Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation

By Bret Swanson

May 2019

Key Points

- Explosive growth of digital products and services shows that the benefits of data flows far outweigh the costs. Real anxieties about privacy and security, however, could undermine confidence in the digital marketplace if we do not update our laws, norms, institutions, and technologies.
- Slow productivity growth in many industries stems from a lack of information intensity—too little data. Policy should encourage the use of more data, while putting consumers in control of sensitive information.
- We need a new national law to consolidate existing industry-specific laws, prevent a patchwork of conflicting state laws, and clarify the Federal Trade Commission's enforcement strategy for the digital age.

In a world of exploding information, privacy and security are central but vexing policy questions. How we govern the collection and use of data will affect public trust of commercial and public institutions and also help determine the rate of innovation across the economy.

Intense engagement with digital products and services, resulting in an exaflood of data usage, demonstrates that firms and consumers enthusiastically embrace the digital world. In 2018, US internet traffic reached nearly 50 exabytes per month, and in 2019, global data center traffic is expected to reach 14 zettabytes.[1] Voting with their feet, consumer actions show that the benefits of these data flows far outweigh the costs.

At the same time, high-profile data breaches, surprisingly intrusive web tracking, and the confusing nature of social interactions in a hyper-transparent world have caused anxiety—for consumers seeking reassurance, for businesses seeking guidance, and for policymakers seeking the right legal balance.

As information continues to diffuse across the economy and culture, digital privacy and security questions are likely to grow in dimension and intensity. Successful economies and cultures are built on trust. If consumers lose trust in the firms offering them products and services, or in the government's basic protections, the health of the digital economy and our civic culture could deteriorate.

Current laws, written for siloed industries in a pre-digital era, are likely not up to the task. In a world of extreme data abundance and dynamic cross-industry and cross-border data flows, we may need a new privacy law to protect consumers and

encourage open-ended innovation. Privacy is a slippery concept, and it is therefore important to set expectations by defining an analytical framework. Bolstering the approach of the Federal Trade Commission (FTC), which focuses on consumer welfare and rigorous analysis of costs and benefits, is a good place to start.

Laws and regulations, however, cannot solve every problem. Evolving social norms, more robust institutions, and new privacy-promoting technologies will play central roles.

Innovation Through Information

So far, the internet has revolutionized media, search, social, finance, entertainment, and e-commerce. Information technology, however, is now poised to revolutionize many sectors of the economy that have not yet fully exploited the internet and other digital tools. As data collection, creation, and analysis become a more important part of other industries—such as health care and transportation—these privacy questions and policy challenges will multiply.

