MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

THE BENEFITS, CHALLENGES, AND POTENTIAL ROLES FOR THE GOVERNMENT IN FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

ADAM THIERER
Senior Research Fellow, Mercatus Center at George Mason University

Agency: National Telecommunications Information Administration, Department of Commerce
Proposed: April 5, 2016
Comment period closes: June 2, 2016
Submitted: June 1, 2016
Docket ID: 160331306–6306–01

My name is Adam Thierer, and I am a senior research fellow at the Mercatus Center at George Mason University, where I study technology policy. Along with other Mercatus Center scholars, I have conducted extensive research on the questions raised in the NTIA's Internet of Things (IoT) proceeding.

Accordingly, I am pleased to submit for the record two recently published Mercatus Center articles. The first article is a compendium of statistics on the economic impact of the IoT and wearables that I coauthored with Andrea Castillo.[1] The second is a law review article I authored for the *Richmond Journal of Law and Technology* last year.[2]

---

1. Adam Thierer and Andrea Castillo, "Projecting the Growth and Economic Impact of the Internet of Things," Economic Perspectives, Mercatus Center at George Mason University, June 15, 2015, http://mercatus.org/publication/projecting-growth-and-economic-impact-internet-things.
2. Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation," *Richmond Journal of Law and Technology* 21, no. 6 (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494382.

For more information, contact
Taylor Barkley, Assistant Director of Outreach for Technology Policy
703-993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor, Arlington, VA 22201

There are two key takeaways from these publications. First, by every measure, the economic benefits associated with IoT adoption will be enormous. Estimates of the total global impact of IoT technologies range from $2.7 trillion to $14.4 trillion in new economic value by 2025.

Second, those amazing benefits will only come about if America gets public policy right for this exciting new set of technologies. The Internet revolution was powered by "permissionless innovation"—the idea that experimentation with new technologies and business models should generally be permitted without prior approval. By embracing the same vision for IoT, the United States can incentivize IoT innovation and also make it more likely that the next generation of tech entrepreneurs launch those devices and services domestically.

The Mercatus Center has also recently published a book[3] and paper[4] that present a blueprint for how to make permissionless innovation the foundation of tech policy going forward, including for the Internet of Things and "smart" technologies. We hope these publications will be of assistance as the NTIA studies these important issues.

3. Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2016), http://mercatus.org/permissionless/permissionlessinnovation.html.
4. Adam Thierer, "Permissionless Innovation and Public Policy: A 10-Point Blueprint," Mercatus Center, April 8, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2761139.

MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

ECONOMIC PERSPECTIVES

PROJECTING THE GROWTH AND ECONOMIC IMPACT OF THE INTERNET OF THINGS

Adam Thierer and Andrea Castillo

The next big wave of data-driven technological innovation will connect physical devices embedded with tiny computing devices to the Internet in an effort to seamlessly improve the measurements, communications, flexibility, and customization of our daily needs and activities. This "Internet of Things" (IoT) is already growing at a breakneck pace and is expected to continue to accelerate rapidly.

Adam Thierer of the Mercatus Center at George Mason University writes in a 2015 journal article that as is the case with any emerging technology, some groups have already started petitioning policymakers to limit or control IoT technologies out of fears of poor privacy or security outcomes. Policymakers are already investigating these issues. The Senate Committee on Commerce, Science, and Transportation recently held a hearing related to these issues, and in January the Federal Trade Commission (FTC) released a major report recommending a variety of privacy and security "best practices" for IoT. While some of these concerns are understandable, as Thierer writes in his 2014 book *Permissionless Innovation*, good public policy requires an appropriately weighted consideration of the projected benefits of any new development alongside the costs of regulatory interventions aimed at preemptively addressing perceived (and in some cases entirely hypothetical) fears.

In a testimony before the Senate Committee on Commerce, Science, and Transportation, Thierer highlighted that industry research groups have published several recent analyses that project the economic and social benefits of IoT technologies. While the methodologies, specific technologies analyzed, and final figures among these studies vary, they all indicate an industry consensus that the coming decades will be characterized by the introduction of billions of "smart" devices, millions of job opportunities, and trillions of dollars in economic growth and cost savings. The total number of connected devices in use globally—including such items as smart home appliances, "wearables," smart metering systems, and autonomous vehicles—is projected to grow from 10 billion in 2013 to anywhere from 19 billion to 40 billion

by 2019. The cost savings and productivity gains generated through "smart" device monitoring and adaptation are projected to create $1.1 trillion to $2.5 trillion in value in the health care sector, $2.3 trillion to $11.6 trillion in global manufacturing, and $500 billion to $757 billion in municipal energy and service provision over the next decade. The total global impact of IoT technologies could generate anywhere from $2.7 trillion to $14.4 trillion in value by 2025.

This summary provides a brief explanation of IoT technologies before describing the current projections of the economic and technological impacts that IoT could have on society. In addition to creating massive gains for consumers, IoT is projected to provide dramatic improvements in manufacturing, health care, energy, transportation, retail services, government, and general economic growth. Poorly considered policies should not prevent us from reaping these enormous benefits.

WHAT IS THE INTERNET OF THINGS?

IoT, sometimes called "machine-to-machine" (M2M) communication technologies, is a series of networked "smart devices" that are equipped with microchips, sensors, and wireless communications capabilities. The underlying drivers of the Internet revolution—massive increases in processing power, storage capacity, and networking capabilities; the miniaturization of chips and cameras; and the digitization of data and assembly of "big data" repositories—have dramatically lowered the costs of integrating microchips, sensors, cameras, and accelerometers into everyday devices. Existing technologies and tools can be cheaply integrated with the Internet to engage with external information and react according to preprogrammed commands. The major categories of IoT technologies include "smart" consumer technologies, wearables, "smart" manufacturing and infrastructure technologies, and unmanned transportation.

"Smart" Consumer Technologies

Consumer products will be designed with sensors and wireless capabilities to dynamically automate routine tasks. Mundane appliances that consumers have long taken for granted—like refrigerators, cooking devices, lights, and even weight scales—all will soon be networked, sensing, automated, and communicating as "smart" home technologies. Refrigerators are being designed to measure and record internal temperatures, monitor for bacteria or spoilage, and even keep track of food stocks to alert owners when supplies are running low—or just order a new delivery directly from the nearest grocery store's website. Thermostats can already learn and adjust to household behavior and program themselves to save money on heating and cooling bills. Networked consumer products are expected to provide dramatic economic benefits by lowering the costs of household drudgery through automation, freeing up time for more productive activities, and extending the use and life of household goods by improving maintenance.

Wearables

Wearables are a subset of consumer technologies that integrate networked devices into portable accessories like watches, jewelry, clothes, and glasses to collect data, track activities, and customize experiences to users' needs and desires. Wearable technologies are among the fastest-growing segment of the IoT and promise to have widespread societal influences in the coming years, particularly in the areas of personal safety and security, health, wellness, fitness, personal organization, communication, and fashion. Popular examples of wearables include fitness tracking and feedback products like Jawbone and FitBit that allow individuals to continuously measure and share daily fitness activities to isolate and improve their outcomes. Sophisticated wearable health devices will soon remind users to take medications or contact medical professionals as necessary and eventually help users track and even diagnose various conditions before advising a course of action. Other experiments with implantable "hearable" devices, "smart" contact lenses and glasses, and even tactile networked patches and fabrics seek to cheaply and seamlessly monitor other health vitals like blood glucose levels, blood pressure, brain activity, and stress. Dr. Eric Topol explains in his book *The Creative Destruction of Medicine* that these and other advances will improve preventative medicine and save billions of dollars in health care costs.

"Smart" Manufacturing and Infrastructure Technologies

While flashy IoT applications to consumer technologies understandably generate the most media buzz, networked devices perhaps hold the most promise to cut costs and raise efficiency in production, manufacturing, and even traditional municipal waste services.

In this age of "Industry 4.0," factory managers will create networks of connected production facilities along entire value chains that can autonomously communicate with each other and direct changes in response to unexpected developments. Devices will provide constant, accurate measurements of output, resource depletion, and capital depreciation to isolate sources of waste and maximize factor productivity. Smart infrastructure technologies can allow government planners to measure and monitor traffic management, waste and water services, and even police services to lower costs and improve services for citizens. The dramatic improvements to marginal production and cost reduction in manufacturing wrought by IoT technologies are projected to generate billions in revenue growth and productivity over the next decade.

Intelligent Vehicles and Unmanned Transportation

Adam Thierer and Ryan Hagemann of the Mercatus Center at George Mason University predict that networked vehicles and aircraft equipped with sensors, wireless communication, and dynamic programming will make unmanned transportation widely available and generate considerable benefits for consumers and manufacturing. "Autonomous vehicles" or "driverless cars" are automotive technologies that permit automobiles to operate without human assistance. Driverless cars are expected to dramatically reduce the number and costs of highway deaths and injuries while lowering the costs of shipping and transportation. Autonomous

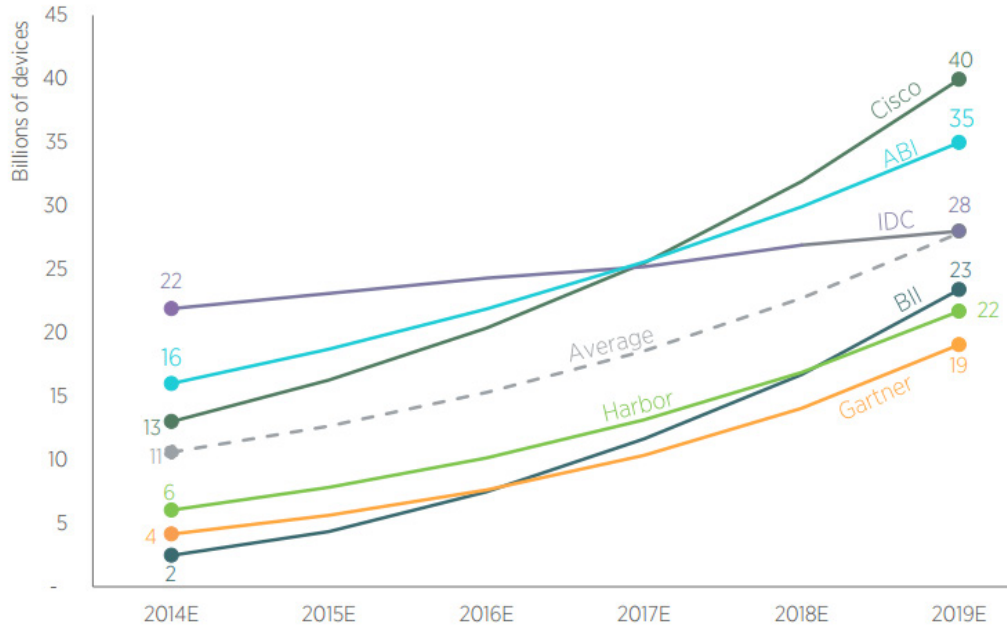
vehicles can also be used in manufacturing and warehouse capacities to improve speed and efficiency while lowering human injury and costs. Even short of fully autonomous systems, more "intelligent vehicle" technologies could produce significant social and economic benefits. On-board vehicle technologies are already an integral part of the expanding IoT universe. Experts at *Ars Technica* predict that "the automobile could be the first great wearable computer" and "your car might be the second most–used computing device you own before too long."

Jerry Brito, Eli Dourado, and Adam Thierer of the Mercatus Center at George Mason University explain that "Unmanned aerial vehicles" (UAVs) or "Unmanned Aircraft Systems" (UASs), informally known as "drones," employ similar networked concepts to automate aerial operations. UAVs will provide enormous productivity gains and cost savings in agricultural output, product delivery, and journalism and data gathering, as well as providing another exciting outlet as a good old-fashioned consumer hobby.

PROJECTED TECHNOLOGICAL ADVANCEMENTS

Industry analyses of market trends anticipate robust growth in the total number of networked devices in use over the next decades. An estimated 10 billion wirelessly connected devices were already in use globally in 2013, according to ABI Research analysts. Similar research from other organizations provides a wide range of estimates of the total number of IoT devices anticipated to be in operation by 2019, from a low of 19 billion to an optimistic projection of 40 billion devices. These and other projections are discussed in more detail below.

Figure 1. Industry Estimates of Total Internet of Things–Connected Devices by 2019



Source: John Greenough, "The Internet of Things is Rising: How the IoT Market Will Grow Across Sectors," *Business Insider Intelligence*, October 8, 2014. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

Cisco projects that 40 billion intelligent things will be connected and communicating by 2019.

ABI Research estimates that more than 35 billion networked devices will be in use by 2019.

International Data Corporation (IDC) predicts that around 28 billion networked devices will be in use by 2012 and that 212 billion devices will be connectable by 2020, 15 percent (around 31.8 billion) of which will be installed and operational by the end of 2020.

Gartner anticipates that 19 billion IoT devices will be in operation by 2019 and 25 billion devices will be online by 2020.

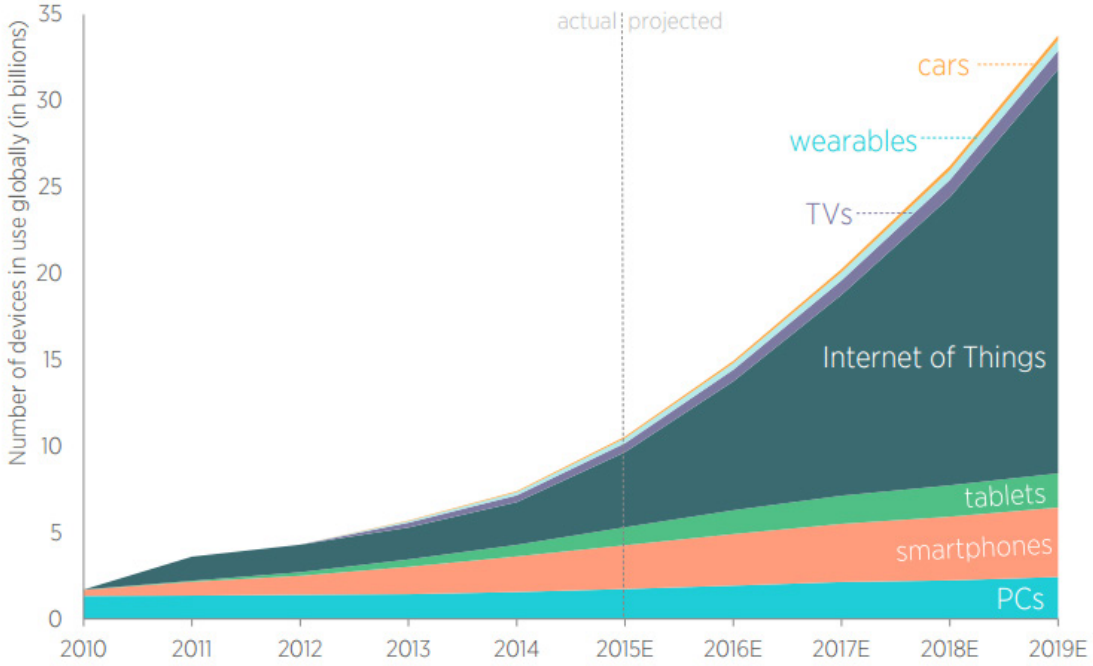
Harbor projects that 21.7 billion IoT devices will be connected and in use by 2019.

Machina Research reports that roughly 7.2 billion "machine-to-machine connected consumer electronic devices" will be in global use by 2023.

Business Insider Intelligence (BII) estimates that will be a total of 23.4 billion IoT devices connected by 2019 and that adoption will be driven by enterprise and manufacturing sectors.

Several analyses attempt to separate or isolate the total numbers within specific categories of IoT devices that will be connected over the next decade. Business Insider Intelligence provides historical and projected data on the number of installed IoT devices compared with PCs, smartphones, and tablets along with "smart" TVs, wearables, and "smart" cars (which are counted separately from IoT) from 2010 to 2019, which are displayed on the chart below. Growth in the number of installed IoT technologies is projected to exceed that of personal computers a factor of ten over the next four years, increasing from roughly 4.3 billion in 2015 to 23.4 billion by the end of 2019. Business Insider Intelligence anticipates that businesses will account for most of the growth in IoT-connected devices, projecting that almost 10 billion devices will be used in enterprise applications. "Smart" home, security, and energy devices will be another major consumer market and are projected to constitute almost 2 million of the total connected devices by 2019.

Figure 2. The Internet of Everything: Devices in Use Globally



Source: John Greenough, "The Internet of Everything 2015," *Business Insider Intelligence*. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

Other studies focus on specific market segments.

Navigant Research predicts that more than 1 billion smart meters will be installed globally by 2022, up from 313 million in 2013.

ON World projects that roughly 100 million Internet-connected wireless lights will be in operation by 2020.

Business Insider Intelligence projects that the annual number of wearables shipped will grow from 14.04 million in 2013 to 162.8 million in 2020, and that a total of 730.58 million wearable devices will be shipped throughout those years. Smartwatches are projected to lead the market, with 503.1 million devices projected to be shipped from 2013 to 2019, followed by fitness bands and activity trackers, projected at 168.9 million devices shipped, while another 58.54 million devices are projected to be shipped from remaining wearables markets. However, these projections were revised downwards from earlier BII projections anticipating shipments of more than 300 million devices by 2018 owing to persistent barriers to adoption and underwhelming market performance.

IDC analysts report that the global wearables market reached a total of 19.2 million devices in 2014 and project that the worldwide market will swell to 111.9 million networked devices sold in 2018.

The International Federation of Robotics reports that 806,000 connected industrial robots have been installed in manufacturing and shipping facilities and projects that roughly 2.6 million will be in operation by 2020.

