29-64, https://pdfs.semanticscholar.org/43c8/f25b626cb154969a61cc26c94936b62a3091.pdf; D. McKnight, , V. Choudhury, and C. Kacmar, "Trust in E-Commerce Vendors: A Two-Stage Model," Proceedings of the 21st International Conference on Information Systems, W. Orlikowski, S. Ang, P. Weill, H. Kacmar, and J. I. DeGross (eds), Brisbane, Australia, 2000, accessed June 10, 2018, 532-536, http://aisel.aisnet.org/icis2000/54/.

35. Bill McEvily and Marco Tortoriello. "Measuring Trust in Organisational Research: Review and Recommendations." Journal of Trust Research, April 1, 2011, no. 1, accessed June 14, 2018, 23–63. https://doi.org/10.1080/21515581.2011.552424.

36. Matthew Lee and Efraim Turban, "A Trust Model for Consumer Internet Shopping." International Journal of Electronic Commerce /Fall 6, September 21, 2001, accessed June 10, 2018, 75–91, https://www.researchgate.net/profile/Matthew_Lee3/publication/228540562_A_Trust_Model_for_Consumer_Internet_Shopping/links/00b4951806a572497e000000/A-Trust-Model-for-Consumer-Internet-Shopping.pdf.

37. Ibid.

38. Heather Green, "A Little Net Privacy, Please," *Bloomberg*, March 16, 1998, accessed June 12, 2018, https://www.bloomberg.com/news/articles/1998-03-15/a-little-net-privacy-please; Lynn Margherio et al, "The Emerging Digital Economy," (the Economics and Statistics Administration, July 1, 1998), accessed June 12, 2018, http://www.esa.doc.gov/sites/default/files/emergingdig_0.pdf.

39. "Special Eurobarometer 431," (European Commission, June 2015), accessed June 19, 2018, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf; "Special Eurobarometer 431," (European Commission, November 2013), accessed June 19, 2018, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_404_en.pdf.

40. Inc, Gallup. "Few Consumers Trust Companies to Keep Online Info Safe." *Gallup.com*. accessed June 12, 2018. http://news.gallup.com/poll/171029/few-consumers-trust-companies-keep-online-info-safe.aspx.

41. Ibid.

42. "Social Media Fact Sheet." *Pew Research Center: Internet, Science & Tech*, February 5, 2018. http://www.pewinternet.org/fact-sheet/social-media/; "UPS Study: U.S. Online Shoppers Turning to International Retailers." *comScore, Inc.*, accessed June 12, 2018. http://www.comscore.com/Insights/Press-Releases/2017/6/UPS-Study-US-Online-Shoppers-Turning-to-International-Retailers.

43. Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," *Pew Research Center: Internet, Science & Tech*, May 20, 2015, accessed June 12, 2018, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

44. "Inaugural Tech Media Telecom Pulse Survey 2018," *HarrisX*, April 2018, accessed June 12, 2018, http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-16Apr18_Library_V3.pdf.

45. Robert Atkinson, "I Object, Your Honor: Pew Is Leading the Witness (and Confirming Its Own Bias) in Its Survey on Automation and Jobs," (the Information Technology and Innovation Foundation, October 6, 2017), accessed June 12, 2018, https://itif.org/publications/2017/10/06/i-object-your-honor-pew-leading-witness-and-confirming-its-own-bias-its.

46. Lymari Morales, "U.S. Internet Users Ready to Limit Online Tracking for Ads," *Gallup*, December 21, 2010, accessed June 19, 2018, http://news.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx.

47. Lee Rainie and Maeve Duggan, "Privacy and Information Sharing," (Pew Research Center, Science & Tech, January 14, 2016), accessed June 19, 2018, http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

48. Ibid.

49. Daniel Castro, "No Americans Are Not Afraid of Smart Homes," *Center for Data Innovation*, January 18, 2016, accessed June 19, 2018, https://www.datainnovation.org/2016/01/no-americans-are-not-afraid-of-smart-homes/.