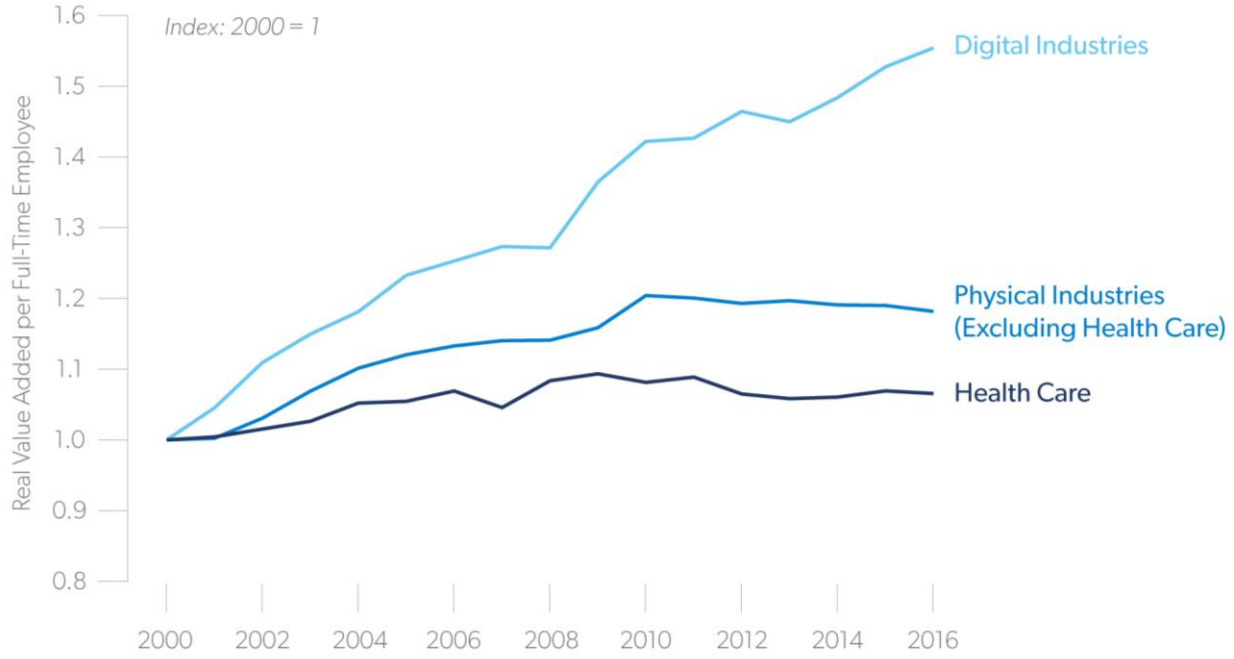
Troves of genetic information and location data and video from vehicles, as just two examples, will radically improve health and safety. But these biological, location, and "surveillance" data are particularly sensitive and need protection. Because digital innovation in the traditional industries that comprise 70 percent of the economy is so important for overall economic growth, getting our privacy and security policies right is crucial for overall economic performance.[2]

Health care is perhaps the starkest example of an industry starved for innovation. Health care spending in the US is pushing past 18 percent of gross domestic product and will likely top 20 percent in the next five years.[3] Yet, this industry, which makes up one-fifth of the economy, is among its very least productive.

Figure 1 shows the vast productivity divergence between industries that make intensive use of information technologies and those that do not. By this rough measure, the digital industries are eight times more innovative than health care.

Fortunately, health care is on the cusp of an information revolution.[4] First, smartphones and other wearable devices will make medicine more personal and cost-effective. Second, based in part on the data collected by these devices, Big Data and artificial intelligence will revolutionize health research. Third, our new understanding of the human body as a complex information network, embodied in genomics

Figure 1. Health Care Productivity Is Stagnant . . . But More Data Can Transform This Crucial Sector



Source: US Bureau of Economic Analysis; and author's calculations.

and proteomics, for example, is finally turning health into an information science. And fourth, building on the foundation of these advances, the business of health care is ripe for transformation, making insurance, diagnostics, delivery, prevention, and maintenance look far more like the modern digital economy than the industrial-era industry it still is today. Increasingly, digital tools will help empower and incentivize healthy behavior, instead of merely fixing what is broken. And health is just one example showing how boosting the information intensity of the economy is central to fostering long-term economic growth.

Europe's and California's Good Intentions

Overly restrictive policies meant to protect consumers could have harmful, unintended consequences. If we preemptively close off creative uses of data and new business models in these heretofore non-digital industries, we could severely depress innovation in many sectors of the economy that need a boost in productivity. On the other hand, if we do not develop a coherent set of legal principles that protect and reassure consumers while offering clarity to businesses, we could lose trust in the digital tools that promise so much commercial and civic innovation.

For the past 20 years, the Section 230 safe harbor has encouraged experimentation and investment across the internet, but new privacy proposals and critiques of Section 230 itself are threatening to upend the bias toward innovation that has, on balance, served us well. (At the same time, technology firms would do well to stop tempting revision of Section 230 by flouting the perceived neutrality of their platforms.)