The Teal Group estimates that the global civilian aerial drone market, worth roughly $10 million in 2013, will grow by over 2,000 percent to reach $2.2 billion in 2023.

IHS Automotive anticipates that the number of cars connected to the Internet will grow more than six fold from 2013 to reach 152 million internationally by 2020.

Industry projections present a vision of the future where billions of formerly dormant "things" actively sense, respond, and communicate with not only the people and environments but also other devices around them. The number of connected consumer devices—like wearables, TVs, and intelligent vehicles—will grow gradually but impressively. Smart appliances and climate control devices will become normal household objects in the coming decades. Networked manufacturing, production, and industrial delivery devices will largely drive the growth in the total number of IoT devices. We will now consider some of the economic benefits that will accompany these technological advancements.

PROJECTED ECONOMIC BENEFITS

The growth in the total number of IoT devices is projected to provide substantial economic and social benefits in the way of cost savings, value creation, productivity improvements, and general economic growth. Improved industrial monitoring and automation techniques will help manufacturers and distributors to quickly pinpoint inefficiencies, minimize waste, and streamline processes. Consumer health measurement technologies will help to promote preventative health practices and identify risk factors while emergency response communications can provide near-instant care in life-threatening situations. Hospitals can cut down on costs through accurate patient monitoring and pharmaceutical management. "Smart" city technologies can help municipalities to improve service delivery and save resources through infrastructure monitoring and automatic optimization. Recent analyses of IoT technologies project these and other savings and productivity gains in agriculture, security, energy, retail, and resource extraction will amount to trillions in value over the coming decades.

McKinsey Global Institute researchers estimate the potential economic impact of IoT technologies to be $2.7 trillion to $6.2 trillion per year by 2025, the largest of which will be felt in the manufacturing and health care industries. By sector, IoT is projected to create each year:

- $1.1 trillion to $2.5 trillion in value in the health care sector
- $0.9 trillion to $2.3 trillion in value in manufacturing
- $200 billion to $500 billion in value in electricity provision

- $100 billion to $300 billion in value in urban infrastructure
- $100 billion to $200 billion in value in security provision
- $100 billion to $200 billion in value in resource extraction
- around $100 billion in value in agriculture
- around $50 billion in value in vehicle use

Cisco analysts estimate that IoT will create $14.4 trillion in net profit between 2013 and 2022, which amounts to an increase in global corporate profits by roughly 21 percent. By sector, the "Value at Stake" generated by IoT is projected to be:

- $1.95 trillion for manufacturing through "smart factory" techniques
- $1.95 trillion for marketing and sales through location-based mobile advertising
- $757 billion for municipalities through "smart grid" technologies
- $635 billion for entertainment through connected gaming and media
- $349 billion for infrastructure through "smart building" technologies
- $347 billion for transportation through connected ground vehicles
- $106 billion from health care through connected patient monitoring
- $78 billion for education through connected private colleges

General Electric projects that industrial IoT technologies could add about $15 trillion to global GDP by 2030 (in constant 2005 dollars) if they raise global annual productivity growth by 0.5 to 1 percentage points. Additionally, an estimated $32.3 trillion in total global output can benefit from "Industrial Internet" technologies by optimizing information flows. The report estimates that the Industrial Internet opportunities of these sectors by 2025 will be:

- $11.6 trillion in manufacturing
- $7 trillion in health care
- $4.8 trillion in transportation

IDC estimated in 2013 that IoT market would grow at a compound annual growth rate of 7.9 percent to reach $8.9 trillion by 2020.

Business Insider estimates that IoT will add approximately $5.6 trillion in value to the global economy in between 2014 and 2019, $2.4 trillion of which will accrue to enterprise industry, $1.7 trillion of which will accrue to government and municipal services, and $1.5 trillion of which will accrue to home consumption.

Accenture estimates that the industrial IoT could add $14.2 trillion to the global economy by 2030, and that the US economy will gain at least $6.1 trillion in cumulative GDP by that year. If the US takes additional measures to employ IoT to improve domestic infrastructure, then Accenture projects that the gains to the US will rise to $7.1 trillion over that same time. Another survey assembled by Accenture finds that 87 percent of the executives surveyed believe that IoT will result in long-term job growth.

VisionMobile projects that the number of IoT developers will grow from roughly 300,000 in 2014 to more than 4.5 million by 2020.

Morgan Stanley forecasts that driverless cars will save the US economy $1.3 trillion per year once they fully penetrate the market, while saving the world another $5.6 trillion a year. Specifically, they predict:

- $507 billion in productivity gains
- $488 billion in prevented accident costs
- $158 billion in fuel cost savings
- $138 billion in productivity gains from congestion prevention
- $11 billion in fuel cost savings from congestion prevention

This growing body of research indicates that IoT will not just provide marginal consumer benefits and technological intrigue—it will change the industrial paradigm of the 21st century and can jump-start global economic productivity gains for decades to come.

CONCLUSION

Recent projections of the economic and social benefits of networked IoT technologies suggest that their technological and economic impact will be significant. These analyses predict that tens or even hundreds of millions of networked devices will proliferate globally as industrial and infrastructure inputs, consumer wearables, smart home technologies, and automated transportation services. The economic gains in terms of cost savings and enhanced productivity growth are projected to be enormous. Trillions in value will be created through cost-savings through preventative health care, minimized accidents, patient monitoring, efficiencies in manufacturing and distribution, and seamless home and municipal infrastructure improvements.

These potentially large economic gains must be considered when policymakers are debating policy for IoT. It is always easy to conjure up hypothetical worst-case scenarios about how some of these technologies may be misused, or how they might disrupt certain sectors and professions. But, as Thierer writes, if public policy is based upon fear of worst-case scenarios, then best-case scenarios will never come about. As economic historian Joel Mokyr has observed, "technological progress requires above all tolerance toward the unfamiliar and the eccentric." More generally, long-term social progress and economic prosperity hinge upon a general willingness to engage in ongoing trial-and-error experimentation with new technologies like IoT.

Policymakers should carefully weigh the costs associated with any proposed IoT regulations against the enormous projected benefits: both in the short term and long term. Smart technologies require smart regulations.

CONTACT

Taylor Barkley, 703-993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor, Arlington, VA 22201
www.mercatus.org

ABOUT THE AUTHORS

Adam Thierer is a senior research fellow with the Technology Policy Program at the Mercatus Center at George Mason University. He specializes in technology, media, Internet, and free-speech policies, with a particular focus on online safety and digital privacy. His latest book is *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Thierer is a frequent guest lecturer, has testified numerous times on Capitol Hill, and has served on several distinguished online safety task forces, including Harvard University's Internet Safety Technical Task Force and the federal government's Online Safety Technology Working Group. He received his MA in international business management and trade theory at the University of Maryland.

Andrea Castillo is the program manager of the Technology Policy Program for the Mercatus Center at George Mason University and is pursuing a PhD in economics at George Mason University. She is a coauthor of Liberalism and Cronyism: Two Rival Political and Economic Systems with Randall G. Holcombe and Bitcoin: A Primer for Policymakers with Jerry Brito. Castillo received her BS in economics and political science from Florida State University.

ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org

THE INTERNET OF THINGS AND WEARABLE TECHNOLOGY: ADDRESSING PRIVACY AND SECURITY CONCERNS WITHOUT DERAILING INNOVATION

Adam D. Thierer*

Cite as: Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.

I. INTRODUCTION

[1] The next great wave of Internet-enabled innovation has arrived, and it is poised to revolutionize the way humans interact with the world around them. This paper highlights some of the opportunities presented by the rise of the so-called Internet of Things (IoT) in general and wearable technology in particular and encourages policymakers to allow these technologies to develop in a relatively unabated fashion.

[2] Wearable technologies are networked devices that can collect data, track activities, and customize experiences to users' needs and desires. These technologies are a subset of IoT, which comprises networked "smart devices" equipped with microchips, sensors, and wireless communications capabilities.[1] Wearable technologies are among the

* Senior Research Fellow, Mercatus Center at George Mason University. Portions of this paper have been adapted from Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (2014). The author thanks the following individuals for their helpful comments on various drafts of this paper: Robert Graboyes, Jerry Brito, Dan Caprio, Ryan Hagemann, Will Rinehart, Ryan Radia, and two anonymous reviewers.

[1] *See* Charles McLellan, *M2M and the Internet of Things: A Guide*, ZDNET (Jan. 10, 2013, 1:27 PM), http://www.zdnet.com/m2m-and-the-internet-of-things-7000008219, *archived at* http://perma.cc/XNK7-GJEY.

fastest-growing segment of IoT and promise to have widespread societal influences in the coming years.[2]

[3] As with other new and highly disruptive digital technologies, however, IoT and wearable technology will challenge existing social, economic, and legal norms. In particular, these technologies raise a variety of privacy and safety concerns. Other barriers exist that could hinder IoT and wearable technology—including disputes over technical standards, system interoperability, and access to adequate wireless spectrum to facilitate ubiquitous networking capabilities—but those issues will not be discussed in this paper.[3] Some wearable technologies will raise safety concerns, but those issues will be only briefly addressed. The focus of this paper will be on the privacy and security concerns that are already prompting calls for policy interventions.[4]

[4] Some of the privacy and security concerns about IoT and wearable technologies are legitimate and deserve responses. But those responses should not be top down or command and control in nature. Privacy and security are important values worthy of attention, but so too are

[2] *See, e.g.*, David Evans, *The Future of Wearable Technology: Smaller, Cheaper, Faster, and Truly Personal Computing*, LINKEDIN (Oct. 24, 2013), http://www.linkedin.com/today/post/article/20131024145405-122323-the-future-of-wearable-technology-smaller-cheaper-faster-and-truly-personal-computing, *archived at* http://perma.cc/GL2Y-9MMS (addressing various new wearable technologies and their likely impacts on society).

[3] *See, e.g.*, Bob Violino, *The Internet of Things Gets Real*, NETWORK WORLD (June 2, 2014, 6:00 AM), http://www.networkworld.com/news/2014/060214-internet-of-things-281935.html?hpg1=bn, *archived at* http://perma.cc/DC4S-YDEE (quoting Daniel Castro, Director of the Information Technology and Innovation Foundation's Center for Data Innovation in Washington, saying that "[a] big issue is standards and interoperability" and that "[b]uilding the IoT will require massive amounts of cooperation and coordination between firms.").

[4] *See, e.g.*, Amadou Diallo, *Do Smart Devices Need Regulation? FTC Examines Internet Of Things*, FORBES (Nov. 23, 2013, 9:01 AM), http://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/, *archived at* http://perma.cc/K772-7HSY.

innovation, entrepreneurialism, economic growth, price competition, and consumer choice. Regulation—especially regulation of fast-moving, rapidly evolving technologies—is likely to be premature and overly rigid and is unlikely to allow the many beneficial uses of these technologies.[5] Such constraints would be highly unfortunate because these technologies "will have profound implications for addressing important social and economic issues."[6]

[5] Therefore, generally speaking and barring clear evidence of direct risk to health or property—not merely hypothetical or ephemeral fears—policymakers should not impose prophylactic restrictions on the use of new wearable technologies and IoT. The default position toward these technologies should be "innovation allowed" or "permissionless innovation."[7] The burden of proof rests on those who favor precautionary regulation; they must explain why ongoing experimentation with IoT technologies should be prevented preemptively by force of law.[8]

[6] The better alternative to top-down regulation is to deal with concerns creatively as they develop, using a combination of educational

[5] *See* Daniel F. Spulber, *Unlocking Technology: Antitrust and Innovation*, 4 J. COMPETITION L. & ECON. 915, 965 (2008) ("Governments are notoriously inept at picking technology winners. Understanding technology requires extensive scientific and technical knowledge. Government agencies cannot expect to replicate or improve upon private sector knowledge. Technological innovation is uncertain by its very nature because it is based on scientific discoveries. The benefits of new technologies and the returns to commercial development also are uncertain.").

[6] Daniel Castro, *Internet of Things Meets Holiday Wish Lists*, INFORMATIONWEEK (Dec. 4, 2013, 10:56 AM), http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-meets-holiday-wish-lists/d/d-id/1112901, *archived at* http://perma.cc/TK89-SBKH.

[7] ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM ix (2014) [hereinafter PERMISSIONLESS INNOVATION].

[8] *See id.*

efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts), as needed.[9] This bottom-up and layered approach to dealing with problems will not preemptively suffocate technological experimentation and innovation in these spaces. This paper will conclude by outlining those solutions.

[7] Finally, and perhaps most importantly, societal and individual adaptation will play a role here, just as it has during so many other turbulent technological transformations. Although formidable privacy and security challenges are ahead, individuals and institutions will adjust in an evolutionary, resilient fashion, just as they adjusted to earlier disruptive technologies.

II. THE GROWTH OF THE INTERNET OF THINGS AND WEARABLE TECHNOLOGY: APPLICATIONS AND OPPORTUNITIES

A. The Internet of Things Arrives

[8] Many of the underlying drivers of the Internet and Information Age revolution—massive increases in processing power,[10] exploding storage capacity,[11] steady miniaturization of computing and cameras,[12]

[9] *See id.*

[10] *See* HAL ABELSON, KEN LEDEEN & HARRY LEWIS, BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 8–9 (2008) ("The rapid increase in processing power means that inventions move out of labs and into consumer goods very quickly.").

[11] *See, e.g.*, Sebastian Anthony, *How Big Is the Cloud?*, EXTREMETECH (May 23, 2012, 10:48 AM), http://www.extremetech.com/computing/129183-how-big-is-the-cloud, *archived at* http://perma.cc/645K-KCH5; Steve Lohr, *Data Explosion Lifts the Storage Market*, N.Y. TIMES (Sept. 9, 2011, 10:20 AM), http://bits.blogs.nytimes.com/2011/09/09/data-explosion-lifts-the-storage-market/?_r=0, *archived at* http://perma.cc/SS2K-FL72.

ubiquitous wireless communications and networking capabilities,[13] digitization of all data,[14] massive datasets (or "big data"[15])—are beginning to have a profound influence beyond the confines of cyberspace.[16] For example, it is cheaper than ever to integrate a microchip, a sensor, a camera, and even an accelerometer into devices today.[17] "Thanks to

[12] *See* Patrick Thibodeau, *Lens-less Camera, Costing Pennies, Brings Vision to the Internet of Things*, COMPUTERWORLD (Sept. 18, 2014, 12:25 PM), http://www.computerworld.com/article/2685246/lens-less-camera-costing-pennies-brings-vision-to-the-internet-of-things.html, *archived at* http://perma.cc/2VNP-XHK4; David G. Stork & Patrick R. Gill, *Lensless Ultra-Miniature CMOS Computational Imagers and Sensors*, RAMBUS LABS (unpublished manuscript), http://www.rambus.com/assets/documents/papers/StorkGillSensorComm.pdf, *archived at* http://perma.cc/MQA7-9C74 (last visited Dec. 3, 2014) (describing a new class of lensless, ultra-miniature computational imagers).

[13] *See* Darrell M. West, *The State of the Mobile Economy, 2014: Its Impact and Future*, CTR. FOR TECH. INNOVATION RESEARCH PAPER (Brookings Institution), Sept. 10, 2014, at 10, *available at* http://www.brookings.edu/research/papers/2014/09/10-state-mobile-economy-2014-west, *archived at* http://perma.cc/MEY3-Q394; *see also* CHRISTOPHER S. YOO, THE DYNAMIC INTERNET: HOW TECHNOLOGY, USERS, AND BUSINESS ARE TRANSFORMING THE NETWORK 48–54 (2012).

[14] *See* NICHOLAS NEGROPONTE, BEING DIGITAL 14–20 (1995); *see also* ABELSON ET AL., *supra* note 10, at 5–6.

[15] *See* Letter from Daniel Castro, Dir., Ctr. for Data Innovation, to Nicole Wong, Big Data Study, Office of Sci. and Tech. Policy (Mar. 31, 2014), *available at* http://www2.datainnovation.org/2014-ostp-big-data-cdi.pdf, *archived at* http://perma.cc/RJ8C-D4XC.

[16] *See e.g.*, Luke Dormehl, *Internet of Things: It's All Coming Together for a Tech Revolution*, GUARDIAN (June 7, 2014, 7:04 PM), *available at* http://www.theguardian.com/technology/2014/jun/08/internet-of-things-coming-together-tech-revolution, *archived at* http://perma.cc/T297-M3QR.

[17] *See* Bill Wasik, *Why Wearable Tech Will Be as Big as the Smartphone*, WIRED (Dec. 17, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/12/wearable-computers, *archived at* http://perma.cc/G92A-VKVM ("Thanks to what former *Wired* editor in chief Chris Anderson has called the 'peace dividend of the smartphone wars,' sensors and chip sets are cheaper now than ever, making it easier for small companies to incorporate sophisticated hardware into wearable devices." This means, Wasik explains, that "it has

advances in circuits and software," observe Neil Gershenfeld and J. P. Vasseur, "it is now possible to make a Web server that fits on (or in) a fingertip for $1."[18] As costs continue to fall[19] and these technologies are increasingly embedded into almost all devices that consumers own and come into contact with, a truly seamless web of connectivity and pervasive computing will exist.[20]

[9] As a result of these factors, mundane appliances and other machines and devices that consumers have long taken for granted—cars, refrigerators, cooking devices, lights, weight scales, watches, jewelry, eyeglasses, and even their clothing—all will soon be networked, sensing, automated, and communicating.[21] In other words, consumers are

become possible for tiny companies to dream up, build, and sell wearable devices in competition with big companies, a feat that was never possible with smartphones.").