50. "Privacy Statement for Nest Products and Services," *Nest*, May 23, 2018, accessed June 19, 2018, https://nest.com/legal/privacy-statement-for-nest-products-and-services/; "Privacy Policy and Terms of Use*, Ecobee*, accessed June 19, 2018, https://www.ecobee.com/legal/use/; "Honeywell Connected Home Privacy Statement," *Honeywell*, May 23, 2018, accessed June 19, 2018, https://yourhome.honeywell.com/privacy-statement.

51. Naveen Farag Awad and M. S. Krishnan, "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," MIS Quarterly, 2006, 30 (1), accessed June 20, 2018, 13–28, https://doi.org/10.2307/25148715.

52. Alessandro Acquisti and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." IEEE Security & Privacy 1, 2005, accessed June 20, 2018, 26-33, https://www.dtc.umn.edu/weis2004/acquisti.pdf.

53. Soren Preibusch et al., "Price versus Privacy: An Experiment into the Competitive Advantage of Collecting Less Personal Information | SpringerLink." Electronic Commerce Research, Vol. 13, Iss. 4, November 2013, accessed June 19, 2018, 423-455, https://link.springer.com/article/10.1007/s10660-013-9130-3.

54. Ibid.

55. Christian Happ et al., "Trick with Treat – Reciprocity Increases the Willingness to Communicate Personal Data - ScienceDirect." Computers in Human Behavior, Vol. 61, August 2016, 372-377, accessed June 19, 2018. https://www.sciencedirect.com/science/article/pii/S0747563216301935.

56. Susan Athey, Christian Catalini, and Catherine Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," NBER Working Paper No. 23488, June 2017, accessed June 19, 2018, https://people.stanford.edu/athey/sites/default/files/digital_privacy_paradox_02_13_17.pdf.

57. Mary Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era," (Pew Research Center, November 12, 2014), accessed June 19, 2018, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

58. "Special Eurobarometer 431," (European Commission, June 2015).

59. Alan F. Westin "The Public's View of When Privacy Self-Regulation Is Appropriate: 'Whatever Works' The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues," NTIA, Privacy & American Business, accessed June 19, 2018, https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

60. Jennifer King, "Taken Out of Context: An Empirical Analysis of Westin's Privacy Scale," Symposium on Usable Privacy and Security (SOUPS), 2014, accessed June 19, 2018, https://pdfs.semanticscholar.org/22a4/a1e952c163b91b9fb3aaf5ad7fdc026e16d1.pdf.

61. Ibid.

62. Ibid.

63. Alan F. Westin "The Public's View of When Privacy Self-Regulation Is Appropriate: 'Whatever Works' The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues.

64. Helen Nissenbaum, « Can Trust Be Secured Online? A theoretical Perspective," *Erica e Politica,* 1(2) December 1999, accessed June 11, 2018, https://www.openstarts.units.it/bitstream/10077/5544/1/Nissenbaum_E%26P_I_1999_2.pdf.

65. "Bicycle Helmet Standards," *Helmets.org*, accessed June 11, 2018, https://helmets.org/standard.htm.

66. These countries include Australia, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Mexico, Nigeria, Pakistan, Poland, Russia, Sweden, South Africa, Turkey, the United Kingdom, and the United States.

67. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust," (Centre for International Governance Innovation and IPSOS, May 2018), accessed June 11, 2018, https://www.cigionline.org/internet-survey-2018.

68. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust." Question: To what extent do you agree or disagree with the following statements: Base: All Respondents 2018 (n=24,962); 2017 (n=24,22).

69. "Data Protection Laws of the World," *DLA Piper*, accessed June 2018, https://www.dlapiperdataprotection.com/.

70. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust."