Europe's new General Data Protection Regulation (GDPR) is an example of well-meaning overreach. In an attempt to protect the public, the GDPR in its short life has already proved to restrict digital offerings, favor large firms over smaller competitors and would-be rivals, confuse international policy and compliance, *and* frustrate consumers. The GDPR may offer several useful ideas for a US law, but overall it continues the over-regulatory approach that has curtailed European innovation over the past few decades.

The new California Consumer Privacy Act (CCPA) is the most ambitious effort so far in the US. Enacted hastily in 2018, it is scheduled to go into effect in 2020. Because of California's size and because so many data-intensive technology firms call California home, its law could have outsize effects across the country and the globe. Several US states are considering similarly counterproductive, although inevitably conflicting, legislation.

As Congress contemplates federal privacy legislation, the CCPA and the GDPR are good examples of what to avoid. The CCPA will be cumbersome for big technology firms, but its effects on small, non-tech businesses are perhaps even more troublesome. Jim Relles, the owner of an independent flower shop in Sacramento, summed up the possible effects.

> To understand why the act will hurt me, consider a consumer who's searching online for a dozen roses for a loved one, or a delicate corsage for a wedding or prom date. The search engine that individual is using provides my advertisement to that individual and if I am fortunate, the consumer visits my store to purchase that floral arrangement.
>
> We have a small website; we keep records of calls; we text customers; we have a "leads" database; we buy digital ads. We do not "collect" data. But under the provisions of the CCPA, we would be considered to be collecting "personal information," even when it is not linked to an individual.
>
> Even as a small business, my company would suffer from CCPA because it would diminish the value and effectiveness of the online marketing tools I'm using now. And if I hit a certain threshold for sales or customer interactions, then I have a whole set of daunting legal compliance obligations. In response, our company would be required to collect more information about consumers than we need and provide it to the consumer upon request. Relles Florist is not a big tech company. The compliance costs of such an effort, in terms of person-hours and data capture, would be hard to bear.[5]

As Eric Goldman, a law professor at Santa Clara University, testified to the California Assembly: "An over-broad definition of 'personal information' creates problems throughout the entire law. . . . Personal information isn't limited to sensitive or obviously identifiable information. . . . It sweeps in any scrap of data that has the theoretical *capability* of being associated with a consumer." He concluded that "CCPA's definition of 'personal information' reaches beyond the analogous GDPR definition" and would be "impossible to administer."[6]

The internet and related data-intensive products and services are the ultimate forms of interstate commerce. A patchwork of state laws could fragment the inherently borderless data economy. Thus, the highly problematic CCPA suggests that a new US law is needed to preempt the states and harmonize the nation's privacy regime.

A Flexible Focus on Consumer Welfare

In the US, the FTC has been grappling with these topics for the past two decades. The FTC has made important progress and is in the middle of a wide-ranging overview of its approach. The next steps are to (1) develop sound legal principles that can address a wide range of digital questions across diverse circumstances, (2) provide clear guidance to both consumers and businesses, and (3) develop the technical and empirical expertise and capacity to address growing challenges.

In such a fast-moving arena, we probably cannot write detailed prescriptive rules that can anticipate every data practice, firm type, degree of injury, and legal clash. The heterogeneity of data (types and sensitivities) and consumers (preferences and prices) argues for more generality and flexibility in enforcement.

Approaches that mimic the common law may thus be appropriate—for example, employing a negligence standard instead of strict liability for data breaches. Some argue that mandating strict liability would encourage firms to substantially boost their focus and spending on security, which may be true in many cases. However, in a world filled with highly sophisticated hackers, including large state actors with massive resources, strict liability may be unrealistic. If the US government cannot protect its own data, nor protect US firms from these powerful adversaries, strict liability seems an overreach.[7] Firms should be held accountable for negligent security practices, but they also need far more support from government to defend themselves and their customers.