[18] Neil Gershenfeld & J. P. Vasseur, *As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things*, FOREIGN AFFAIRS, Mar.–Apr. 2014 *available at* http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/as-objects-go-online, *archived at* http://perma.cc/2EMP-EXKL.

[19] DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 11 (2014) ("[N]ow it seems as if we're getting closer to the Internet of Things, primarily because the price of computation and connectivity has been reduced to almost nothing.").

[20] *See* DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 2 (Apr. 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, *archived at* http://perma.cc/D6AM-PTC9.

[21] *See, e.g.*, Glen Martin, *Wearable Intelligence: Establishing Protocols to Socialize Wearable Devices*, O'REILLY RADAR (Apr. 1, 2014), http://radar.oreilly.com/2014/04/wearable-intelligence.html, *archived at* http://perma.cc/264F-UA3E ("Intelligent devices other than phones and screens—smart headsets, glasses, watches, bracelets—are insinuating themselves into our daily lives. The technology for even less intrusive mechanisms, such as jewelry, buttons, and implants, exists and will ultimately find commercial applications."). A database of many current wearable technologies can be found at http://vandrico.com/database. *See also* Abigail Tracy, *How the Internet of Things Actually Works [Infographic]*, INC. (Mar. 25,

transitioning to what Alex Hawkinson, CEO and founder of SmartThings, calls a "programmable world" where "things will become intuitive [and] connectivity will extend even further, to the items we hold most dear, to those things that service the everyday needs of the members of the household, and beyond."[22]

[10] This so-called Internet of Things—or machine-to-machine connectivity and communications [23] —promises to usher in "a third computing revolution"[24] and bring about profound changes that will rival the first wave of Internet innovation.[25] The first use of the term "Internet of Things" is attributed to Kevin Ashton, who used it in the title of a 1999 presentation.[26] A decade later, he reflected on the term and its meaning:

2014), http://www.inc.com/abigail-tracy/inforgraphic-understand-the-internet-of-things.html, *archived at* http://perma.cc/UU2X-23DV.

[22] Alex Hawkinson, *What Happens When the World Wakes Up*, MEDIUM (Sept. 23, 2014), https://medium.com/@ahawkinson/what-happens-when-the-world-wakes-up-c73a5c931c17, *archived at* https://perma.cc/WY5Z-85X5.

[23] *See* John Naughton, *The Internet of Things: It's a Really Big Deal*, GUARDIAN (June 14, 2014, 7:05 PM), http://www.theguardian.com/technology/2014/jun/15/networker-internet-of-things-john-naughton-hacking, *archived at* http://perma.cc/8GXF-7Q4V.

[24] Timothy B. Lee, *Everything's Connected: How Tiny Computers Could Change the Way We Live*, VOX (Aug. 13, 2014), http://www.vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live, *archived at* http://perma.cc/EE2L-49QD.

[25] *See* Michael Mandel, *Can the Internet of Everything Bring Back the High-Growth Economy?*, PROGRESSIVE POL'Y INST., 2–3, 9 (Sept. 9, 2013), http://www.progressivepolicy.org/wp-content/uploads/2013/09/09.2013-Mandel_Can-the-Internet-of-Everything-Bring-Back-the-High-Growth-Economy-1.pdf, *archived at* http://perma.cc/4U4Y-46WA ("No one can predict the ultimate course of innovative technologies, but it appears that the Internet of Everything has the potential to help revive the high-growth economy.").

[26] Kevin Ashton, *That 'Internet of Things' Thing*, RFID JOURNAL (June 22, 2009), http://www.rfidjournal.com/articles/pdf?4986, *archived at* http://perma.cc/CS6G-9DYW.

> If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best.
>
> We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory. RFID [radio-frequency identification] and sensor technology enable computers to observe, identify, and understand the world—without the limitations of human-entered data.[27]

[11] More recently, analysts with Morrison Foerster have defined IoT as "the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings."[28] These low-power devices typically rely on sensor technologies[29] as well as

[27] *Id.*

[28] Amy Collins, Adam J. Fleisher, D. Reed Freeman Jr. & Alistair Maughan, *The Internet of Things Part 1: Brave New World*, MORRISON FOERSTER CLIENT ALERT, 1 (Mar. 18, 2014), http://www.jdsupra.com/legalnews/the-internet-of-things-part-1-brave-new-23154, *archived at* http://perma.cc/6G95-L8LU.

[29] *See, e.g.*, Shawn G. DuBravac, *A Hundred Billion Nodes*, *in* FIVE TECHNOLOGY TRENDS TO WATCH 2014 7 (2014), *available at* https://web.archive.org/web/20140703002255/http://content.ce.org/PDF/2014_5tech_web.pdf , *archived at* https://perma.cc/3ABK-YSGH ("The 'sensor'ization of technology creates a deluge of connected devices digitizing information in near real-time and providing this data in troves to anything they can . . . . There are already hundreds of ways sensors and computing partner with connectivity to create an Internet of Things. All of these systems can become a function of a series of data points captured from a wide swath of sensors. These systems become contextually aware and continuously updated as new information becomes available.") (accessed by searching for http://www.ce.org/i3/pages/Five-Tech-Trends-to-Watch in the Internet Archive Wayback Machine).

existing wireless networking systems and protocols (Wi-Fi, Bluetooth, near field communication, and GPS) to facilitate those objectives.[30] In turn, this reliance will fuel the creation of even more "big data."[31] Many of these technologies and capabilities will eventually operate in the background of consumers' lives and be almost invisible to them.[32]

[12] IoT is sometimes understood as being synonymous with "smart" systems: smart homes,[33] smart buildings,[34] smart appliances,[35] smart

[30] *See, e.g.*, Rahul Patel, *Where Is Wearable Tech Headed?*, GIGAOM (Sept. 28, 2013, 10:30 AM), http://gigaom.com/2013/09/28/where-is-wearable-tech-headed, *archived at* http://perma.cc/Y8MH-CWAX.

[31] Gil Allouche, *Big Data and the Internet of Things: A Powerful Combination*, SMARTDATA COLLECTIVE (June 4, 2014), http://smartdatacollective.com/gilallouche/202371/big-data-and-internet-things-powerful-combination, *archived at* http://perma.cc/TB69-88Q2 ("What happens, then, when you combine these two seemingly up and coming enigmas? You have an extremely powerful combination. Working together, big data and IoT have the potential to drastically change how things are done.").

[32] *See* DuBravac, *supra* note 29, at 8 ("For the foreseeable future, the Internet of Things will toggle between the visible and invisible world and eventually, a large portion of the Internet of Things will slip into invisibility. Using sensors to collect information digitally, and employing algorithms and computing to utilize this information, a device's ability to self-regulate will increasingly take place in the background.").

[33] *See* Mike Robuck, *Smart Home Survey: 'Internet of Things' Will Take Flight in Five Years*, CED (May 14, 2014, 12:41 PM), http://www.cedmagazine.com/news/2014/05/smart-home-survey-%E2%80%98internet-of-things%E2%80%99-will-take-flight-in-five-years, *archived at* http://perma.cc/FG74-9Q2D; Sarah Susanka, *Sarah Susanka Says the Home of the Future Will Be a Portal*, WALL ST. J. (July 8, 2014), *available at* http://online.wsj.com/articles/sarah-susanka-says-the-home-of-the-future-will-be-a-portal-1404764842, *archived at* http://perma.cc/Q5CW-VFHY ("We're hearing a lot of late about 'smart homes,' but like the Internet in 1995, it hasn't quite caught on yet. Watch out, though. This is one of the big shifts headed our way.").

[34] *See* Mellisa Tolentino, *Smart Building Projects to Boom in 2018*, SILICON ANGLE (Apr. 16, 2014), http://siliconangle.com/blog/2014/04/16/smart-building-projects-to-boom-in-2018, *archived at* http://perma.cc/CQS4-HWUP.

health,[36] smart mobility, smart cities,[37] and so on.[38] Smart car technology is also expanding rapidly.[39] Some experts even predict that "the automobile could be the first great wearable computer" and "your car might be the second most-used computing device you own before too long."[40] (Intelligent vehicle technology was the subject of another recent working paper published by the Mercatus Center at George Mason University.)[41] The systems undergirding IoT are still evolving rapidly with a variety of wireless technologies and protocols being used to connect these devices and let them communicate.[42] "In blending the

[35] *See* Yohana Desta, *Why You're Not Seeing More Smart Home Appliances*, MASHABLE (Apr. 26, 2014), http://mashable.com/2014/04/26/smart-home-appliances, *archived at* http://perma.cc/3GHB-5JHX.

[36] *See* James Temple, *The Race to Dominate Digital Health Heats Up*, RE/CODE (June 23, 2014, 5:00 AM), http://recode.net/2014/06/23/the-race-to-dominate-digital-health-heats-up, *archived at* http://perma.cc/2KMZ-EXGJ.

[37] *See* ANTHONY TOWNSEND, SMART CITIES: BIG DATA, CIVIC HACKERS, AND THE QUEST FOR A NEW UTOPIA 93–114 (2013).

[38] *See* THE INTERNET OF THINGS 2012: NEW HORIZONS 29–31 (Ian G. Smith ed., 2012), *available at* http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf, *archived at* http://perma.cc/XNZ2-JZC7.

[39] *See* Jonathan M. Gitlin, *The Past, Present, and Future of In-Car Infotainment*, ARS TECHNICA (June 3, 2014, 7:00 AM), http://arstechnica.com/gadgets/2014/06/the-past-present-and-future-of-in-car-infotainment, *archived at* http://perma.cc/D6UY-DU9Y.

[40] Jonathan M. Gitlin, *How Can Cars Keep up With Gadget Innovation?*, ARS TECHNICA (June 3, 2014, 7:00 AM), http://arstechnica.com/cars/2014/06/industries-collide-how-automakers-are-adapting-to-consumer-tech-life-cycles/, *archived at* http://perma.cc/8ZRN-XCEQ.

[41] *See* Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars* (Mercatus Working Paper, Sept. 17, 2014), forthcoming , WAKE FOREST J.L. & POL'Y (2015), *available at* http://mercatus.org/sites/default/files/Thierer-Intelligent-Vehicles.pdf, *archived at* http://perma.cc/R2GB-5KPY.

[42] *See* Patrick Thibodeau, *Explained: The ABCs of the Internet of Things*, COMPUTERWORLD (May 6, 2014, 7:30 AM),

physical and digital worlds, we essentially extend the original concept of hyperlinking to include physical objects," notes Shawn G. DuBravac, chief economist and senior director of research for the Consumer Electronics Association (CEA).[43] "The power of these devices, in essence, is their ability to sample information millions of times more often than we as people can," he says.[44]

[13] The promise of IoT, as described by *New York Times* reporter Steve Lohr, is that "[b]illions of digital devices, from smartphones to sensors in homes, cars, and machines of all kinds, will communicate with each other to automate tasks and make life better."[45] "Consumers and public officials can use the connected world to improve energy conservation, efficiency, productivity, public safety, health, education, and more," predicts CEA.[46] "The connected devices and applications that consumers choose to adopt will make their lives easier, safer, healthier, less expensive, and more productive."[47] In addition to giving consumers more control over their lives, these technologies can also help them free up time by automating routine tasks and chores.[48] In a new book on these

http://www.computerworld.com/s/article/9248058/Explained_The_ABCs_of_the_Internet_of_Things_, *archived at* http://perma.cc/KV5N-YJ9N.

[43] DuBravac, *supra* note 29, at 4.

[44] *Id.* at 6.

[45] Steve Lohr, *A Messenger for the Internet of Things*, N.Y. TIMES (Apr. 25, 2013, 12:15 AM), http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things, *archived at* http://perma.cc/649A-PQAY.

[46] Gary Shapiro & Laura Knapp Chadwick, *Comments of the CEA in re Privacy and Security Implications of the Internet of Things [to the FTC]* 7 (June 10, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00027-86193.pdf, *archived at* http://perma.cc/J2JZ-FRRQ.

[47] *Id.*

[48] *See* Daniel Castro, *Algorithms and Automation Will Give Us More Freedom and Control*, IDEAS LAB (July 8, 2014), http://www.datainnovation.org/2014/07/algorithms-and-automation-will-give-us-more-freedom-and-control/, *archived at*

technologies and their promise, David Rose of the Massachusetts Institute of Technology Media Lab describes an emerging world of "enchanted objects," which are objects that "start as ordinary things," but then are "augmented and enhanced through the use of emerging technologies—sensors, actuators, wireless connection, and embedded processing—so that it becomes extraordinary."[49] Through this transformation from ordinary to extraordinary, the newly enchanted object "evokes an emotional response from you and enhances your life," he argues.[50]

[14] This technological "enchantment" is already occurring at a breakneck pace. According to Cisco, by 2020, 37 billion intelligent things will be connected and communicating.[51] Thus, society is rapidly approaching the point where "[e]veryone and everything will be connected to the network."[52] ABI Research estimates that there are more than 10 billion wirelessly connected devices in the market today and more than 30 billion devices expected by 2020.[53] The Consultancy IDC (International

http://perma.cc/PBD3-NGTJ ("Because as more processes are put on autopilot, we will unyoke ourselves from routine tasks and enjoy the freedom to help those on the margins.").

[49] ROSE, *supra* note 19, at 47.

[50] *Id.*

[51] CISCO, THE INTERNET OF EVERYTHING AND THE CONNECTED ATHLETE: THIS CHANGES . . . EVERYTHING 2 (2013), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html, *archived at* http://perma.cc/CE79-96N3.

[52] INFSO D.4 NETWORKED ENTERPRISE & RFID INFSO G.2 MICRO & NANOSYSTEMS, INTERNET OF THINGS IN 2020: A ROADMAP FOR THE FUTURE 21 (2008), *available at* http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf, *archived at* http://perma.cc/L4U2-W5TA.

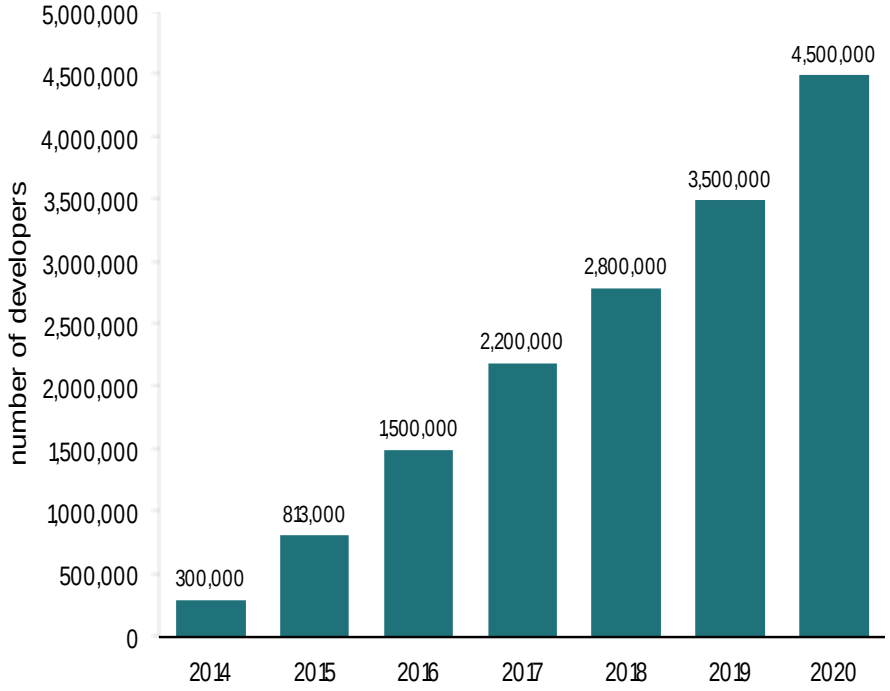
[53] *See, e.g.*, Press Release, ABI Research, More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020 (May 9, 2013), *available at* https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne, *archived at* https://perma.cc/CAT8-MK8G.

Data Corporation) predicts far greater penetration of 212 billion installed devices by that year.[54] VisionMobile projects that the number of IoT developers will grow from roughly 300,000 in 2014 to more than 4.5 million by 2020 (Figure 1).[55]

[54] *See, e.g.*, Jaikumar Vijayan, *The Internet of Things Likely to Drive an Upheaval for Security*, COMPUTERWORLD (May 2, 2014, 7:07 AM), http://www.computerworld.com/s/article/9248069/The_Internet_of_Things_likely_to_drive_an_upheaval_for_security, *archived at* http://perma.cc/BQW9-JQY7.

[55] *See, e.g.*, Matt Asay, *The Internet of Things Will Need Millions of Developers by 2020*, READWRITE (June 27, 2014), http://readwrite.com/2014/06/27/internet-of-things-developers-jobs-opportunity, *archived at* http://perma.cc/2888-DPSK.

Figure 1. Estimated Number of Internet of Things Developers, 2014–2020



Source: VisionMobile (June 2014).

[15] The benefits associated with these developments could be enormous.[56] McKinsey Global Institute researchers estimate the potential economic impact of IoT to be $2.7 trillion to $6.2 trillion per year by 2025,[57] and IDC estimates that this market will grow at a compound

[56] *See generally* Emily Adler, *The 'Internet of Things' Will Soon Be a Truly Huge Market, Dwarfing All Other Consumer Electronics Categories*, BUS. INSIDER (July 10, 2014, 7:50 AM), http://www.businessinsider.com/internet-of-things-will-soon-be-a-truly-huge-market-dwarfing-all-other-consumer-electronics-categories-2014-7, *archived at* http://perma.cc/3BM9-K78C.