71. "Standard Eurobarometer 88 Autumn 2017," (European Commission and Directorate-General for Communication, November 2017), accessed June 11, 2018, 21. Specifically, the Eurobarometer question asks, "I would like to ask you a question about how much trust you have in certain media and institutions. For each of the following media and institutions, please tell me if you tend to trust it or tend not to trust it."

72. For examples, see "Directive on Privacy and Electronic Communications," Official Journal of the European Union, December 18, 2009, accessed June 18, 2018, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF; Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014).

73. "Reasons for Not Having Internet Access At Home," *Eurostat,* accessed June 19, 2018, http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do Households- reasons for not having the internet access at home.

74. "Reasons for Not Having Internet Access At Home," *Eurostat;* "Level of Internet Access – Households," *Eurostat*, accessed June 19, 2018, http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00134&plugin=1.

75. Ibid.

76. "Reasons for Not Having Internet Access At Home," *Eurostat;* "Level of Internet Access – Households," *Eurostat*; Data from Internet Use at Home "Digital Nation Data Explorer," National Telecommunications and Information Administration, June 06, 2018, accessed June 19, 2018, https://www.ntia.doc.gov/data/digital-nation-data-explorer#sel=internetUser&demo=&pc=prop&disp=chart; Data from Nonuse of the Internet at Home "Digital Nation Data Explorer," National Telecommunications and Information Administration, June 06, 2018, accessed June 19, 2018, https://www.ntia.doc.gov/data/digital-nation-data-explorer#sel=internetUser&demo=&pc=prop&disp=chart.

77. "Global Internet Report 2016," (Internet Society, 2016), accessed June 19, 2018, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf; "Internet Use at Home" -"Digital Nation Data Explorer," National Telecommunications and Information Administration; "Main Reason for Not Going Online at Home: Privacy and Security Concerns," -"Digital Nation Data Explorer," National Telecommunications and Information Administration, accessed June 21, 2018, https://www.ntia.doc.gov/data/digital-nation-data-explorer#sel=privSecMainReason&demo=&pc=prop&disp=chart.

78. Data from Nonuse of the Internet at Home "Digital Nation Data Explorer," National Telecommunications and Information Administration.

79. "Global Internet Report 2016," (Internet Society, 2016), accessed June 19, 2018, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.

80. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust."

81. See Internet use over time, "Internet Fact Sheet," (Pew Research Center, February 5, 2018), accessed June 19, 2018, http://www.pewinternet.org/fact-sheet/internet-broadband/; "Level of Internet Access – Households," *Eurostat*; "Percentage of Individuals Using the Internet," International Telecommunications Union, 2005-2017, accessed June 19, 2018, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
82. "Directive on privacy and electronic communications," Official Journal of the European Union.
83. "Digital Nation Data Explorer," National Telecommunications and Information Administration.
84. "Percentage of Individuals Using the Internet," International Telecommunications Union.
85. "EU Law on Cookies," *DLA Piper*, September 2014, accessed June 19, 2018, https://iapp.org/media/pdf/resource_center/DLA_EU_cookie_implementation_9-14.pdf.
86. Ibid.
87. "Internet Fact Sheet," Pew Research Center; "Percentage of Individuals Using the Internet," International Telecommunications Union.
88. "Internet Fact Sheet," Pew Research Center; "Internet Use by Individuals in the last 12 months," *Eurostat,* accessed June 21, 2018, http://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00028&language=en.
89. Ibid.
90. "Individuals Using the Internet for Participating in Social Networks," *Eurostat*, accessed June 20, 2018, http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&plugin=1&pcode=tin00127&language=en.
91. See Social Media Use Over Time, "Social Media Fact Sheet," (Pew Research Center, February 5, 2018), accessed June 19, 2018, http://www.pewinternet.org/fact-sheet/social-media/; "Individuals Using the Internet for Participating in Social Networks," *Eurostat*.
92. Ibid.
93. Ibid.
94. Data from Shopping, Making Reservations, or Using Other Consumer Services Online, "Digital Nation Data Explorer," *National Telecommunications and Information Administration*, accessed June 2-, 2018, https://www.ntia.doc.gov/data/digital-nation-data-explorer#sel=eCommerceUser&demo=&pc=prop&disp=chart; "Internet Purchases by Individuals – All Individuals," *Eurostat*, March 15, 2018, accessed June 20, 2018, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bdek_smi&lang=en.
95. Ibid.
96. Ibid.
97. "Digital Single Market – Promoting e-Commerce for Individuals," *Eurostat*.
98. Rita Heimes and Same Pfeifle, "Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide." November 9, 2016, accessed June 12, 2018. https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.
99. "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce," (European Centre for International Political Economy, March 2013), accessed June 12, 2018, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.
100. Daniel Castro and Alan McQuinn, "The Economic Costs of the European Union's Cookie Notification Policy," (the Information Technology and Innovation Foundation, November 2017), accessed June 12, 2018, http://www2.itif.org/2014-economic-costs-eu-cookie.pdf?_ga=2.39300707.1184190800.1523899147-2007345232.1523368944.