In the privacy realm, the FTC's existing consumer welfare standard may be especially well suited to deal with a highly dynamic and evolving digital marketplace. To date, the FTC has approached digital privacy through its Section 5 authority to police deceptive and unfair practices. One way the FTC can help protect consumers is to enforce firms' publicly declared privacy policies. Holding firms accountable for their own assurances is a good baseline for consumer protection.

Although the FTC has historically relied far more heavily on its deceptive practices prong, it has recently begun thinking about and using its unfairness authority to address "information injuries" in a more robust way. First outlined in 1980, the unfairness test, which focuses on consumer injury, was essentially codified by Congress in 1994. On a case-by-case basis, it seeks to assess both costs *and benefits* and thus attempts to quantify net harm. Such categorization and quantification is often difficult, but it is likely better than other, less analytical methods. And it is not limited to clear-cut financial injuries.

Former FTC Commissioner Maureen Ohlhausen has described five types of information injury that the FTC considers: (1) deception injury, which subverts consumer choice; (2) financial injury; (3) health or safety injury; (4) unwarranted intrusion injury; and (5) reputational injury.[8] Over the past two decades, the FTC has brought "at least twenty-eight data privacy cases" in which unfairness was a component and 12 cases in which unfairness was the only component.[9]

The volumes and types of data are likely to grow far faster than our ability to categorize and legally define them. For example, today's health data are mostly confined to hospital and clinic settings. But tomorrow, all sorts of personal data may be considered "health data." There will be all sorts of blurry lines about whose data are whose. Likewise, many new data practices may impose some costs but confer far higher benefits, thus resulting in substantial net consumer gains.

At the same time, an overly detailed set of regulations could, paradoxically, actually leave consumers unprotected from harms that are unforeseen but in

fact very real. It would thus be unwise to attempt to capture every type of data and potential injury and to prescribe every data-handling practice in detailed regulations. A principles-based approach, similar to the FTC's unfairness regime, can better adapt to fast-changing circumstances.

The FTC's data privacy and security regime is not above criticism—far from it. One criticism of the FTC's approach is that the agency does not have the ability to punish firms on the first instance of harm. The agency typically warns a firm or, in more severe cases, enters into a consent decree where the firm agrees to better behavior. Only then, on a second violation, does the agency impose real penalties. Some have suggested that this practice allows "get out of jail free" cards for egregious behavior and that penalties for first violations should be considered.

Many policy proposals underestimate firms' natural incentives to protect user privacy.

This is an example of a marginal policy change in which reasonable people may disagree. However, compared to other proposals that would empower multiple agencies or a new digital economy superregulator, it makes more sense to build on and improve the FTC's existing expertise. Where the FTC lacks the resources to investigate and analyze the burgeoning digital world, Congress would probably do well to enhance its capabilities.

A new federal law reinforcing the FTC's primary role would not only prevent conflicting laws among the states but also help avoid conflicting rules among federal agencies. For example, the Federal Communications Commission's 2015 Open Internet Order sought to impose intrusive privacy regulations on internet service providers, but not on the rest of the online ecosystem. These asymmetric rules, along with the rest of the 2015 Open Internet Order, were quickly repealed. Had the rules remained in place, however, they would have unfairly tilted the playing field for (and against) particular firms and likely depressed investment and innovation in new broadband networks, such as 5G wireless.

Institutions, Norms, and Technologies

Many policy proposals underestimate firms' natural incentives to protect user privacy. As we exit the early internet phase and as data and connectivity diffuse into every part of our lives, privacy protection and data security will likely become an even greater portion of the value proposition, as suppliers of digital devices, tools, software, and content vie for the customer's trust.