[57] *See* JAMES MANYIKA ET AL., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 12 (McKinsey Global Institute

annual growth rate of 7.9% between now and 2020, to reach $8.9 trillion.[58] Cisco analysts estimate that IoT will create $14.4 trillion in value between 2013 and 2022.[59] Many other analysts and consultancies have predicted similar growth and economic impacts[60] and agree with Michael Mandel, chief economic strategist at the Progressive Policy Institute, who argues that the positive effects could reverberate throughout the economy.[61] Mandel believes that "[W]e are at the next stage of the Internet Revolution" and that "the Internet of Everything has the potential to help revive the high-growth economy."[62]

[16] The biggest impacts will likely be in health care, energy, transportation, and retail services.[63] But governments will benefit too. "Governments are deploying sensors to alert them to failed street lights, leaks in water systems, and full trash cans. Sensors will likely have a

May 2013), *available at* http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx, *archived at* http://perma.cc/3DU5-4LXH.

[58] *See* Antony Savvas, *Internet of Things Market Will Be Worth Almost $9 Trillion*, CNME (Oct. 6, 2013), http://www.cnmeonline.com/news/internet-of-things-market-will-be-worth-almost-9-trillion, *archived at* http://perma.cc/97B3-CJ7G.

[59] *See* JOSEPH BRADLEY ET AL., EMBRACING THE INTERNET OF EVERYTHING TO CAPTURE YOUR SHARE OF $14.4 TRILLION 1 (Cisco 2013), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf, *archived at* http://perma.cc/YMG7-RGE9.

[60] *See e.g.*, Gil Press, *Internet of Things by the Numbers: Market Estimates and Forecasts*, FORBES (Aug. 22, 2014, 1:17 PM), http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts, *archived at* http://perma.cc/QRD8-4VAJ.

[61] *See* Mandel, *supra* note 25, at 9.

[62] *Id.*

[63] *See, e.g.*, Thibodeau, *supra* note 42.

major role in traffic control, fighting forest fires, and landslide detection."[64]

[17] But that just scratches the surface of potential money-saving and life-saving applications for IoT technologies.[65] IoT technologies will produce benefits for firms and consumers.[66] Many of these benefits will come about only after data is collected and used for entirely new purposes.

[18] For firms, "IoT has great potential to generate new sources of revenue, improve efficiencies and allow businesses to both increase profits and cut costs."[67] IoT will have many important applications for traditional manufacturing industries as well.[68] General Electric coined the term *Industrial Internet* to explain how "[t]he advent of networked machines with embedded sensors and advanced analytics tools" could revolutionize industrial machinery in coming years.[69] This "the fourth industrial

[64] *Id.*

[65] *See* Daniel Castro & Travis Korte, *Data Innovation 101*, CENTER FOR DATA INNOVATION (Nov. 3, 2013), http://www.datainnovation.org/2013/11/data-innovation-101, *archived at* http://perma.cc/HS9R-LGBN.

[66] *See id.*

[67] Collins et al., *supra* note 28, at 3.

[68] *See* Steve Lohr, *The Internet Gets Physical*, N.Y. TIMES, Dec. 17, 2011 at SR1, *available at* http://www.nytimes.com/2011/12/18/sunday-review/the-internet-gets-physical.html, *archived at* http://perma.cc/9FMZ-HY4P.

[69] *What Is the Industrial Internet?*, GE SOFTWARE, https://www.gesoftware.com/industrial-internet, *archived at* https://perma.cc/TZD9-6HU4 (last visited Jan. 19, 2015).

revolution"[70] could result in improved efficiencies and significant cost savings.[71]

[19] For consumers, IoT technologies will offer a staggering array of new devices and service options that will make their lives and jobs easier.[72] That is especially the case with the subset of IoT technologies known as *wearables*, which will be discussed extensively throughout this paper.

B. The Expanding World of Wearables

[20] In its massive 2002 report titled *Converging Technologies for Improving Human Performance*, the U.S. National Science Foundation predicted that, within the next two decades, "[c]omfortable, wearable sensors and computers will enhance every person's awareness of his or her health condition, environment, chemical pollutants, potential hazards, and information of interest about local businesses, natural resources, and the like."[73] Thirteen years later, the future that the National Science Foundation predicted is starting to emerge.

---

[70] Chloe Green, *The Internet of Things Business Process Revolution*, INFO. AGE (Sept. 10, 2014), http://www.information-age.com/it-management/strategy-and-innovation/123458453/internet-things-business-process-revolution, *archived at* http://perma.cc/E7M4-D2EH.

[71] *See* Jon Bruner, *Defining the Industrial Internet*, O'REILLY RADAR (Jan. 11, 2013), http://radar.oreilly.com/2013/01/defining-the-industrial-internet.html, *archived at* http://perma.cc/2RZP-22LU.

[72] *See* DANIEL CASTRO & JORDAN MISRA, THE INTERNET OF THINGS 2 (Ctr. For Data Innovation Nov. 2013), *available at* http://www2.datainnovation.org/2013-internet-of-things.pdf, *archived at* http://perma.cc/4L6H-5XUZ.

[73] NAT'L SCI. FOUND., CONVERGING TECH. FOR IMPROVING HUMAN PERFORMANCE 4–5 (Mihail C. Roco & William Sims Bainbridge eds., 2003), *available at* http://www.wtec.org/ConvergingTechnologies/Report/NBIC_report.pdf, *archived at* http://perma.cc/E52K-3UDY.

[21] Although rudimentary wearable technologies—such as calculator wristwatches, hearing aids, and Bluetooth-enabled communications headsets—have been on the market for many years, this market is now expanding quite rapidly.[74] Even though "[w]earables are still looking for their killer app,"[75] health and fitness wearables are already widely used today.[76] Popular examples include the FitBit and Jawbone wearable fitness bracelets, which have been on the market for several years and command the bulk of market share.[77] The so-called quantified self movement refers to individuals who use such digital logging tools to continuously track their daily activity and well-being.[78] Many users share their data with others to compare results and provide "instant feedback,"[79]

[74] *See* Max Knoblauch, *The History of Wearable Tech, From the Casino to the Consumer*, MASHABLE (May 13, 2014), http://mashable.com/2014/05/13/wearable-technology-history, *archived at* http://perma.cc/HBM8-KSVG.

[75] Rachel Metz, *The Internet of You*, MIT TECH. REV. (May 20, 2014), http://www.technologyreview.com/news/527386/the-internet-of-you, *archived at* http://perma.cc/FV4T-YUPH.

[76] *See* Brian Bennett, *Wearable Tech Multiplies and Goes Mainstream at MWC 2014*, CNET (Feb. 27, 2014, 10:49 AM), http://reviews.cnet.com/8301-13970_7-57619658-78/wearable-tech-multiplies-and-goes-mainstream-at-mwc-2014, *archived at* http://perma.cc/LMK6-UJU5; *Health and Appiness*, ECONOMIST (Feb. 1, 2014), *available at* http://www.economist.com/news/business/21595461-those-pouring-money-health-related-mobile-gadgets-and-apps-believe-they-can-work, *archived at* http://perma.cc/ZLY2-YKA8.

[77] *See* Dara Kerr, *Fitbit Rules 50 Percent of the World's Wearable Market*, CNET (May 21, 2014, 6:31 PM), http://www.cnet.com/news/fitbit-rules-50-percent-of-the-worlds-wearable-market, *archived at* http://perma.cc/5Q4Y-AAMX.

[78] *See* Leandro Castelao, *The Quantified Self: Counting Every Moment*, ECONOMIST, Mar. 3, 2012, at Q1, *available at* http://www.economist.com/node/21548493, *archived at* http://perma.cc/822H-8CJ2; *see also* Deborah Lupton, *Understanding the Human Machine*, IEEE TECH. & SOC'Y MAG. (Dec. 9, 2013), at 25, *available at* https://www.academia.edu/5392119/Understanding_the_human_machine, *archived at* https://perma.cc/C7FA-EUCS.

[79] Katrina Plyler, *What Is Everybody Wearing? Fitness Tech Gadgets!*, U.S. NEWS (Apr. 11, 2014, 8:00 AM), http://health.usnews.com/health-news/blogs/eat-

for example, by notifying individuals about how many steps they have taken or buzzing (or even shocking them)[80] to remind them to be more active. Users of fitness bracelets often share results and compete for "step supremacy."[81]

[22] As they grow more sophisticated, wearable health devices will help users track, and even diagnose various conditions, and potentially advise a course of action or, more simply, remind users to take medications or contact medical professionals as necessary.[82] In the process, these health and fitness devices and applications could eventually become "lifestyle remotes" that help consumers control or automate many other systems around them, regardless of whether they are in their homes, offices, cars, or the like.[83] As a result, wearables will have even more uniquely personal properties and capabilities than the broader IoT, which will raise special privacy concerns discussed later in this paper.

[23] These wearable technologies are gaining more widespread public visibility and now even have their own product section on Amazon.com.[84]

---

run/2014/04/11/what-is-everybody-wearing-fitness-tech-gadgets?int=9a5208, *archived at* http://perma.cc/2TN8-ARGM.

[80] *See* James Trew, *Pavlok Is A Habit-Forming Wearable That Will Shock You*, ENGADGET (July 4, 2014, 10:40 AM), http://www.engadget.com/2014/07/04/pavlok-wearable, *archived at* http://perma.cc/MPW6-LP4B.

[81] Michael S. Rosenwald, *A New Washington Rat Race: Fitbit-Wearing Power Walkers Vie for Step Supremacy*, WASH. POST (Sept. 16, 2014), http://www.washingtonpost.com/local/a-new-washington-rat-race-fitbit-wearing-power-walkers-vie-for-step-supremacy/2014/09/16/63022b5c-39e9-11e4-9c9f-ebb47272e40e_story.html, *archived at* http://perma.cc/9ZZH-EEQX.

[82] *See* Nathan Olivarez-Giles, *WebMD Relaunches iPhone App as a Hub for Fitness Data*, WALL ST. J. (June 16, 2014, 1:22 AM), http://blogs.wsj.com/personal-technology/2014/06/16/webmd-relaunches-iphone-app-as-a-hub-for-fitness-data, *archived at* http://perma.cc/N2P9-4636.

[83] Metz, *supra* note 75; DuBravac, *supra* note 29, at 7–8.

According to the research firm Canalys, there was a 700% growth in the market for wearable smart bands in the second half of 2013 over the first half.[85] IDC reports that "wearables took a huge step forward over the past year and shipment volumes will exceed 19 million units in 2014, more than tripling last year's sales. From there, they predict that the global market will swell to 111.9 million units in 2018, resulting in a CAGR [compound annual growth rate] of 78.4%."[86] "Hearables", or small devices worn in the ear to provide users with relevant real-time information, are also expected to become a major part of the wearable market in coming years.[87] One wireless analyst estimates that such "smart earbuds" could constitute a $5 billion market by 2018.[88]

[84] *See* Hayley Tsukayama, *Wearable Tech Grows Enough to Get Its Own Section on Amazon*, WASH. POST (Apr. 29, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/29/wearable-tech-grows-enough-to-get-its-own-section-on-amazon, *archived at* http://perma.cc/Q56S-EXRH.

[85] *See, e.g.*, Matt Clinch, *Wearable Smart Bands Set for 350% Growth in 2014*, CNBC (Feb. 12, 2014, 8:34 AM), http://www.cnbc.com/id/101410507#, *archived at* http://perma.cc/LFY3-XA3Q.

[86] Press Release, Int'l Data Corp., Worldwide Wearable Computing Market Gains Momentum with Shipments Reaching 19.2 Million in 2014 and Climbing to Nearly 112 Million in 2018, Says IDC (Apr. 10, 2014), *available at* http://www.idc.com/getdoc.jsp?containerId=prUS24794914, *archived at* http://perma.cc/N6DS-4XHW.

[87] *See* Jessica Glazer, *Psst! Wearable Devices Could Make Big Tech Leaps, into Your Ear*, NPR (Apr. 29, 2014, 12:03 PM), http://www.npr.org/blogs/alltechconsidered/2014/04/23/306171641/psst-wearable-devices-could-make-big-tech-leaps-into-your-ear, *archived at* http://perma.cc/59X7-GEPN.

[88] *See* Rachel Feltman, *Hearables: The Next Big Thing in Wearable Tech May Be Ear Computers*, QUARTZ (Apr. 10, 2014), http://qz.com/196886/the-next-big-thing-in-wearable-tech-may-be-ear-computers/, *archived at* http://perma.cc/YTK4-G5LN.

[24] Major smartphone and tablet developers such as Apple[89] and Samsung[90] are also getting more active in this space, which will likely give these applications and services even greater visibility. Beyond their touch screens and wireless networking capabilities, modern smartphones include sensors, accelerometers, cameras, microphones, and other capabilities that can be used to collect and transmit various types of user information. At a summer 2014 conference for developers, Apple "unveiled plans to let people use their iPhones and iPads to control an array of Internet-connected devices in their homes, from door locks to lightbulbs."[91] Apple simultaneously launched "HealthKit," which will "help apps, third party devices and healthcare services collect, quantify, and share your health data . . . [and] could change the way you track and manage your well-being."[92] Google promptly responded with a competing service called Google Fit.[93]

[89] *See, e.g.*, *Apple's HealthKit Platform– Revolutionizing the Healthcare Industry*, BIDNESS ETC, http://www.bidnessetc.com/business/apples-healthkit-platform-revolutionizing-the-healthcare-industry, *archived at* http://perma.cc/N7NL-J4KT (last visited Jan. 19, 2015).

[90] *See, e.g.*, Stacey Higginbotham, *Samsung Launches a Wearable Wristband and Cloud Platform for Tracking Your Health*, GIGAOM (May 28, 2014, 11:16 AM), https://gigaom.com/2014/05/28/samsung-launches-a-wearable-and-cloud-platform-for-tracking-your-health, *archived at* https://perma.cc/AX5L-M87W; *see also Samsung Unwraps Tizen for 'Internet of Things*,' TAIPEI TIMES (June 5, 2014), *available at* http://www.taipeitimes.com/News/biz/archives/2014/06/05/2003592005, *archived at* http://perma.cc/9EDP-59DG.

[91] Erin Mershon, *Apple Dives into "Internet of Things,"* POLITICO (June 2, 2014, 6:01 PM), http://www.politico.com/story/2014/06/apple-wwdc-2014-internet-of-things-107336.html#ixzz33hMxZTIN, *archived at* http://perma.cc/5PQU-TBVY.

[92] Lance Ulanoff, *Inside HealthKit: Apple's Answer to the Quantified You*, MASHABLE (June 3, 2014), http://mashable.com/2014/06/03/inside-apple-healthkit, *archived at* http://perma.cc/8TCT-68NP.

[93] *See, e.g.*, Ben Gilbert, *Google Fit Is Android's Answer to Exercise and Health Tracking*, ENGADGET (June 25, 2014, 2:30 PM), http://www.engadget.com/2014/06/25/google-fit, *archived at* http://perma.cc/FJM6-K55X.

[25] Flurry Analytics has found that usage of health and fitness apps is up sixty-two percent in the past six months compared to thirty-three percent growth for the entire market of other applications, an eighty-seven percent faster pace.[94] The firm reports that there are more than 6,800 apps in the health and fitness category on the iPhone and iPad today.[95] Meanwhile, Samsung's newest phones can measure a user's heart rate and also feature extensive integration with fitness-tracking applications made by Samsung as well as other developers.[96]

[26] Microsoft also recently announced it would be "making home automation even easier for everyone, from the ultra-techie to the average homeowner" by integrating IoT technologies into tablets running Windows 8.1 as well as Windows Phone.[97] Microsoft is also developing a wearable band that will help blind people navigate their surroundings.[98] Also, Google, which earlier made a major splash in this space by developing Google Glass, recently announced it will develop a wearable-specific variant of its Android mobile operating system to optimize the

[94] *See* Kyle Russell, *Fitness App Usage Is Growing 87% Faster Than the Overall App Market*, TECH CRUNCH (June 19, 2014), http://techcrunch.com/2014/06/19/fitness-app-usage-is-growing-87-faster-than-the-overall-app-market, *archived at* http://perma.cc/WVG8-GZC7.

[95] *See id.*

[96] *See* Tom Warren, *Samsung's Free Galaxy S5 "Gifts" Focus on Fitness*, VERGE (Mar. 10, 2014, 6:40 AM), *available at* http://www.theverge.com/2014/3/10/5490078/free-samsung-galaxy-s5-apps-health-fitness, *archived at* http://perma.cc/7G6P-AFD4.

[97] Daniel Kline, *How Microsoft Will Incorporate the Internet of Things into Windows 8.1*, MOTLEY FOOL (May 20, 2014), http://www.fool.com/investing/general/2014/05/20/how-microsoft-will-incorporate-the-internet-of-thi.aspx, *archived at* http://perma.cc/DN93-EGVT.

[98] *See* Jack Schofield, *Microsoft's Wearable Alice Band Is Not a Rival to Google Glass*, ZDNET (July 14, 2014, 11:03 AM), http://www.zdnet.com/microsofts-wearable-alice-band-is-not-a-rival-to-google-glass-7000031563, *archived at* http://perma.cc/P4NN-KY89.

developer and user experience of devices of that size.[99] Google also recently patented "smart contact lenses" (otherwise known as *ophthalmic electrochemical sensors*) that will help diabetics more easily monitor their blood sugar levels and that could also lead to other wearable medical applications in the future.[100]

[27] Many current-generation wearables are clunky and unsightly, which probably has limited their adoption to some degree.[101] But "sensor-rich fabric"[102] and "conductive fiber" technologies are now proliferating, meaning that "fabric itself can now become an electronic device, allowing wearables to be incorporated into the most stylish clothing," as *The Economist* recently noted.[103] These conductive fibers are flexible and

[99] *See* Hayley Tsukayama, *Google Develops Android for Wearables You May Actually Want to Wear*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/18/google-develops-android-for-wearables-you-may-actually-want-to-wear, *archived at* http://perma.cc/TNU5-LGJL.

