Why Stronger Privacy Regulations Do Not Spur Increased Internet Use

BY ALAN MCQUINN AND DANIEL CASTRO | JULY 2018

Policymakers are often told that data protection regulations are justified because they will increase consumer trust, and therefore technology adoption and use. But there is little evidence to back up this claim.

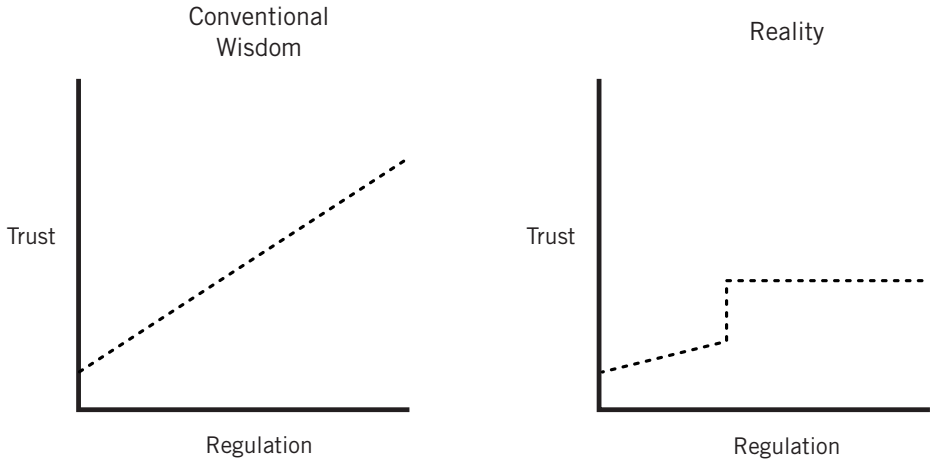
Over the last two decades, it has become the conventional wisdom in tech policy circles that stronger privacy regulations increase consumer trust, and higher levels of consumer trust will lead to more technology use. Few observers who should know better have challenged this assumption, and now many who 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.

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.[1] The European Union has also invoked increasing trust as a justification for numerous data protection regulations, including its new General Data Protection Regulation (GDPR).[2] And most privacy advocates have justified their calls for stricter privacy laws on the grounds that they boost trust, which in turn boosts digital technology usage.

In this framing, the relationships between trust and regulation as well as between regulation and technology adoption and use are linear: More regulation leads to more trust, and more trust produces more adoption and use. Therefore, stricter privacy regulations will boost adoption and use—regardless of baseline levels of regulation that already exist. For policymakers considering regulation, this is the proverbial free lunch: The more regulations they create, the larger the economic benefits they will reap. In fact, however, the relationship between trust and regulation is likely not 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.[3] As such, there is 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 can mean 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).

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



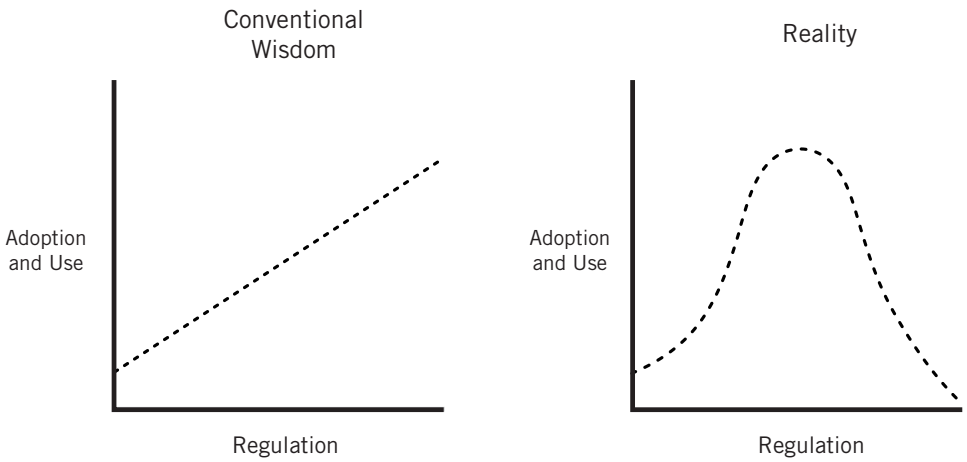
Even if strengthening data privacy rules beyond some baseline level does not increase trust, what would be wrong with enacting additional rules? In other words, if a three-meter fall standard would provide even a modicum of greater bicycle safety than the current two-meter standard, why not simply mandate the higher standard? The answer is the same for all regulatory decisions: to balance costs 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.

Stringent data protection regulations are the digital equivalent of the three-meter helmet standard. More stringent rules raise compliance costs and reduce advertising revenues for companies that provide online services. And higher costs with lower revenues reduces the investments companies can make to improve their services. For example, one reason there are relatively few high-quality, ad-supported websites and apps for children in the United States is that the U.S. Congress has enacted strict privacy laws that limit the viability of these services.[4] While baseline protections may have a modest effect in increasing the trust people place in digital technologies, past a certain point, stronger data protection regulations usually have the unintended consequence of decreasing the supply of technology. Therefore, rather than describe the relationship between regulation and digital technology adoption and use as linear, it is best described as an inverted U-curve (figure 2).

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.

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



In this report, we attempt to decipher which is correct, the conventional wisdom or our hypothesis. To achieve this, we analyze three relationships: whether regulation has an effect on trust, whether regulation has an effect on willingness to adopt, and whether regulation has an effect on production and, as a result, usage.