101. Nigel Corey, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," (the Information Technology and Innovation Foundation, May 1, 2017), accessed June 12, 2018, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

102. "Qualifying the Cost of Forced Localization," (Leviathan Security Group, June 2015), accessed June 12, 2018, https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization.

103. Ibid.

104. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, March 27, 2018), accessed June 12, 2018, http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

105. Thomas Lenard and Paul Rubin, "In Defense of Data: Information and the Costs of Privacy," (Technology Policy Institute, May 2009), accessed June 12, 2018, https://techpolicyinstitute.org/wp-content/uploads/2009/05/in-defense-of-data-information-2007385.pdf.

106. Ibid.

107. Hal Varian, "Economic Aspects of Personal Privacy." Privacy and Self-regulation in the Information Age (1996); Thomas Lenard and Paul Rubin, "In Defense of Data: Information and the Costs of Privacy," (Technology Policy Institute, May 2009), accessed June 19, 2018, https://techpolicyinstitute.org/wp-content/uploads/2009/05/in-defense-of-data-information-2007385.pdf.

108. "Consumers Driving the Digital Update: The Economic Value of Online Advertising-based Services For Consumers," (McKinsey & Company for Internet Advertising Board Europe, September 2010), accessed June 12, 2018, https://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf.

109. "Net Benefits: How to Quantify the gains that the Internet has brought to consumers," *The Economist*, March 7, 2013. accessed June 12, 2018, http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gainsinternet-has-brought-consumers-net-benefits.

110. "IAB Internet advertising revenue report," (IAB, April 2013), accessed July 5, 2018, https://www.iab.com/wp-content/uploads/2015/05/IABInternetAdvertisingRevenueReportFY2012POSTED.pdf; "IAB Internet advertising revenue report," (IAB, May 2018), accessed July 5, 2018, https://www.iab.com/wp-content/uploads/2018/05/IAB-2017-Full-Year-Internet-Advertising-Revenue-Report.REV2_.pdf; "ADEX Benchmark 2017," (IAB Europe and IHS Markit, 2017), accessed July 5, 2018, https://www.iabeurope.eu/wp-content/uploads/2018/06/IAB-Europe_AdEx-Benchmark-2017-Report_FINAL-V2.pdf.

111. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules," *the Information Technology and Innovation Foundation*, October 6, 2017, accessed June 12, 2018, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.

112. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising." SSRN Scholarly Paper ID 1600259, 2010, Rochester, NY, Social Science Research Network, accessed June 12, 2018, https://papers.ssrn.com/abstract=1600259.

113. Alan McQuinn, "The Detractors are Wrong, Online Ads Add Value," *the Information Technology and Innovation Foundation*, December 8, 2016, accessed June 12, 2018, https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value.