[100] *See, e.g.*, Kia Makarechi, *Move Over, Google Glass; Here Come Google Contact Lenses*, VANITY FAIR (Apr. 22, 2014, 10:48 AM), http://www.vanityfair.com/online/daily/2014/04/google-contact-lenses, *archived at* http://perma.cc/6NAL-CVZF; *see also* Lance Ulanoff, *Google Smart Contact Lenses Move Closer to Reality*, MASHABLE (Apr. 21, 2014), http://mashable.com/2014/04/21/google-smart-contact-lenses-patents, *archived at* http://perma.cc/KE3W-XFHB.

[101] *See* Connie Guglielmo & Parmy Olson, *The Case Against Wearables, or Why We Won't All Look Like the Borg This Year*, FORBES (Mar. 3, 2014), *available at* http://www.forbes.com/sites/connieguglielmo/2014/02/12/the-case-against-wearables, *archived at* http://perma.cc/H4F9-JFZ4; Nick Warnock, *Wearable Tech: Fashion Will Rule*, INFORMATIONWEEK (June 18, 2014, 9:06 AM), http://www.informationweek.com/strategic-cio/digital-business/wearable-tech-fashion-will-rule/a/d-id/1278629, *archived at* http://perma.cc/75V9-4NPL.

[102] Stacey Higginbotham, *You Call Google Glass Wearable Tech? Heapsylon Makes Sensor-Rich Fabric*, GIGAOM (May 16, 2013, 7:00 AM), http://gigaom.com/2013/05/16/you-call-google-glass-wearable-tech-heapsylon-makes-sensor-rich-fabric, *archived at* http://perma.cc/FUF7-QUG3.

[103] *Woven Electronics: An Uncommon Thread*, ECONOMIST, Mar. 8, 2014, *available at* http://www.economist.com/news/technology-quarterly/21598328-conductive-fibres-

resilient, which "means they can be fed into a loom or embroidered directly onto cloth that can be worn and washed as normal. With costs falling and use increasing, the threads are a rapidly growing business."[104] Meanwhile, technology developers are working actively to make these wearable devices more fashionable.[105]

[28] The medical monitoring capabilities associated with wearable technologies are particularly compelling. Eric Topol, author of *The Creative Destruction of Medicine: How the Digital Revolution Will Create Better Health Care*, predicts that in the coming years, we'll see apps and adds that "will bring with it the ability to obtain measurements continuously, even during sleep and times of substantial stress, which, as you might expect, are periods that represent essential gaps in our ability to track things today."[106]

[29] Many elderly individuals are already using wearable technologies to ensure they can report medical emergencies to caregivers and family

lighter-aircraft-electric-knickers-flexible-filaments, *archived at* http://perma.cc/N5HL-FZCF.

[104] *Id.*

[105] *See* Nick Bilton, *Tech, Meet Fashion*, N.Y. TIMES, Sept. 4, 2014, at E2 *available at* http://www.nytimes.com/2014/09/04/fashion/intel-and-opening-ceremony-collaborate-on-mica-a-stylish-tech-bracelet.html, *archived at* http://perma.cc/97C3-QAHN; Elizabeth Holmes, *Tech Companies and Fashion Designers Try to Put the 'Wear' in 'Wearables,'* WALL ST. J., Sept. 9, 2014, *available at* http://online.wsj.com/articles/tech-companies-and-fashion-designers-try-to-put-the-wear-in-wearables-1410305929, *archived at* http://perma.cc/HMH6-KLU5.

[106] ERIC TOPOL, THE CREATIVE DESTRUCTION OF MEDICINE: HOW THE DIGITAL REVOLUTION WILL CREATE BETTER HEALTH CARE 61 (2012). Topol goes on to examine how technology and these apps can revolutionize monitoring blood glucose, diabetes, heart rhythms, vital signs, asthma attacks, sleep apnea, and mood disorders. *See id.* at 65–73.

members.[107] Medical Body Area Network (MBAN) sensors in professional health care are also set to take off. MBAN sensors "will enable patient monitoring information such as temperature to be collected automatically from a wearable thermometer sensor."[108] South Korean scientists have already developed a flexible electronic skin patch "that's thinner than a sheet of paper and can detect subtle tremors, release drugs stored inside nanoparticles on-demand, and record all of this activity for review later."[109] Also, health technology provider MC10 has created Biostamp, a thin, bandage-like sensor patch that can be worn anywhere on the body to "monitor temperature, movement, heart rate, and more, and transmit this data wirelessly back to patients and their clinicians."[110]

[30] Many other medical and health-related wearable applications that take advantage of the aforementioned smartphone and tablet capabilities are already on the market. Nathan Cortez of the Southern Methodist University School of Law has developed a six-part typology of mobile health applications, some of which potentially butt up against existing Food and Drug Administration (FDA) regulatory authority (table 1).[111] In

[107] *See, e.g.*, Susan Young Rojahn, *An Activity Tracker for Seniors*, MIT TECH. REV. (Feb. 27, 2014), http://www.technologyreview.com/news/525016/an-activity-tracker-for-seniors, *archived at* http://perma.cc/NL4P-7EQY.

[108] *Disposable Wireless Sensor Market Shows Signs of Life: Healthcare Shipments to Reach 5 Million in 2018*, ABI RES. (May 3, 2013), *available at* http://www.abiresearch.com/press/disposable-wireless-sensor-market-shows-signs-of-l, *archived at* http://perma.cc/V6PX-VVV6.

[109] David Talbot, *A Bandage That Senses Tremors, Delivers Drugs, and Keeps a Record*, MIT TECH. REV. (Apr. 1, 2014), http://www.technologyreview.com/news/525976/a-bandage-that-senses-tremors-delivers-drugs-and-keeps-a-record, *archived at* http://perma.cc/RH9N-FJ7J.

[110] Sindya N. Bhanoo, *When Wearable Tech Saves Your Life, You Won't Take It Off*, FAST COMPANY (July 23, 2014, 12:00 PM), http://www.fastcompany.com/3033417/when-wearable-tech-saves-your-life-you-wont-take-it-off, *archived at* http://perma.cc/3YK3-XLFS.

[111] *See* Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1181–90 (Apr. 2014).

September 2013, the FDA issued draft guidance for mobile medical applications, which attempted to explain which mobile health apps qualified as regulated "medical devices" and which did not.[112] The agency noted that it "intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended."[113] Legislation has also been floated that would clarify the FDA's regulatory authority in this area.[114] Meanwhile, health insurance providers are starting to experiment with wearables to offer customers more tailored plans and premiums, which will likely drive greater regulatory interest.[115]

[112] *See* FDA, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (Sept. 25, 2013), *available at* http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm, *archived at* http://perma.cc/G7YH-PBBN.

[113] *Id.*

[114] *See, e.g.*, Ferdous Al-Faruque, *Are Smartphones the Best Medicine?*, THE HILL (June 17, 2014, 6:01 AM), http://thehill.com/policy/technology/209534-are-smartphones-the-best-medicine, *archived at* http://perma.cc/7A76-DLP9.

[115] *See, e.g.*, Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014. 1:26 PM), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance, *archived at* http://perma.cc/VG5W-6YUB.

Table 1. Typology of Mobile Health Technologies

Connectors: applications that connect smartphones and tablets to FDA-regulated devices, thus amplifying the devices' functionalities.
Replicators: applications that turn a smartphone or tablet itself into a medical device by replicating the functionality of an FDA-regulated device.
Automators and customizers: apps that use questionnaires, algorithms, formulas, medical calculators, or other software parameters to aid clinical decisions.
Informers and educators: medical reference texts and educational apps that primarily aim to inform and educate.
Administrators: apps that automate office functions, like identifying appropriate insurance billing codes or scheduling patient appointments.
Loggers and trackers: apps that allow users to log, record, and make decisions about their general health and wellness.

Source: Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. Davis L. Rev. 1181 (Apr. 2014).

[31] Beyond health and fitness applications, wearables can be used to enhance personal convenience. For example, wearables can be used in homes to tailor environmental experiences, such as automatically adjusting lighting, temperature, or entertainment options as users move from one space to another. Even if these technologies do not catch on as mass-market consumer products, wearable technology may come to be more widely used in a variety of business and organizations.[116] Some of the more exciting potential professional uses of wearable technology include the following:

[116] *See, e.g.*, H. James Wilson, *Wearables in the Workplace*, HARV. BUS. REV., Sept. 2013, *available at* http://hbr.org/2013/09/wearables-in-the-workplace/ar/1, *archived at* http://perma.cc/4BLQ-7MG4; *see also* Claire Cain Miller, *At Google, Bid to Put Its Glasses to Work*, N.Y. TIMES, Apr. 7, 2014 at B1, *available at* http://www.nytimes.com/2014/04/08/technology/google-begins-a-push-to-take-glass-to-work.html?_r=0, *archived at* http://perma.cc/J2Z7-WLLW.

- **Surgery:** Surgeons are already using wearable technology to better perform complex procedures, and in the future, wearable technology might be able to help them do this remotely.[117]
- **Emergency care:** Ambulances can be equipped with various IoT devices to more quickly diagnose what ails patients and then provide immediate treatment in the precious minutes after accidents or other health emergencies.[118]
- **Firefighting:** In coming years, firefighters might use wearable technology to respond to fires and other emergencies more rapidly using heads-up displays to obtain instant readouts of building schematics or environmental conditions.[119]
- **Law enforcement:** Wearables could transform the field of law enforcement but also raise some surveillance concerns in the process. Importantly, however, average citizens will also be able to use wearable technologies to monitor the activities of those same law enforcement officials.[120] They will have the First

[117] *See* Derek Mead, *Google Glass Is Already Being Used in the Operating Room*, MOTHERBOARD (June 24, 2013, 1:30 PM), http://motherboard.vice.com/blog/google-glass-is-already-being-used-in-the-operating-room, *archived at* http://perma.cc/NH4S-2DSB; Liz Gannes, *A Google Glass App That Would Be Hard for Even the Haters to Hate*, RE/CODE (Apr. 8, 2014, 9:00 AM PDT), http://recode.net/2014/04/08/a-google-glass-app-that-would-be-hard-for-even-the-haters-to-hate, *archived at* http://perma.cc/H8CG-J3LZ; Susan Young Rojahn, *Why Some Doctors Like Google Glass So Much*, MIT TECH. REV. (May 6, 2014), http://www.technologyreview.com/news/526836/why-some-doctors-like-google-glass-so-much, *archived at* http://perma.cc/8MVU-LF7J.

[118] *See* Maria K. Regan, *Saving Lives: Ambulances Get Connected to the IoT*, PTC (July 25, 2014), http://blogs.ptc.com/2014/07/25/saving-lives-ambulances-get-connected-to-the-iot, *archived at* http://perma.cc/SD58-FH7P.

[119] *See* Joanie Ferguson, *Firefighter Creates Google Glass App to Help Save Lives*, DAILY DOT (Mar. 5, 2013), http://www.dailydot.com/technology/firefighter-google-glass-app, *archived at* http://perma.cc/EXP8-SN4S.

[120] *See* Steve Mann, *Eye Am a Camera: Surveillance and Sousveillance in the Glassage*, TIME (Nov. 2, 2012), http://techland.time.com/2012/11/02/eye-am-a-camera-surveillance-and-sousveillance-in-the-glassage, *archived at* http://perma.cc/GP6F-N3JR; Alex Howard, *The 'Right to Record' Is Not a Question of Technology, but Rather Power*

Amendment right to do so.[121] This technology could provide a powerful check on abusive behavior by law enforcement officers, while giving those officers the ability to corroborate their accounts of incidents and altercations.[122]

- **Retailing:** Retailers will be able to target shoppers with personalized services and promotions either inside their stores or before the customers even arrive.[123] "As wearable technology gains popularity and becomes integrated into everyday life," says

and Policy, TECH REPUBLIC (May 22, 2014, 8:03 AM PST), http://www.techrepublic.com/article/the-right-to-record-is-not-a-question-of-technology-but-rather-power-and-policy/#, *archived at* http://perma.cc/3SED-M5PF.

[121] *See Recording Police Officers and Public Officials*, DIGITAL MEDIA LAW PROJECT (Dec. 18, 2013), http://www.dmlp.org/legal-guide/recording-police-officers-and-public-officials%20, *archived at* http://perma.cc/M8EN-785Y ("A number of U.S. Courts of Appeals have held that, in such circumstances, the First Amendment protects the right to record audio and video regardless of whether the police/officials consent. This constitutional right would override any state or federal laws that would otherwise prohibit such recording."); *see also* Marianne F. Kies, *Policing the Police: Freedom of the Press, the Right to Privacy, and Civilian Recordings of Police Activity*, 80 GEO. WASH. L. REV. 274, 276–66, 296 (2011); Steven A. Lautt, *Sunlight Is Still the Best Disinfectant: The Case for a First Amendment Right to Record the Police*, 51 WASHBURN L.J. 349, 350–51 (2012); Michael Potere, Note, *Who Will Watch the Watchmen?: Citizens Recording Police Conduct*, 106 NW. U. L. REV. 273, 316 (2012).

[122] *See* Tim Cushing, *After Two Officers Are Indicted for Shooting Citizens, Dallas Police Dept. Decides Body Cameras Might Be a Good Idea*, TECHDIRT (May 20, 2014, 12:48 AM), http://www.techdirt.com/articles/20140507/10325727152/after-two-officers-are-indicted-shooting-citizens-dallas-police-dept-decides-body-cameras-might-be-good-idea.shtml, *archived at* http://perma.cc/25U6-7Y6V.

[123] *See* Angela Benton, *Angela Benton on the Future of Entrepreneurship*, WALL ST. J., July 7, 2014, *available at* http://online.wsj.com/articles/angela-benton-on-the-future-of-entrepreneurship-1404762819, *archived at* http://perma.cc/EF9W-67CM ("[IoT presents] the opportunity for budding entrepreneurs of the future to access an individual's data and get a 360-degree view of that person. If you think the recommendation engines of today are good, wait until you see what the future holds. Every business and startup will compete to get to a customer at the perfect moment and with the perfect product that is so 'uniquely' them . . . .").

Giovanni DeMeo, vice president of Global Marketing and Analytics at Interactions, it will help retailers "establish a strong connection with shoppers" and also "provide a unique and improved shopping experience."[124]

- **Entertainment services:** Like retailers, entertainment companies, amusement parks, and vacation providers will also be able to use wearables to tailor services to users who visit their establishments or use their services. Disney has already created MagicBand, which can help those who will visit Disney's entertainment parks to personalize their experiences before they even get to the facilities.[125]
- **Airlines:** Some airlines are experimenting with wearable technologies "in a quest to provide an ever more personal service" and to "allow them to compile valuable information about passenger behaviors and preferences."[126]
- **Financial services:** Providers of personal finance and investment services are considering how wearable technologies might be adapted to better inform consumers of superior spending and investment opportunities.[127]

[124] Giovanni DeMeo, *Wearable Tech: If It Benefits You, It Benefits Retailers*, VENTUREBEAT (Dec. 24, 2013, 7:00 AM), http://venturebeat.com/2013/12/24/wearable-tech-if-it-benefits-you-it-benefits-retailers, *archived at* http://perma.cc/GCS4-2VW8.

[125] *See* Matthew Panzarino, *Disney Gets into Wearable Tech with the MagicBand*, NEXT WEB (May 29, 2013, 7:24 PM), http://thenextweb.com/insider/2013/05/29/disney-goes-into-wearable-tech-with-the-magic-band, *archived at* http://perma.cc/HD8S-XWBU.

[126] *Daily Report: Airlines Use Wearables to Get More Personal*, N.Y. TIMES (Mar. 18, 2014, 8:11 AM), http://bits.blogs.nytimes.com/2014/03/18/daily-report-airlines-use-wearables-to-get-more-personal, *archived at* http://perma.cc/79AP-MMGM.

[127] *See* Daniel Nader, *The Quantified Self Movement Reaches Personal Finance*, INSTITUTIONAL INVESTOR (Mar. 4, 2014), http://www.institutionalinvestor.com/Article/3315313/Banking-and-Capital-Markets-Trading-and-Technology/The-Quantified-Self-Movement-Reaches-Personal-Finance.html, *archived at* http://perma.cc/FVE9-93MG.

- **Political campaigning:** Politicians and "political professionals are eagerly exploring how [Google Glass] could become a powerful campaign tool" and how wearable technologies could help engage potential voters.[128]
- **Sports:** Teams and athletes may use wearables not only to improve their own abilities but also to potentially give fans an additional ways to see how they practice or even play their games.[129]

C. The Sci-Fi Future of Wearables: "Implantables," "Ingestibles," and "Biohacking"

[32] Wearable technologies will continue to evolve and could offer applications that might seem to have been ripped from the pages of science fiction novels.[130] For example, implantables, embeddables, and even ingestibles are already emerging as the next wave of wearable technology.[131] These technologies are now worn somewhere on the body,

[128] Don Gonyea, *Google Glass: Coming Soon to a Campaign Trail Near You*, NPR (Mar. 17, 2014, 5:00 AM), http://www.npr.org/blogs/itsallpolitics/2014/03/17/290714189/google-glass-coming-soon-to-a-campaign-trail-near-you, *archived at* http://perma.cc/FH7A-H6B9.