In early 2019, for example, Apple launched a major advertising campaign highlighting its "privacy matters" approach to all its products and services. Indeed, there is some evidence that Apple's proprietary and privacy-centric approach has helped it sell smartphones and other products at higher price points than its rivals with more "open" ecosystems, which rely on consumer data for digital advertising. Each approach may have its advantages, and the competition allows consumers to choose how much they value privacy.[10]

In fact, Apple's long focus on privacy may be spurring even data-hungry Google to follow suit. For example, Apple attempts to process as much data on the device as possible to avoid transmitting sensitive information across the network or storing it in the cloud. At its May 2019 I/O conference, Google revealed it would also use more on-device processing and adopt other privacy enhancements, such as "incognito mode" for maps and search.[11]

Other market forces will push and pull on corporate behavior. For instance, Moody's, the bond-rating agency, is now encouraging lenders to consider health care firms' cyber vulnerabilities before making loans.[12]

Varied business models can give consumers a range of options and accommodate a range of consumer preferences regarding privacy trade-offs. For example, some consumers may prefer advertising-based models that offer inexpensive or even "free" content and services in return for more customer data. Other consumers may prefer platforms that do not rely on tracking and sharing (or selling) consumer data. There is likely to be a widely varied mix of these approaches across products and services. And as firms experiment with privacy-price trade-offs, we will learn much more than we know now about people's real preferences. We should not prescribe or proscribe any of these approaches. Consumer choice and control will be the key.

Privacy and security technology will themselves prove to be fast-growing markets. Over the past several years, for example, simple ad blockers were widely deployed, possibly reaching 30 percent of users in 2018.[13] A company called Brave, founded by Brendan Eich, the creator of JavaScript, took the ad blocker several steps further. It developed a new ad-blocking browser and combined it with a new concept of content financing, based not on advertising but on micropayments, to reduce the need for web tracking. Would you rather pay five cents for an article or face an array of banner and pop-up ads? Brave has not yet displaced the dominant browsers, but it is making inroads and is possibly steering the market in a new direction.

In the fall of 2018, the venture firm Andreessen Horowitz announced major funding for a company called Very Good Security (VGS).[14] The name is a takeoff on the encryption software known as Pretty Good Privacy (PGP), which has been around since the early 1990s. VGS asks why we use our Social Security numbers, names, addresses, credit card numbers, and other similar identifiers across the whole range of life's transactions. This common practice is just one way among many that our systems seem to have been designed to fail.

VGS's solution is to mediate—and anonymize—all these transactions, authorizations, and authentications so that our personal information is not stored and transmitted along the daisy chain of hospitals, retailers, online stores, and other points of sale, including all their vendors and vendors' vendors. Using advanced cryptography and segregated storage systems, VGS hopes to act as a turnkey privacy and security solution for businesses large and small. Alex Rampell of Andreessen Horowitz described the solution:

> Did you ever wonder why doctor offices ask for your social security number?
>
> They don't want to keep your SSN, but it's the primary "key" that identifies you to an insurance company. In computer science/math terms, they need to call a function. Let's call it: int reimbursement(char * ssn)
>
> When they plug your SSN into said function it returns a result (success, failure, more information needed, etc). Why does a lending company ask for your social? Same thing, but to look up your credit report. Why does Netflix need your credit card number? Same thing, but to get money from your bank. The problem is that these "keys" never change, are presented in the clear (your SSN never changes and you always write it down!), and function as a sort of bearer instrument—if you have the key, you can make a purchase, apply for a loan, etc.
>
> It turns out none of these companies want to store this "confidential" and sensitive data (SSNs, credit cards, etc). They just want to perform operations on them.
>
> Enter Very Good Security, aka VGS. (Cryptography people might recognize the name as a play on PGP, aka Pretty Good Privacy.) What VGS does is effectively redact and tokenize structured sensitive data—think credit cards, social security numbers, etc—returning a hashed form to the requestor. So instead of a doctor's office storing your social, they might store a random string of letters returned to them by VGS (that is called the "tokenized" version, because it maps to the real version stored by VGS, and is not the same even across different VGS customers). When it's time to bill your insurance company, their "reimbursement" code goes through VGS which "reveals" the token and sends the real version to the insurance company. VGS functions as a proxy server that scrambles/unscrambles sensitive information in real time.[15]

In other words, increasingly we will deploy new technologies to combat the downsides of the digital world and cleanse data pollution. VGS happens to be a centralized solution.