114. Sandra Milberg, Jeff Smith, and Sandra J. Burke. "Information Privacy: Corporate Management and National Regulation." Organization Science 11, no. 1 (2000), accessed June 12, 2018, 35-57, https://pubsonline.informs.org/doi/abs/10.1287/orsc.11.1.35.12567?journalCode=orsc.

115. Caleb Fuller. "The Perils of Privacy Regulation." The Review of Austrian Economics 30 (2): 193 –214. https://doi.org/10.1007/s11138-016-0345-0.

116. Ibid.

117. Josh Lerner, "The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies," Analysis Group, 2012, accessed June 12, 2018, 1-2, https://slidex.tips/download/the-impact-of-privacy-policy-changes-on-venture-capital-investment-in-online-adv.

118. Anja Lambrecht, "E-Privacy Provisions and Venture Capital Investments in the EU," (Disruptive Competition Project, January 15, 2018), accessed June 12, 2018, https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF.

119. Regulation 2016/679 (General Data Protection Regulation), Article 6, (see page L 119/36-37), accessed December 19, 2017, http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf; Directive 95/46/EC (Data Protection Directive), Article 6(1)(b), (see page L 281/40), accessed January 3, 2018, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

120. "Internet of Things: Privacy and Security in a Connected World," (Federal Trade Commission, January 2015), accessed June 12, 2018, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

121. Joshua New, "5 Q's for Andrea Burbank, Search and Data Mining Engineer at Pinterest," *Center for Data Innovation*, February 23, 2015, accessed June 12, 2018, http://www.datainnovation.org/2015/02/4077/.

122. Amalia Miller, and Catherine Tucker "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Management Science, 2009, 55 (7), accessed June 12, 2018, 1077–1093, https://doi.org/10.1287/mnsc.1090.1014.

123. Ibid.

124. Daniel Castro, "Benefits and Limitations of Industry Self-Regulation For Online Behavioral Advertising," (the Information Technology and Innovation Foundation, December 2011) accessed June 11, 2018, http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

125. Robert Atkinson, Daniel Castro and Alan McQuinn, "ITIF Filing to FTC on Informational Injury Workshop," (the Information Technology and Innovation Foundation, October 27, 2017), accessed June 11, 2018, https://itif.org/publications/2017/10/27/itif-filing-ftc-informational-injury-workshop.

126. Ibid.

127. Daniel Castro and Alan McQuinn, "Comments to FTC on Nomi Technologies, Inc," (The Information Technology and Innovation Foundation, May 26, 2015), accessed June 19, 2018, https://itif.org/publications/2015/05/26/comments-ftc-nomi-technologies-inc.

128. Spokeo, Inc. v. Robins, 578 S. Ct. ___, No. 13-1339 (2016). This harm-based approach was recently upheld in spirit in Spokeo, Inc. v. Robins, where the Supreme Court found that a lawsuit based on a technical violation of the FCRA that did not result in harm lacked standing. Regulators should follow this example and avoid issuing "gotcha" style statutory penalties.

129. "FTC Policy Statement on Unfairness," *The Federal Trade Commission*, accessed June 11, 2018, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

130. Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation," *Center for Data Innovation*, November 4, 2013, accessed June 19, 2018, http://www2.datainnovation.org/2013-data-innovation-101.pdf.

131. "Data Protection Laws of the World," *DLA Piper.*

132. "Data Protection Laws of the World," *DLA Piper;* "2018 CIGI-Ipsos Global Survey on Internet Security and Trust," (Centre for International Governance Innovation and IPSOS); The Conference Board, Total Economy Database (Per Capita Income, accessed June 21, 2018), https://www.conference-board.org/data/economydatabase/index.cfm?id=27762.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Robert Atkinson, Michael McLaughlin, Alex Key, and Nils Kuehn. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Alan McQuinn is a senior analyst at ITIF. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Representative Anna Eshoo (D-CA) and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He graduated from the University of Texas at Austin with a B.S. in public relations and political communications.

Daniel Castro is vice president of ITIF. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.