[129] *See* Claire Cain Miller, *At Google, Bid to Put Its Glasses to Work*, N.Y. TIMES, Apr. 7, 2014 at B1, *available at* http://www.nytimes.com/2014/04/08/technology/google-begins-a-push-to-take-glass-to-work.html, *archived at* http://perma.cc/4YTZ-NWCW ("Basketball players for the Sacramento Kings and Indiana Pacers have worn [Google] Glass with software from CrowdOptic to broadcast video streams to fans from their points of view, as well as during practice. It gives coaches a different view and a better understanding of court spacing and ball rotation, said Chris Granger, the Kings' chief operating officer . . . .").

[130] *See* Chip Stewart, *Do Androids Dream of Electric Free Speech? Visions of the Future of Copyright, Privacy, and the First Amendment in Science Fiction*, 19 COMM. L. & POL'Y 433, 433 (2014).

[131] *See, e.g.*, Tom Abate, *Stanford Engineer Invents Safe Way to Transfer Energy to Medical Chips in the Body*, STANFORD REPORT (May 19, 2014), http://news.stanford.edu/news/2014/may/electronic-wireless-transfer-051914.html, *archived at* http://perma.cc/A4ED-JNUY; Martyn Landi, *Wearable Tech to Evolve Inside the Human Body*, IRISH EXAMINER (Mar. 20, 2014),

but in the future might be swallowed or implanted within the body, potentially even in people's brains.[132] Some current examples include the following:

- SetPoint Medical, which was recently profiled by the *New York Times*, "began the world's first clinical trial to treat rheumatoid-arthritis patients with an implantable nerve stimulator . . . ."[133] The implant is roughly the size of a dime. "To recharge the device's batteries and update its software, patients and physicians will use an iPad app to control a wearable collar that transmits power and data wirelessly through the skin," the story noted.[134] The firm's goal is to use "bioelectronics" to "[g]et the nervous system to tell the body to heal itself."[135] Meanwhile, a variety of firms and university research centers are experimenting with neural interfaces and

http://www.irishexaminer.com/world/wearable-tech-to-evolve-inside-the-human-body-262624.html, *archived at* http://perma.cc/42DC-KJD3; George Skidmore, *Ingestible, Implantable, or Intimate Contact: How Will You Take Your Micro-scale Body Sensors*, FORBES (Apr. 17, 2013, 9:00 AM), http://www.forbes.com/sites/singularity/2013/04/17/ingestible-implantable-or-intimate-contact-how-will-you-take-your-micro-scale-body-sensors, *archived at* http://perma.cc/KJ37-448H; Cadie Thompson, *Wearable Tech Is Getting a Lot More Intimate*, ENTREPRENEUR (Dec. 26, 2013), http://www.entrepreneur.com/article/230555, *archived at* http://perma.cc/4RUR-MKXJ (originally appearing on CNBC).

[132] *See* Gary Marcus & Christof Koch, *The Future of Brain Implants*, WALL ST. J. (Mar. 14, 2014, 7:30 PM), http://online.wsj.com/news/articles/SB10001424052702304914904579435592981780528, *archived at* http://perma.cc/PV8M-YS97.

[133] Michael Behar, *Can the Nervous System Be Hacked*?, N.Y. TIMES, May 25, 2014 at MM36, *available at* http://www.nytimes.com/2014/05/25/magazine/can-the-nervous-system-be-hacked.html?partner=rssnyt&emc=rss, *archived at* http://perma.cc/M5Y9-TG2T.

[134] *Id.*

[135] *Id.*

bionic prosthetics to help individuals overcome various physical disabilities or simply enhance other human functions.[136]

- PillCam Colon, recently featured in the *Wall Street Journal*, has created "a capsule the size of a large vitamin [that] travels through a patient's digestive system over the course of several hours, wirelessly transmitting video images to an external data recorder."[137] As the *Journal* noted, this technology means that "[c]olon-cancer screening may soon become less invasive, more accurate—and more prevalent."[138] The FDA approved the device in February 2014 for patients who have received incomplete colonoscopies.[139]
- MicroCHIPS has created a contraceptive implant that can be wirelessly controlled by women without having to make a trip to a clinic, but doctors would be able to adjust dosages remotely if the patient so requested.[140]
- CardioMEMS HF System uses a wireless sensor, implanted in the pulmonary artery, to transmit health information to an external device, and "then [it] forwards the data to the patient's

[136] *See* Eliza Strickland, *We Will End Disability by Becoming Cyborgs*, IEEE SPECTRUM (May 27, 2014), http://spectrum.ieee.org/biomedical/bionics/we-will-end-disability-by-becoming-cyborgs, *archived at* http://perma.cc/E6YE-VEVM.

[137] Joseph Walker, *New Ways to Screen for Colon Cancer*, WALL ST. J. (June 8, 2014, 4:54 PM), http://online.wsj.com/articles/new-ways-to-screen-for-colon-cancer-1402063124, *archived at* http://perma.cc/V2LN-C5LC.

[138] *Id.*

[139] *See id.*

[140] *See* Gwen Kinkead, *A Contraceptive Implant with Remote Control*, MIT TECH. REV. (July 4, 2014), http://www.technologyreview.com/news/528121/a-contraceptive-implant-with-remote-control, *archived at* http://perma.cc/3M85-78D9.

medical team."[141] It "is designed to reduce hospitalizations among patients with moderate heart failure by enabling physicians to identify problems and modify treatment before patients end up in the [emergency room]."[142]

- Proteus Digital Health has created an ingestible sensor no bigger than a grain of sand that "it hopes will increase the effectiveness of existing medications by helping to ensure they're taken as prescribed."[143] Users would swallow the pill while administering other medications. After it is activated by stomach fluids, the pill transmits relevant information to a small disposable body patch as well as to the patient's computing devices via a Bluetooth connection. That information can then be shared with medical professionals "to better understand how patients are responding to their treatments."[144]

[33] Importantly, many of these implantable and ingestible innovations will be driven not just by commercial vendors, but also by average citizens working together to enhance various human capabilities.[145] Amateur body hacking or "biohacking" efforts will likely grow more prevalent in coming years.[146] Collaborative forums where individuals can share information

[141] Maria K. Rega, *Implantable Med Devices: 3 Smart Technologies to Watch*, PTC (June 2, 2014), http://blogs.ptc.com/2014/06/02/implantable-med-devices-3-smart-technologies-to-watch, *archived at* http://perma.cc/6KH4-UDPP.

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *See* Glen Martin, *"Biohackers" Mining Their Own Bodies' Data*, SF GATE (last updated June 28, 2012, 12:09 PM), http://www.sfgate.com/health/article/Biohackers-mining-their-own-bodies-data-3668230.php, *archived at* http://perma.cc/L4R4-YXZB; Jim McLauchlin, *The Future of Bionic Humans: What's Next in Bio-Hacking?*, LIVESCIENCE (June 18, 2013, 7:52 PM), http://www.livescience.com/37507-biohacking-james-rollins.html, *archived at* http://perma.cc/626V-4CGC.

and collaborate on various projects of this sort, such as Biohack.Me,[147] already exist.[148] Advocates of such amateur biohacking sometimes refer to themselves as "grinders," which Ben Popper of *The Verge* defines as "homebrew biohackers [who are] obsessed with the idea of human enhancement [and] who are looking for new ways to put machines into their bodies."[149]

[34] As these technologies and capabilities advance, they will raise thorny ethical and legal issues. Ethically, they will raise questions of what it means to be human and the limits of what people should be allowed to do to their own bodies.[150] In the field of law, they will challenge existing health and safety regulations imposed by the FDA and other government agencies.

[35] However, efforts to restrict such activities could be complicated by both practical and legal factors. Practically speaking, if enough people are attempting to modify their bodies or enhance various human capabilities, it may become very difficult for the law to keep up. Also—in terms of the

---

[146] Carolyn Y. Johnson, *As Synthetic Biology Becomes Affordable, Amateur Labs Thrive*, BOSTON GLOBE (Sept. 16, 2008), http://tech.mit.edu/V128/N39/biohack.html, *archived at* http://perma.cc/CFV3-LTC2.

[147] *See Biohack* (last visited Oct. 30, 2014), http://discuss.biohack.me, *archived at* http://perma.cc/5984-UQU7.

[148] *See* Keiron Monks, *Forget Wearable Tech: Embeddable Implants Are Already Here*, CNN (last updated Apr. 9, 2014, 1:08 PM), http://www.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/, *archived at* http://perma.cc/J43N-FW5N.

[149] Ben Popper, *Cyborg America: Inside the Strange New World of Basement Body Hackers*, VERGE (Aug. 8, 2012, 10:37 AM), http://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers, *archived at* http://perma.cc/WUK6-846A.

[150] *See generally* JOEL GARREAU, RADICAL EVOLUTION: THE PROMISE AND PERIL OF ENHANCING OUR MINDS, OUR BODIES—AND WHAT IT MEANS TO BE HUMAN (2005) (providing an overview of the differing opinions about how these technologies may affect our humanity).

law—because many of these activities will be of a voluntary, noncommercial nature, those producing and sharing information about biohacking activities will likely have First Amendment protection to do so, thereby making regulatory efforts even more challenging. Hence, regulators might have to focus on limiting the supply of materials and devices used by biohackers to achieve these goals. But those materials will likely fall in cost and expand in availability over time, especially with the rise of 3-D printing.[151] The FDA held a public workshop on these issues in early October 2014.[152]

[36] A more robust discussion of biohacking—and the various policy issues it might raise—is beyond the scope of this paper. The debate over wearable technologies, however, could foreshadow many of the same concerns and policy issues that will arise in these future debates. Moreover, some of the solutions that might emerge to deal with concerns about wearables might be useful when the debate over biohacking intensifies, which is why the issue has been discussed in this paper.

[37] At a minimum, these technologies will force a conversation about how much control people have over their bodies or at least about information regarding their bodies. "Studies show that more-engaged patients have lower costs and better health outcomes," a recent *Wall Street Journal* report noted.[153] "Becoming familiar with one's own health records can help patients better understand their own condition and have

[151] *See, e.g.*, Dan Carsen, *With 3-D Printing, Affordable Prosthetics Are in Reach*, NPR (Mar. 13, 2014, 4:00 PM), http://www.npr.org/2014/03/13/289836980/with-3-d-printing-affordable-prosthetics-are-in-reach, *archived at* http://perma.cc/QZ6R-W47M.

[152] *See* Meeting Notice, 79 Fed. Reg. 28732 (May 19, 2014).

[153] Laura Landro, *The Health-Care Industry Is Pushing Patients to Help Themselves*, WALL ST. J. (June 8, 2014, 4:54 PM), http://online.wsj.com/articles/the-health-care-industry-is-pushing-patients-to-help-themselves-1402065145, *archived at* http://perma.cc/9D2J-WEMQ.

more informed conversations with doctors."[154] But it remains to be seen whether such innovations will be allowed or how they might be regulated.

III. WHICH POLICY VISION WILL GOVERN THE INTERNET OF THINGS AND WEARABLE TECHNOLOGY?

[38] Many IoT technologies will be overhyped and could eventually fail.[155] For example, Internet-enabled refrigerators get plenty of attention today, but "the reality is that the average consumer will replace his or her fridge no more than once per decade—and, most likely, not for improved functionality, just to keep the milk cold."[156]

[39] As they become more commonplace and fashionable,[157] however, many other IoT technologies will succeed, including technologies and applications that are unimaginable today—albeit in a sporadic,

[154] *Id.*

[155] *See, e.g.*, Charles Arthur, *Wearables: One-hird of Consumers Abandoning Devices*, GUARDIAN (Apr. 1, 2014), http://www.theguardian.com/technology/2014/apr/01/wearables-consumers-abandoning-devices-galaxy-gear, *archived at* http://perma.cc/R5U9-AFNS; *see also* Zoë Corbyn, *Google Glass: Wearable Tech, but Would You Wear It?*, GUARDIAN (Apr. 6, 2014), http://www.theguardian.com/technology/2014/apr/06/google-glass-technology-smart-eyewear-camera-privacy, *archived at* http://perma.cc/EB2X-VVHC; Pascal-Emmanuel Gobry, *Today's Wearables Are an Overhyped Fad, but Wait a Few Years*, CITEWORLD (Mar. 20, 2014, 4:57 PM), http://www.citeworld.com/consumerization/23142/wearables-overhyped-fad, *archived at* http://perma.cc/VUN2-4NAQ; Duncan McKean, *Wearisome Wearables: Lessons Learned from a BMX Experiment, and Why Some Sections of Media Are Still Taking the Easy Option* CCGROUP (Mar. 5, 2014), http://www.ccgrouppr.com/insights/blog/mobile/wearisome-wearables-lessons-learned-bmx-experiment-sections-media-still-taking-easy-option, *archived at* http://perma.cc/G6R8-LFW5.

[156] Collins et al., *supra* note 28, at 3.

[157] *See, e.g.*, ROSE, *supra* note 19, at 28 ("The adoption of wearable devices will be accelerated as technology blends with fashion.").

unpredictable fashion.[158] Whether such technologies succeed or fail should be left to the interaction of inventors and consumers. What sort of policy regime will govern this fast-moving, constantly evolving space and help incentivize constantly expanding innovation and consumer choice? This paper will turn to that question next.

[40] Wearable technology, like IoT more generally, raises a wide variety of potential concerns, many of which relate to privacy and security.[159] These social and cultural concerns will be the primary focus of this paper. Economic concerns—including worries about job dislocations because of increasing automation[160]—also will come up in discussions about some of these technologies, but they will not be the primary focus of this paper.

[41] Such concerns are leading to a replay of a debate that has already occurred many times in the modern information economy: the clash between the "permissionless innovation" and "precautionary principle" mindsets.[161] A recent book published by the Mercatus Center discussed

[158] *See* DuBravac, *supra* note 29, at 8 ("While some of these things might seem far off, their foundations are already unfolding before us. We tend to think about linearly moving from point A to point B, but that is not the process through which tech adoption and innovation diffusion typically occur. These advancements—the little steps for man and the big steps for mankind—tend to occur through a series of hybrid periods.").

[159] *See, e.g.*, John Brandon, *Wearable Devices Pose Threats to Privacy and Security*, FOX NEWS (June 18, 2014), http://www.foxnews.com/tech/2014/06/18/wearable-devices-pose-threats-to-privacy-and-security, *archived at* http://perma.cc/9JM8-NC6E; *see also* Kashmir Hill, *The Half-Baked Security of Our 'Internet of Things*, FORBES (May 27, 2014, 2:56 PM), http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things, *archived at* http://perma.cc/2T42-VPP7; Raj Samani, *The IoT Is Already Here: Will You Be Secure?*, INFORMATION SECURITY BUZZ (Feb. 27, 2014), http://mcaf.ee/h2xom, *archived at* http://perma.cc/XRT3-JR7Y.

[160] *See* NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US 19 (2014); Michael Sacasas, *It's Alive, It's Alive!*, FRAILEST THING (June 6, 2014), http://thefrailestthing.com/2014/06/06/its-alive-its-alive, *archived at* http://perma.cc/N5ME-XF92.

[161] PERMISSIONLESS INNOVATION, *supra* note 7.

the interplay between these two worldviews and the implications of this policy battle for the future of various emerging technologies.[162] Each of these policy visions will be summarized below, and then their applicability to the debate over wearables and IoT will be discussed.

A. Permissionless Innovation vs. the Precautionary Principle

[42] Should the creators of new technologies seek the blessing of public officials before they develop and deploy their innovations? How people answer this question—which they might think of as "the permission question"—depends on the disposition they adopt toward new inventions.

[43] One policy disposition is known as the *precautionary principle*.[163] Generally speaking, it refers to the belief that new innovations should be curtailed or disallowed until their developers can prove that they will not cause any harms to individuals, groups, specific entities, cultural norms, or various existing laws, norms, or traditions.[164] Advocates believe policymakers should regulate new technology "early and often" to "get ahead of it" and address social and economic concerns preemptively.[165]

[44] The other policy vision can be labeled *permissionless innovation*.[166] The term refers to the notion that experimentation with new technologies and business models should generally be permitted by default.[167] Unless a compelling case can be made that a new invention

[162] *Id.*

[163] *See id.* at vii.

[164] *See id.*

[165] John Frank Weaver, *We Need to Pass Legislation on Artificial Intelligence Early and Often*, FUTURE TENSE (Sept. 12, 2014, 3:53 PM), http://www.slate.com/blogs/future_tense/2014/09/12/we_need_to_pass_artificial_intelligence_laws_early_and_often.html, *archived at* http://perma.cc/RH82-JJRM.

[166] *See, e.g.*, PERMISSIONLESS INNOVATION, *supra* note 7, at vii.

[167] *See, e.g., id.*

will bring serious harm to individuals, innovation should be allowed to continue unabated, and problems—if they develop at all—can be addressed later.[168] Permissionless innovation is not an absolutist position that denies any role for government. Rather, it is an aspirational goal that stresses the benefit of pushing "innovation allowed" as the best default position to begin debates about technology policy.[169] The burden of proof is on those who favor preemptive, precautionary controls to explain why ongoing trial-and-error experimentation with new technologies or business models should be disallowed.

[45] The clash between these two visions is already evident in today's policy discussions regarding wearable and IoT technologies. Again, some already worry about the security[170] and privacy implications of a world of wearable technology.[171] Others worry about the overquantification of people's lives[172] or—more profoundly—that these technologies will turn people into robots[173] or "cyborgs."[174]

---

[168] *See, e.g.*, *id.*

[169] *See e.g.*, *id.* at 5–6.

[170] *See Home, Hacked Home*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home, *archived at* http://perma.cc/P9C9-2QVE.