But in the future, blockchains and crypto assets, for example, will be used to verify identities and transactions without creating massive, centralized repositories of data, which can create attractive targets for malicious actors and concentrated risk for human error. Blockchains can, in other words, provide *decentralized* trust. But they are just one example of the phenomenon in which we develop new technologies to solve technology problems. What is the solution to technology failures? In many cases, more technology.

A central danger in any new privacy and security legislation and regulation is that we could discourage the use of information. Consider the analogy with free speech. Usually, the best solution to the problem of incorrect or obnoxious speech is not to ban said speech but to promote more speech. Truth and reason act as an error-correcting code. Similarly, the solution to the misuse of information will often be more information.

Consider the health privacy startup Verifyr, which collects and analyzes data on the use of a health provider's data. In health, we cannot abide unauthorized users accessing our data, and yet internal, unauthorized human access is a huge and growing problem. At the same time, we desperately need some physicians and nurses to access our information, with immediacy and precision. How we manage this bipolarity is a central challenge across the privacy spectrum.

By monitoring and processing the data about the data, Verifyr thinks it has developed a more flexible and powerful solution. Instead of a top-down, command-and-control regime, which rigidly prohibits behavior, it creates a bottom-up environment, which flexibly incentivizes good behavior.[16] This is the type of organic, unbureaucratic solution that may help us succeed in the nuanced, delicate world of privacy. In this way, we will refine information with information.

When technology alone cannot solve these problems, we will develop new institutions to help consumers understand and control their options and firms live up to expectations. Consumers cannot be expected to read hundreds of different 30-page Terms of Service and Privacy Policy documents. So we will develop privacy and security ratings, seals of approval, consumer reports, secondary markets, and other codes that compress the information firms provide (and their historical performance) into an easily digestible form.

The heterogeneity of data, consumers, and service providers—and the complexity of the relationships among them—will require new, creative associations to protect privacy while promoting data flows. Depending on the context, data might be considered a private good, club good, commons good, public good, or even some overlapping combination. Elinor Ostrom, the Nobel Prize–winning economist, showed how private and quasi-private institutions often emerge to bolster market incentives, competition, and cooperation in such complicated and nuanced spheres.[17] Privacy, where strict "private property" is often not the proper conceptual guide, is an arena where these ideas might be successfully applied.

When technology alone cannot solve these problems, we will develop new institutions to help consumers understand and control their options and firms live up to expectations.

Some critics, acknowledging the efficacy of "Ostrom organizations" for narrow applications, assert that Ostrom does not scale. We cannot count on a single Ostrom-like arrangement to provide an all-encompassing solution to data privacy governance. But this is not the suggestion; critics miss the point. Instead, many Ostrom organizations will emerge to govern and guide a multitude of data practices across applications and industries. Varied data categories, markets, and economic sectors will need varied levels of privacy and flow, shareability and sensitivity, and, depending on their place in the rivalry-excludability (private-club-commons-public) matrix, they will require distinct cooperative arrangements. These Ostrom organizations will serve as foundations that can both protect consumers and propel innovation.

In March 2019, Marsh & McLennan announced that it and a dozen of the world's largest insurers are collaborating on a ratings service for the cybersecurity industry.[18] The goal is to encourage best practices to avoid "data breach, business interruption, data corruption and cyber extortion."[19] This is a modern version of institutions that have sprung up to mitigate risks for new technologies and social phenomena of the past. As the *Wall Street Journal* notes,

> Such collaboration across the insurance industry is unusual but not unprecedented. In the 1950s, three insurance associations teamed to create the Insurance Institute for Highway Safety, a nonprofit organization dedicated

to reducing deaths, injuries and property damage from motor-vehicle crashes.[20]

Social norms, too, will evolve as we decide what behaviors are acceptable on social media and across the digital world. The ability of Facebook and Twitter to connect us has been powerful and in many ways magical. But it was also sudden and incendiary. There seems to be a mismatch between hyper-scale information networks and hyper-diverse social networks.[21]

Society was in many ways not ready for social media. Sharing some personal information is a deep part of the human experience. But so is keeping other personal information private. Social media supercharged our ability to share, with many benefits, but the new platforms (and their users) lacked many of the nuanced behavioral tools, strategies, and mores that humans had developed over millennia.