Does Digital Regulation Increase Trust?

First, we use survey evidence to analyze levels of trust across countries with data protection laws and enforcement of various levels of strength.[5] Our analysis suggests that strong data protections regulations have little to no positive effect on trust when compared to other countries with moderate or limited levels of digital regulation. This is perhaps because people interpret stringent privacy regulations as a sign the government is telling its citizens the technology cannot be trusted. As a result, this relationship does not appear to be linear.

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

Does Digital Regulation Increase Willingness to Adopt Internet Applications?

Second, we used survey data to analyze whether digital regulation actually improves individuals' willingness to adopt Internet applications in the European Union and United States.[6] This evidence does not suggest increased regulation leads to a greater willingness to adopt, as countries with stronger regulations also have higher percentages of people who claim to avoid using such technologies due to privacy or security concerns.

We conclude that the relationship between regulation and willingness to adopt is not linear. 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 who do not subscribe to Internet access make that choice for other reasons, such as the lack of a perceived need, insufficient skills, or cost concerns.[7]

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.

Does Digital Regulation Increase Peoples' Usage of Internet Applications?

Finally, we analyze usage rates for three different technology applications—Internet access, social media, and online shopping—before and after the implementation of a European privacy law.[8] In all three categories, the United States showed higher increases in usage than the European Union, despite having more stringent privacy regulation. We found similar patterns comparing usage rates in the United States to those in France and the United Kingdom. In short, the data show no evidence that implementation of strong data protection rules spurred more people to use technology.

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

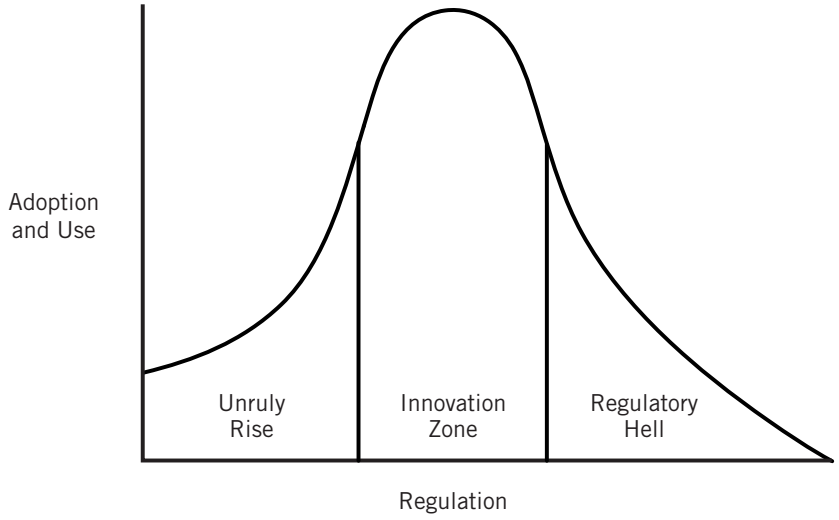
Proponents of strict data regulation ignore the costs. Companies have to devote resources to compliance, which reduces the amount of money that can be invested in innovation. Moreover, strict privacy regulations reduce the revenue digital companies can earn from online ads, thereby reducing the overall 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.[9]

Given the negative effects of overly strict regulation, we conclude that if one of the goals of data protection rules is to increase consumer adoption of online services, then creating rules that add costs and reduce revenues is not the best solution. While baseline protections may have a modest effect in increasing the trust people place in digital technologies, stringent rules not only do not increase trust, they reduce the revenues companies have to develop and improve online 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 digital services is best described as an inverted U-curve with three stages (figure 3). In the

first stage, which we call the "Unruly Rise," a lack of protections—either from government or industry practices—may reduce the growth of consumer adoption and use of Internet applications, because consumers may have lower levels of trust. 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 coupled with a robust digital innovation ecosystem. 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 third stage, which we call "Regulatory Hell," is where overly strict rules can actually harm consumers by creating excessive burdens on digital innovators. After passing the GDPR, the European Union now appears to be descending into the early stages of "Regulatory Hell."

Figure 3: Inverted U-curve showing relationship between regulation and technology adoption and use.



This relationship suggests that there is an optimal level of regulation—a Goldilocks level—of rules that are neither too weak nor too strong. Too little regulation is problematic as it does not provide baseline protections that encourage consumer trust. 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, which in turn results in a reduced supply of technologies and constrains a nation's overall Internet ecosystem.

It is time, therefore, to end the spurious claims that more privacy regulation is pro-innovation and pro-consumer. Policymakers should strive to achieve the right balance between legitimate privacy and security concerns on the one hand and innovation on the other by employing a three-part test for data protection regulations: First, they should target specific, substantial harms. Second, they should directly limit those harms. Third, the costs of the regulations must be outweighed by their countervailing benefits.

ENDNOTES

1. 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.
2. "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.
3. "Bicycle Helmet Standards," *Helmets.org*, accessed June 11, 2018, https://helmets.org/standard.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. "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; "Data Protection Laws of the World," *DLA Piper*, accessed June 2018, https://www.dlapiperdataprotection.com/.
6. For this analysis we used data from nonusers in the European Union and the United States that asked them about why they were not adopting the Internet at home. "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.
7. "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.
8. 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.
9. "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.

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 one of the world's leading science and technology think tanks, 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.