[171] *See* Hayley Tsukayama, *Wearable Tech Such as Google Glass, Galaxy Gear Raises Alarms for Privacy advocates*, WASH. POST (Sept. 30, 2013), http://www.washingtonpost.com/business/technology/wearable-technology-raise-privacy-concerns/2013/09/30/0a81a960-2493-11e3-ad0d-b7c8d2a594b9_story.html, *archived at* http://perma.cc/WU5J-B2FX.

[172] *See* Brendan O'Connor, *When Quantified-Self apps Leave You with More Questions Than Answers*, DAILY DOT (Feb. 27, 2014), http://www.dailydot.com/technology/reporter-quantified-self-app, *archived at* http://perma.cc/S8RA-9Z2M; Ben Williamson, *Calculating the Child Through Technologies of the 'Quantified Self,'* DMLCENTRAL (May 26, 2014, 8:00 AM), http://dmlcentral.net/blog/ben-williamson/calculating-child-through-technologies-%E2%80%98quantified-self%E2%80%99, *archived at* http://perma.cc/QHN6-U292.

[46] Some of these fears are likely driven by the rapid evolution of technologies in this space.[175] The most notable wearable technology on the market today—and among the most controversial—is Google Glass.[176] The peer-to-peer surveillance capabilities of Google Glass and other wearables—such as the Narrative clip-on camera, which allows users to automatically take snapshots of their daily activities every 30 seconds[177]—

[173] *See* Evan Selinger, *Google vs. Our Humanity: How the Emerging "Internet of Things" Is Turning Us into Robots*, SALON (May 22, 2014, 1:13 PM), http://www.salon.com/2014/05/22/google_vs_our_humanity_how_the_emerging_internet_of_things_is_turning_us_into_robots, *archived at* http://perma.cc/KVM4-CLB3.

[174] *See* Dann Berg, *Will Google Glasses Make Us Cyborgs?*, LAPTOP (Nov. 19, 2012, 1:26 PM), http://blog.laptopmag.com/will-google-glasses-make-us-cyborgs, *archived at* http://perma.cc/7TGL-M2T3; John Danaher, *Is Modern Technology Creating a Borg-Like Society?*, REAL CLEAR TECH. (June 11, 2014), http://www.realcleartechnology.com/articles/2014/06/11/is_modern_technology_creating_a_borg-like_society_1184.html, *archived at* http://perma.cc/82N7-9PB2; Cyrus Farivar, *"Stop the Cyborgs" Launches Public Campaign Against Google Glass*, ARS TECHNICA (Mar. 22, 2013, 2:50 PM), http://arstechnica.com/tech-policy/2013/03/stop-the-cyborgs-launches-public-campaign-against-google-glass, *archived at* http://perma.cc/RX8Z-KSV4.

[175] *See* Amy Collins, Adam J. Fleisher, D. Reed Freeman, Jr. & Alistair Maughan, *The Internet of Things Part 2: The Old Problem Squared*, MORRISON FOERSTER 6 (Mar. 20, 2014), http://media.mofo.com/files/Uploads/Images/140320-The-Internet-of-Things-Part-2.pdf, *archived at* http://perma.cc/YAG8-LB8Q (raising the question "whether the regulators can work fast enough to keep up with what the technology is capable of doing").

[176] *See* Clive Thompson, *Googling Yourself Takes on a Whole New Meaning*, N.Y. TIMES, Aug. 30, 2013, *available at* http://mobile.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html?pagewanted=5&_r=0&hpw=&, *archived at* http://perma.cc/6PMB-AUQT.

[177] *See* Liz Gannes, *Narrative—Formerly Known as Memoto—Launches Life-Logging Camera, Raises $3M*, ALL THINGS D (Oct. 3, 2013, 5:00 AM), http://allthingsd.com/20131003/narrative-formerly-known-as-memoto-launches-life-logging-camera-raises-3m, *archived at* http://perma.cc/HAA9-MRHH.

have already spawned a variety of privacy fears.[178] Other forms of wearable microphotography are coming to market just now (see, e.g., Butterfleye,[179] Autographer,[180] and CA7CH Lightbox[181]). They will eventually allow users to snap pictures at regular intervals but soon will likely also enable real-time audio and video streaming.[182] Of course, many other wearable cameras (e.g., GoPro) have been on the market for years, but the quality of those technologies is now rising as rapidly as their size and cost are falling.[183]

[47] Such real-time "life-logging" tools and activities raise a variety of privacy concerns.[184] In particular, how much data will these devices

[178] *See* Brandon, *supra* note 159; Thompson, *supra* note 176.

[179] *See An Intelligent, Sneaky, Wireless Camera for the Ultra-Connected Home*, CNET (May 21, 2014, 5:00 AM), http://www.cnet.com/products/butterfleye, *archived at* http://perma.cc/6S8P-4XD4.

[180] *See* Hugh Langley, *Autographer Boss: Google Glass Privacy Fears Have Been Exaggerated by the Media*, TECH RADAR (June 18, 2014), http://www.techradar.com/news/photography-video-capture/google-glass-privacy-fears-have-been-exaggerated-by-the-media-says-autographer-creator-1253837, *archived at* http://perma.cc/AZ3N-39FR.

[181] *See* Edgar Cervantes, *CA7CH Lightbox: The Next Wearable Camera to Compete Against the GoPro*, ANDROID AUTHORITY (June 18, 2014), http://www.androidauthority.com/ca7ch-lightbox-wearable-camera-394812, *archived at* http://perma.cc/QA7Q-DNBG.

[182] *See* E. J. Dickson, *Google Glass Livestream Brings Your Privacy Nightmares to Life*, DAILY DOT (Apr. 8, 2014), http://www.dailydot.com/technology/google-glass-livestream, *archived at* http://perma.cc/P33X-UZD9.

[183] *See* Alyssa Bereznak, *Panasonic's New Head-Mounted 4K Camera Will Capture Your Adventures More Clearly Than Ever*, YAHOO! TECH (Mar. 24, 2014), https://www.yahoo.com/tech/panasonics-new-head-mounted-4k-camera-will-capture-80589689809.html, *archived at* https://perma.cc/B8AE-5XY2.

[184] *See* Heather Kelly, *Google Glass Users Fight Privacy Fears*, CNN (Dec. 12, 2013, 2:47 PM), http://www.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions, *archived at* http://perma.cc/YN3Z-N7DB.

collect about users, how long will the data be retained, and who else might have access to that information?[185] The answers to these questions remain unclear at this point, but it is equally unclear what sort of beneficial uses and applications might flow from such technologies.[186] Those beneficial uses are often only discovered after a great deal of experimentation.

[48] Nonetheless, some policymakers, academics, and regulatory activists are calling for policy action on the potential privacy and security vulnerabilities associated with IoT and wearable technologies.[187] In a new paper titled "Regulating the Internet of Things," University of Colorado Law School professor Scott R. Peppet says that mere potential for certain harms "suggests a need for urgency" on this front.[188] He continues,

> Not only are consumers currently vulnerable to the discrimination, privacy, security and consent problems outlined here, but it may become harder over time to address such issues. In technological and political circles it may be convenient to prescribe a "wait and see—let the market evolve" stance, but the reality is that as time passes

[185] *See* Jamie Carter, *Wearable Cameras Are All the Rage but Should We All Become Lifeloggers?*, TECH RADAR (June 4, 2014), http://www.techradar.com/us/news/world-of-tech/life-through-a-lens-trials-and-tribulations-of-a-life-logger-1251717?src=rss&attr=all, *archived at* http://perma.cc/82EW-F74Q.

[186] *See Every Step You Take*, ECONOMIST (Nov. 16, 2013), http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be, *archived at* http://perma.cc/4CD4-NU49.

[187] *See* Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy?*, GUARDIAN (May 16, 2013), http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google, *archived at* http://perma.cc/RNZ5-XPMM; Mike Wheatley, *Big Brother's Big Data: Why We Must Fear the Internet of Things*, SILICON ANGLE, http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things, *archived at* http://perma.cc/6QTG-C4QS (last visited Dec. 1, 2014).

[188] Peppet, *supra* note 4, at 71.

> it will likely become harder, not easier, for consumer advocates, regulators, and legislators to act. The Internet of Things is here. It would be wise to respond as quickly as possible to its inherent challenges.[189]

In other words, Peppet is suggesting that new innovation in this space should be preemptively curtailed, or at least tightly regulated, to ensure that none of these potential risks or harms develop. Again, this is precautionary principle thinking.

[49] Some lawmakers and regulators have endorsed that sort of precautionary approach as the basis of public policy toward IoT and wearable technologies. Federal Trade Commission (FTC) Chairwoman Edith Ramirez addressed these issues in a 2013 speech, "The Privacy Challenges of Big Data: A View from the Lifeguard's Chair."[190] Ramirez worried about the privacy and security concerns associated with "big data," or the massive datasets of information made available through various modern digital sites and services.[191] Ramirez claimed,

> The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off chance that it might prove useful is not consistent with privacy best practices. And remember, not all data is created equally. Just as there is

[189] *Id.*

[190] *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data, A View From the Lifeguard's Chair (Aug. 19, 2013), *available at* http://www.ftc.gov/public-statements/2013/08/privacy-challenges-big-data-view-lifeguard's-chair, *archived at* http://perma.cc/X3HQ-HNPE.

[191] *Id.* at 1, 3.

> low quality iron ore and coal, there is low quality, unreliable data. And old data is of little value.[192]

Thus, she claimed, "information that is not collected in the first place can't be misused," and then she outlined a parade of "horribles" that will occur if such data collection is allowed at all.[193] She was particularly concerned that companies might use such data to discriminate against certain classes of customers.[194]

[50] There are other concerns regarding data collection practices. Some legal scholars today decry what Ryan Calo of the University of Washington School of Law calls "digital market manipulation," or the belief that "[f]irms will increasingly be able to trigger irrationality or vulnerability in consumers—leading to actual and perceived harms that challenge the limits of consumer protection law, but which regulators can scarcely ignore."[195] Others fear "power asymmetries" between companies and consumers and even suggest that consumers' apparent lack of concern about sharing information means that people may not be acting in their own best self-interest when it comes to online safety and digital privacy choices.[196] "[O]ne can imagine," Calo suggests, "the government

[192] *Id.* at 4.

[193] *Id.* at 6.

[194] *See id.* at 8.

[195] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703, *archived at* http://perma.cc/3XZL-ZMF8; *see also* David Talbot, *Data Discrimination Means the Poor May Experience a Different Internet*, MIT TECH. REV. (Oct. 9, 2013), http://www.technologyreview.com/news/520131/data-discrimination-means-the-poor-may-experience-a-different-internet, *archived at* http://perma.cc/GY7N-327X.

[196] *See, e.g.*, Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 729–30 (1999); *see also* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness, and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 443 (2011) (footnotes omitted) ("The idea is that individual choice in this area would lead, in a piecemeal fashion, to the erosion of privacy protections that are the foundation of the democratic

fashioning a rule—perhaps inadvisable for other reasons—that limits the collection of information about consumers in order to reduce asymmetries of information."[197]

B. The Problem with Precautionary Principle–Based Policymaking

[51] So, what's wrong with this sort of precautionary approach to policymaking? Doesn't it make sense to plan ahead for worst-case scenarios, including those that might develop for IoT and wearable technologies? After all, these technologies clearly have the potential to disrupt well-established social and legal norms.

[52] Anticipating and seeking to avoid potential hazards are important parts of life, but there are problems with converting the logic of "better safe than sorry" from an informal personal or institutional prescription into a formal legal directive. When individuals and institutions apply anticipatory, precautionary thinking and policies in their own lives or business decisions, they bear the cost of those efforts. By contrast, when precautionary thinking is converted into preemptive policy prescriptions, the cost of those actions will be borne by a far greater universe of actors.

[53] Generally speaking, the problem with "precautionary" policymaking comes down to this: if people spend all their time living in constant fear of worst-case scenarios—and premising public policy on such fears—it means that best-case scenarios will never come about. "Wisdom [and progress] are born from experience, including experiences

regime, which is the heart of our political system. Individuals are making an assessment—at least implicitly—of the advantages and disadvantages to them of sharing information. They are determining that information sharing is, on balance, a net gain for them. But the aggregate effect of these decisions is to erode the expectation of privacy and also the role of privacy in fostering self-development, personhood, and other values that underlie the liberal way of life. In this way, individual choices are not sufficient to justify information practices that collectively undermine widely shared public values.").

[197] Calo, *supra* note 195, at 1035.

that involve risk and the possibility of occasional mistakes and failures."[198] As the old adage goes, "nothing ventured, nothing gained."

[54] More concretely, the problem with "permissioning" innovation is that traditional regulatory policies and systems tend to be overly rigid, bureaucratic, costly, and slow to adapt to new realities.[199] Policies and regulatory systems based on precautionary thinking focus on preemptive remedies that aim to predict the future and its hypothetical problems, which may not ever come about. Worse yet, preemptive bans or regulatory prescriptions can limit innovations that yield new and better ways of doing things.[200]

[55] Regardless of whether the technical regulatory specifications for "permissioned" products and services are published in advance or whether firms must seek special permission before they offer a new product or service, both varieties of preemptive regulation have the same effect: they raise the cost of starting or running a business or nonbusiness venture and therefore discourage activities that benefit society. Such precautionary regulation can limit what Angela Benton, founder and CEO of NewME Accelerator, refers to as "democratized entrepreneurship," or the sort of modern start-up culture that means "[j]ust about anyone can afford to launch a business."[201] In turn, such limitation has implications for

[198] PERMISSIONLESS INNOVATION, *supra* note 7, at viii.

[199] *See* ABELSON ET AL., *supra* note 10, at 291 ("[B]ureaucracies change much more slowly than the technologies they govern.").

[200] *See* AARON WILDAVSKY, SEARCHING FOR SAFETY 183 (1988) ("Regulation, because it deals with the general rather than with the particular, necessarily results in forbidding some actions that might be beneficial. Regulators cannot devise specifications sufficiently broad to serve as guidelines for every contingency without also limiting some actions that might increase safety. Because regulation is anticipatory, regulators frequently guess wrong about which things are dangerous; therefore, they compensate by blanket prohibitions.").

[201] Angela Benton, *Angela Benton on the Future of Entrepreneurship*, WALL ST. J. (July 7, 2014, 3:53 PM), http://online.wsj.com/articles/angela-benton-on-the-future-of-entrepreneurship-1404762819, *archived at* http://perma.cc/5N38-WSEP.

consumers and end users of technology. Overly prescriptive regulatory systems can raise the cost of goods and services, diminish the quality of those goods and services, or limit the range of choices that the public has at its disposal.[202] Thus, preemptive, precautionary constraints should generally be reserved for circumstances with immediate and extreme threat to safety, security, or privacy.

[56] Precautionary principle thinking is often discussed in the context of IoT. Recall, for example, Calo's hypothetical rule that "limits the collection of information about consumers in order to reduce asymmetries of information."[203] Although Calo does not endorse the adoption of such a rule at this time, the cost of such a rule and comparable regulatory proposals should be taken into account and subjected to a strict benefit-cost analysis.[204] Alleviating all "information asymmetries" would be impossible without sweeping and constant regulatory interventions. If such precautionary regulation were imposed on IoT technologies, it could stifle the provision of devices and services that could substantially improve consumer welfare.[205]

---

[202] PERMISSIONLESS INNOVATION, *supra* note 7, at viii.

[203] Calo, *supra* note 195, at 1035.

[204] *See, e.g.*, Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1066–69 (2013) [hereinafter *A Framework*], *available at* http://mercatus.org/publication/framework-benefit-cost-analysis-digital-privacy-debates, *archived at* http://perma.cc/6UA4-7PUS; FED. TRADE COMM'N, PROJECT NO. P135405, COMMENTS OF THE FUTURE OF PRIVACY FORUM 13 (2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00013-88250.pdf, *archived at* http://perma.cc/FBX3-9H93 [hereinafter FUTURE OF PRIVACY FORUM] ("The value of the Internet of Things will largely come from rapidly evolving, beneficial uses of data. When considering whether the use of data is appropriate to the context, consideration should instead be given to the likely benefits and the risk, if any, of actual harm.").

[205] *See, e.g.*, Adam D. Thierer, Testimony before the Senate Comm. on Commerce, Sci. & Transp.: A Status Update on the Development of Voluntary Do-Not-Track Standards 2–3 (Apr. 24, 2013) [hereinafter Testimony before the Senate],

[57] The same would likely be true if Chairwoman Ramirez's approach to a preemptive data use "commandment" were enshrined into a law that said, "[t]hou shall not collect and hold onto personal information unnecessary to an identified purpose."[206] Such a precautionary limitation would certainly satisfy her desire to avoid hypothetical worst-case outcomes because, as she noted, "[i]nformation that is not collected in the first place can't be misused,"[207] but it is equally true that information that is never collected may never lead to serendipitous data discoveries or new products and services that could offer consumers concrete benefits. "The socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection," notes Ken Wasch, president of the Software & Information Industry Association.[208] If academics and lawmakers succeed in imposing such precautionary rules on the development of IoT and wearable technologies, many important innovations may never see the light of day.

C. The Importance of Regulatory Patience and Humility

[58] An embrace of permissionless innovation over precautionary principle thinking requires that legislators and regulators understand that patience and humility are worth embracing as policy virtues.[209] To the maximum extent possible, policymakers should exercise restraint and

---

http://mercatus.org/sites/default/files/Thierer_testimony_DNT_042313.pdf, *archived at* http://perma.cc/45LZ-5TZ8.

[206] Ramirez, *supra* note 190, at 4.

[207] *Id.* at 6.