Ultimately, societal and economic trust will also depend on the government's trustworthiness. For many good reasons, the US government owns the world's most powerful surveillance tools. But if it does not live up to the Constitution and the spirit of the rules it imposes on its people, trust will erode.

Although beyond the scope of this report, there is reason to believe the US government may have, over the past decade, engaged in serious abuse of its surveillance tools.[22] New safeguards will be necessary to restore public confidence. Accountability for these breaches of trust will be needed (1) to bolster the credibility of any new rules the government imposes on others and (2) to make possible the continued use of these tools for legitimate purposes of national security.

Conclusion

We need new mediating institutions and behavioral updating to mitigate the worst effects of hyper-connected immediacy. The technology platforms can provide many of the tools to help. New market mechanisms and associations will emerge to balance competing interests. Government can help by setting a good example and updating its guidelines. But much of the work will fall to parents, schools, and individuals, who can steer each other toward higher standards of behavior, in the way we treat others and ourselves.

A new national law can provide the foundation on which we can build new norms, institutions, and technologies, which will do most of the work of protecting privacy while bolstering innovation.

About the Author

Bret Swanson is a visiting fellow at the American Enterprise Institute, where he focuses on emerging technologies and their impact on the US economy. He is concurrently president of the technology research firm Entropy Economics LLC and a fellow at the US Chamber of Commerce Foundation.

Notes

1. See Cisco, *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*, 2018, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html; and Cisco, *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*, 2018, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html.
2. See, for example, Michael Mandel and Bret Swanson, *The Coming Productivity Boom: Transforming the Physical Economy with Information*, Technology CEO Council, March 2017, http://entropyeconomics.com/wp-content/uploads/2017/03/The-Coming-Productivity-Boom-Transforming-the-Physical-Economy-with-Information-March-2017.pdf.
3. See, for example, Maryaline Catillon, David M. Cutler, and Thomas E. Getzen, "Two Hundred Years of Health and Medical Care," Vox CEPR Policy Portal, February 9, 2019, https://voxeu.org/article/two-hundred-years-health-and-medical-care.
4. See, for example, Bret Swanson, "The App-ification of Medicine: A Four-Faceted Information Revolution in Health," US Chamber of Commerce Foundation, September 2015, http://entropyeconomics.com/wp-content/uploads/2016/01/EE-The-App-ification-of-Medicine-2.0-09.15.pdf.
5. Jim Relles, "The New California Privacy Law Will Hurt Sacramento Small Businesses," *Sacramento Business Journal*, February 28, 2019, https://www.bizjournals.com/sacramento/news/2019/02/28/another-voice-the-new-california-privacy-law-will.amp.html.

6. See Eric Goldman, "Recap of the California Assembly Hearing on the California Consumer Privacy Act," Technology & Marketing Law Blog, February 19, 2019, https://blog.ericgoldman.org/archives/2019/02/recap-of-the-california-assembly-hearing-on-the-california-consumer-privacy-act.htm.

7. The 2014 breaches of the Office of Personnel Management are examples of the US government's failure to secure its own data. The recent US indictment of two Chinese military hackers for major breaches of numerous managed cloud service providers is an example of sophisticated private firms being victimized by even more sophisticated foreign state actors. See US Department of Justice, December 17, 2018, https://www.justice.gov/opa/press-release/file/1121706/download.

8. Maureen K. Ohlhausen, "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases," Federal Trade Commission, September 19, 2017, https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

9. See Cobun Keegan and Calli Schroeder, "Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms," *Journal of Law, Economics & Policy* 15, no. 1 (Winter 2018): 19–40, http://jlep.net/home/wp-content/uploads/2019/01/JLEP-Volume-15-1.pdf.

10. Google Chief Economist Hal Varian identified most of the conceptual and economic issues involved with digital privacy back in 1996. In a recent article, Joseph J. Cordes and Daniel R. Pérez examined current efforts to measure the costs and prices of privacy, through such metrics as "willingness to pay." Joseph J. Cordes and Daniel R. Pérez, "Measuring Costs and Benefits of Privacy Controls: Conceptual Issues and Empirical Estimates," *Journal of Law, Economics & Policy* 15, no. 1 (Winter 2018): 1–18, http://jlep.net/home/wp-content/uploads/2019/01/JLEP-Volume-15-1.pdf.

11. Greg Bensinger, "Google Vows Greater User Privacy, After Decades of Data Collection," *Washington Post*, May 7, 2019, https://www.washingtonpost.com/technology/2019/05/07/google-vows-greater-user-privacy-after-decades-data-collection/.

12. See Joseph Marks, "The Cybersecurity 202: These Are the Four Parts of the Economy Most Vulnerable to Cyberattack, According to Moody's," *Washington Post*, February 28, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/28/the-cybersecurity-202-these-are-the-four-parts-of-the-economy-most-vulnerable-to-cyberattack-according-to-moody-s/5c76d8001b326b2d177d5f79/.

13. See Federal Trade Commission, "FTC Hearing #6: Privacy, Big Data, and Competition," Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century, November 6–8, 2018, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-6-competition-consumer-protection-21st-century.

14. See Bret Swanson, "The Business of Digital Privacy and Security Will Be Huge," AEIdeas, September 4, 2018, https://www.aei.org/publication/the-business-of-digital-privacy-and-security-will-be-huge/. These paragraphs were adopted directly from the cited blog item.

15. Alex Rampell, "Very Good Security," Andreessen Horowitz, August 28, 2018, https://a16z.com/2018/08/28/very-good-security/.

16. For a good example of a top-down, command-and-control regime in health information, look no further than the federal electronic health records debacle. See, for example, Fred Schulte and Erika Fry, "Death by 1,000 Clicks: Where Electronic Health Records Went Wrong," Keiser Health Network, March 18, 2019, https://khn.org/news/death-by-a-thousand-clicks/.

17. See, for example, Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (New York: Cambridge University Press, 1990); Elinor Ostrom, "A Behavioral Approach to the Rational Choice Theory of Collective Action," *American Political Science Review* 92, no. 1 (March 1998): 1–22, https://www.jstor.org/stable/2585925?seq=1#metadata_info_tab_contents; and Elinor Ostrom, *Understanding Institutional Diversity* (Princeton: Princeton University Press, 2009).

18. See Leslie Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry," *Wall Street Journal*, March 26, 2019, https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600.

19. Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry."

20. Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry."

21. See Bret Swanson, "Big Tech and the Science of Social Scaling," AEIdeas, March 27, 2019, https://www.aei.org/publication/big-tech-and-the-science-of-social-scaling/.

22. One authoritative source for these concerns is a 99-page opinion written in April 2017 by Rosemary M. Collyer, chief judge of the Foreign Intelligence Surveillance Court. The opinion found serious and widespread abuse of the government's Section 702–based capabilities, where private contractors working with the FBI or CIA improperly and continually accessed raw data on US citizens. Although heavily redacted, her report found that between 2012 and 2016, "improper access granted to" private contractors "seems to have been the result of deliberate decisionmaking." Foreign Intelligence Surveillance Court, "Memorandum Opinion and Order," April 26, 2017, https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.