[208] Letter from Ken Wasch, President, Software & Info. Indus. Ass'n, to Edith Ramirez, Chairwoman, Fed. Trade Comm'n (May 31, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00025-86182.pdf, *archived at* http://perma.cc/6HHS-5HJW.

[209] *See, e.g.*, PERMISSIONLESS INNOVATION, *supra* note 7, at 34–35, 66.

resist the urge to try to plan the future and all the various scenarios—good or bad—that might come about. This policy can be labeled *forbearance*.

[59] FTC Commissioner Maureen K. Ohlhausen concisely elucidated the philosophy of forbearance in an October 2013 speech, "The Internet of Things and the FTC: Does Innovation Require Intervention?," in which she noted that "[t]he success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."[210]

[60] Ohlhausen pointed out that the precautionary mindset is dangerous when enshrined into policy directives because regulators—in their zeal to correct for consumers' supposed irrationality or ignorance—often ignore regulators' irrationality or ignorance.[211] In other words, regulators can spend so much time focused on the supposed irrationality of consumers and their openness to persuasion or manipulation that those regulators end up ignoring their own irrationality or ignorance. Regulators simply do not possess the requisite knowledge to perfectly plan for every conceivable outcome, and attempts to do so will likely have many unintended consequences.[212]

[61] This is particularly true for information technology markets, which generally evolve much more rapidly than other sectors and especially more rapidly than the law itself.[213] Technology author Larry Downes

[210] Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, The Internet of Things and the FTC: Does Innovation Require Intervention?, Remarks Before the U.S. Chamber of Commerce 3 (Oct. 18, 2013), *available at* http://www.ftc.gov/public-statements/2013/10/internet-things-ftc-does-innovation-require-intervention-0, *archived at* http://perma.cc/K3NW-N8S9.

[211] *See id.* at 3–4.

[212] *See* ABELSON ET AL., *supra* note 10, at 159 ("Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent.").

notes that policymaking in the information age is inexorably governed by the "law of disruption" or the fact that "technology changes exponentially, but social, economic, and legal systems change incrementally."[214] This law is "a simple but unavoidable principle of modern life," he said, and it will have profound implications for the way businesses, government, and culture evolve.[215] "As the gap between the old world and the new gets wider," he argues, "conflicts between social, economic, political, and legal systems" will intensify, and "[n]othing can stop the chaos that will follow."[216]

[62] That insight prompts Ohlhausen to caution her fellow regulators:

> It is . . .vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.[217]

---

[213] *See* Collins et al., *supra* note 175, at 6 ("The key issue seems likely to be whether the regulators can work fast enough to keep up with what the technology is capable of doing. . . .").

[214] LARRY DOWNES, THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIFE AND BUSINESS IN THE DIGITAL AGE 2 (2009).

[215] *Id.*

[216] *Id.* at 2–3. In a similar sense, Andy Grove, former CEO of Intel, once reportedly said, "[h]igh tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap." Lillian Cunningham, *Google's Eric Schmidt Expounds on His Senate Testimony*, WASH. POST (Oct. 1, 2011), http://www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html, *archived at* http://perma.cc/UG4G-T5JQ.

[217] Ohlhausen, *supra* note 210, at 3–4.

Compared to Chairwoman Ramirez's policy approach, which is clearly based on precautionary principle thinking rooted in fears about hypothetical worst-case outcomes, Ohlhausen's approach to technological innovation in this space is consistent with the permissionless innovation approach.

[63] If policymakers care about expanding innovation opportunities, boosting consumer choice, and enhancing human welfare, then the philosophy of humility and forbearance should guide public policy. "Policymakers should generally exercise restraint and resist the urge to try to plan the future and [anticipate] all the various scenarios—good or bad—that might come about."[218] "Prospective regulation based on hypothesizing about future harms that may never materialize is likely to come at the expense of innovation and growth opportunities."[219] "To the extent that any corrective action is needed to address harms, *ex post* measures, especially via the common law, are typically superior."[220]

[64] Another lesson flows from this observation: not every wise ethical principle, social norm, or industry best practice automatically makes wise public policy prescriptions.[221] If policymakers hope to preserve a free and open society, they must not convert every ethical directive or societal norm—no matter how sensible—into a legal directive.

[65] For these reasons, more flexible, bottom-up approaches to solving complex problems are almost always superior to preemptive, precautionary, top-down controls. A variety of these less burdensome bottom-up solutions will be outlined in section VI.

---

[218] PERMISSIONLESS INNOVATION, *supra* note 7, at 66.

[219] *Id.* at 75.

[220] Adam Thierer, *Why Permissionless Innovation Matters*, MEDIUM (Apr. 24, 2014), https://medium.com/tech-liberation/why-permissionless-innovation-matters-257e3d605b63, *archived at* https://perma.cc/H997-5S69.

[221] *See, e.g.*, PERMISSIONLESS INNOVATION, *supra* note **7**, at viii.

[66] That being said, IoT and wearable technologies will raise many legitimate issues that deserve to be taken seriously and addressed in a constructive fashion. Some of these concerns, such as the safety of medical apps and wearable health devices, may raise some serious issues that deserve regulatory scrutiny. Such safety concerns will likely relate to only a subset of IoT devices, however. Privacy-related concerns will likely apply to a much wider class of IoT and wearable technologies, which is why those issues receive more attention in this paper. As will be noted next, traditional privacy regulatory paradigms and policies are likely to be unequipped to deal with some of these concerns.

IV. HOW THE INTERNET OF THINGS CHALLENGES TRADITIONAL PRIVACY NORMS AND LEGAL STANDARDS

[67] Because of the massive amount of information that IoT and wearable technologies can gather, privacy and security-related concerns will grow as these devices and services proliferate.[222] Users enjoy the personalization and customization that IoT and wearable technologies offer, yet those same capabilities that are so hotly demanded also exacerbate digital privacy and data security risks that already existed for traditional online services and technologies.[223] These privacy- and

[222] *See* Patrick Thibodeau, *The Internet of Things Could Encroach on Personal Privacy*, COMPUTERWORLD (May 3, 2014, 7:45 AM), http://www.computerworld.com/s/article/9248086/The_Internet_of_Things_could_encroach_on_personal_privacy.hhtml, *archived at* http://perma.cc/QNX5-4BXE; Jaikumar Vijayan, *The Internet of Things Likely to Drive an Upheaval for Security*, COMPUTERWORLD (May 2, 2014, 7:07 AM), http://www.computerworld.com/s/article/9248069/The_Internet_of_Things_likely_to_drive_an_upheaval_for_security.html, *archived at* http://perma.cc/C46Z-MYHX.

[223] *See* Jat Singh & Julia Powles, *The Internet of Things—The Next Big Challenge to Our Privacy*, GUARDIAN (July 28, 2014), http://www.theguardian.com/technology/2014/jul/28/internet-of-things-privacy, *archived at* http://perma.cc/4MA2-TA8D; Alexander Suarez, *Wearable Fitness Device Privacy Concerns Abound*, JDSUPRA (Sept. 11, 2014), http://www.jdsupra.com/legalnews/wearable-fitness-device-privacy-concerns-17278, *archived at* http://perma.cc/HS7A-DV3H.

security-related concerns can arise with regard to access to the device itself (i.e., what happens if it is lost or stolen); access to the information the device shares with nearby devices or systems (i.e., information shared over Wi-Fi or other wireless systems); or access to information transmitted to the cloud or to any remote storage system.[224]

[68] This section will specifically explore how IoT technologies in general and wearables in particular challenge traditional privacy norms—both social and legal—and will explain why a more creative and flexible approach to dealing with these issues will be necessary. It is important that the privacy concerns regarding wearable technologies relate to both the users of those technologies and others in surrounding environments. For users, the privacy concern is that wearables allow a massive amount of data to be observed, gathered, and shared about them—potentially without their knowledge.[225] Moreover, such data can be very sensitive—particularly the information related to their health or specific medical conditions.[226] In turn, these new datasets might be used by third parties for marketing purposes, by employers for job-related purposes, or even by insurers to adjust user premiums. This possibility raises the specter of IoT

[224] Al Sacco, *Fitness Trackers Are Changing Online Privacy—And It's Time to Pay Attention*, CIO (Aug. 14, 2014, 8:31 AM), http://www.cio.com/article/2465142/wearable-technology/fitness-trackers-are-changing-online-privacy-and-its-time-to-pay-attention.html, *archived at* http://perma.cc/X7H6-7FWP.

[225] *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 8/2014 ON THE ON RECENT DEVELOPMENTS ON THE INTERNET OF THINGS 4 (2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, *archived at* http://perma.cc/ZM36-XZ7M ("[O]nce the data is remotely stored, it may be shared with other parties, sometimes without the individual concerned being aware of it. In these cases, the further transmission of his/her data is thus imposed on the user who cannot prevent it without disabling most of the functionalities of the device. As a result of this chain of actions, the IoT can put device manufacturers and their commercial partners in a position to build or have access to very detailed user profiles.").

[226] *See* Sacco, *supra* note 224 ("It's the nature of the data that's being collected . . . . This is really getting to the essence of our being. It's hard to believe people are willing to share all this stuff, especially around health.").

and wearable devices and the datasets they generate being used in a supposedly discriminatory fashion.

[69] There are also concerns for those in environments where others are using wearable technologies. Such individuals may not be able to control how the wearable technologies used by others might be capturing their actions or data, and it may prove difficult if not impossible for them to grant consent in such contexts.[227]

A. Growing Privacy-Related Regulatory Interest in IoT and Wearables

[70] Policymaker interest in IoT and wearable technology is growing, and getting the legislative and regulatory balance right will affect the potential for ongoing innovation in this arena. "Courts, regulators and lawmakers will be fighting over IoT privacy safeguards for years to come," notes Patrick Thibodeau of *Computerworld*.[228] In fact, that process has already begun.

[71] In April 2013, the FTC launched an inquiry into the "Privacy and Security Implications of the Internet of Things" and invited comments.[229] That proceeding was followed by a daylong workshop on November 21, 2013, in Washington, DC.[230] The agency released its final report, *The*

[227] *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 225, at 7 ("[C]lassical mechanisms used to obtain individuals' consent may be difficult to apply in the IoT, resulting in a 'low-quality' consent based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals.").

[228] Thibodeau, *supra* note 42.

[229] *See* Press Release, Fed. Trade Comm'n, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things, *archived at* http://perma.cc/R6M5-69PF.

[230] *See id.*

Internet of Things: Privacy and Security in a Connected World, in January 2015.[231] In May 2014, the White House also completed an expedited ninety-day study "to examine how big data will transform the way we live and work and alter the relationships between government, citizens, businesses, and consumers."[232]

[72] Shortly thereafter, on May 7, 2014, the FTC also hosted a seminar, "Consumer Generated and Controlled Health Data," which explored the privacy concerns surrounding website and digital applications (including wearables) that collect information about personal health and fitness.[233] Following the FDA's draft guidance for mobile medical applications, which was discussed earlier, this FTC effort may become the federal government's next major foray into IoT and wearable technology regulation,[234] especially because many privacy advocates are already clamoring for policy action on this front.[235] This move is happening

[231] *See* FED. TRADE COMM'N, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, (2015) [hereinafter THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD], http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, *archived at* http://perma.cc/C2JF-AV3B.

[232] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, *archived at* http://perma.cc/JWY7-95ST.

[233] *Spring Privacy Series: Consumer Generated and Controlled Health Data*, FTC, http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data, *archived at* http://perma.cc/N72C-LFVF (last visited Dec. 21, 2014).

[234] *See* Mark Sullivan, *FTC May Soon Turn Its Regulatory Gaze Toward Data-Collecting Health Apps*, VENTUREBEAT (May 16, 2014, 3:41 PM), http://venturebeat.com/2014/05/16/ftc-may-soon-turn-its-regulatory-gaze-toward-data-collecting-health-apps, *archived at* http://perma.cc/WB9L-KJYQ.

[235] *See* LINDA ACKERMAN, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY 3, 5–6, 24–25 (2013), *available at*

against the backdrop of broader privacy-related policy efforts. Federal and state lawmakers have introduced a variety of privacy-related measures in recent years,[236] and regulatory interest in IoT and wearable technology is growing in Europe[237] and Asia.[238]

B. IoT and the Fair Information Practice Principles

[73] What these efforts share is a desire to extend traditional privacy norms and protections to the world of "big data" and IoT. With more information being produced, collected, categorized, and repurposed than ever before, policymakers worry that new laws and preemptive regulations may be needed to head off potential worst-case scenarios.[239]

---

https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf, *archived at* https://perma.cc/ZM9G-DS4P; Andrea Peterson, *Privacy Advocates Warn of 'Nightmare' Scenario as Tech Giants Consider Fitness Tracking*, WASH. POST (May 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/19/privacy-advocates-warn-of-nightmare-scenario-as-tech-giants-consider-fitness-tracking, *archived at* http://perma.cc/7TMW-ZY4W.

[236] *See* Pedro Pavón, *The "Internet of Things" Will Impact Law and Regulation in 2014*, LEXOLOGY (Jan. 16, 2014), http://www.lexology.com/library/detail.aspx?g=532f43f1-1bfb-47d0-aa13-096275055c08, *archived at* http://perma.cc/Y86U-4PAW.

[237] *See* HELEN REBECCA SCHINDLER ET AL., EUROPE'S POLICY OPTIONS FOR A DYNAMIC AND TRUSTWORTHY DEVELOPMENT OF THE INTERNET OF THINGS 1 (2013), *available at* http://www.rand.org/pubs/research_reports/RR356.html, *archived at* http://perma.cc/5TFX-V7Y5; *New Guidelines on Data Ownership and Liability Could Be Issued to Address 'Internet of Things' Phenomenon*, OUT-LAW (July 4, 2014), http://www.out-law.com/en/articles/2014/july/new-guidelines-on-data-ownership-and-liability-could-be-issued-to-address-internet-of-things-phenomenon, *archived at* http://perma.cc/X5C2-3HJ9.

[238] *See* Chris Neiger, *China Is Dominating the Internet of Things*, MOTLEY FOOL (June 15, 2014), http://www.fool.com/investing/general/2014/06/15/china-is-dominating-the-internet-of-things.aspx, *archived at* http://perma.cc/E3T9-LLGL.

[239] *See* Kate Tummarello, *Obama's 'Big Data' Report Calls for New Privacy Laws*, HILL (May 1, 2014, 2:28 PM), http://thehill.com/policy/technology/204961-white-house-big-data-report-calls-for-new-privacy-laws, *archived at* http://perma.cc/MK6K-AETX.

[74] Generally, these efforts have focused on translating traditional fair information practice principles (FIPPs) into a workable set of industry best practices. Modern privacy law and policy have been driven by a focus on these FIPPs and how they might guide data collection and use.[240] Obama administration privacy reports have generally listed the following FIPPs: Individual Control (i.e., "notice and consent"), Transparency, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.[241] The administration has advocated that such principles govern private-sector data collection and use and that they be formally enshrined in a congressionally implemented Consumer Privacy Bill of Rights.[242] Congress has not yet acted on the administration's request, however.

[75] That may be because lawmakers understand the challenge of applying FIPPs in a strict, legalistic fashion considering how rapidly technology, business practices, and consumer demands are evolving in the modern economy.[243] The lack of policy action may also be due to a more fundamental problem that has long haunted privacy policy and

[240] *See* Robert Gellman, Fair Information Practices: A Basic History 1, 12–14, 16–26 (Aug. 3, 2014) (unpublished manuscript), *available at* http://bobgellman.com/rg-docs/rg-FIPShistory.pdf, *archived at* http://perma.cc/NL6V-5CEZ.

[241] *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 232, at 19–20.

[242] *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–2, 6–7 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, *archived at* http://perma.cc/5SDE-7978.

[243] *See* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 274 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2019079, *archived at* http://perma.cc/J79P-4JN9 ("To this point, American lawmakers have been wisely reluctant to condemn the accumulation of personal information until we fully understand its consequences.").

enforcement: definitional confusion.[244] Writing at the International Association of Privacy Professionals blog, Brooks Dobbs, chief privacy officer for KBM Group, notes that "the terms 'personal data,' 'personal information,' and 'personally identifiable information' are often used interchangeably, [but] it's apparent they could easily be read to speak to fundamentally different things."[245] He notes:

> [This is] an enormous problem at the heart of our profession. Simply stated, as privacy professionals, we generally believe our jobs revolve around maintaining controls for the appropriate use and disclosure of either PII or personal data, but we can't agree on what those terms mean. This definitional problem is leading to monumental uncertainty at the core of our profession.[246]

Moreover, each of the core FIPPs is open to extensive interpretational disagreements among policymakers and privacy professionals alike. Brookings Institution scholars Benjamin Wittes and Wells C. Bennett conclude that privacy is "something of an intellectual rabbit hole, a notion so contested and ill-defined that it often offers little guidance to

[244] *See* Adam Thierer, *Privacy, Security, and Human Dignity in the Digital Age: The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 415, 424–35 (2013) [hereinafter *Privacy, Security, and Human Dignity*] ("[P]rivacy has always been a highly subjective philosophical concept. It is also a constantly morphing notion that evolves as societal attitudes adjust to new cultural and technological realities. For these reasons, America may never be able to achieve a coherent fixed definition of the term or determine when it constitutes a formal right outside of some narrow contexts.").

[245] Brooks Dobbs, *The Problem at the Heart of the Privacy Profession*, INT'L ASS'N PRIVACY PROFS. (May 19, 2014), https://privacyassociation.org/news/a/the-problem-at-the-heart-of-the-privacy-profession-2/, *archived at* https://perma.cc/8R8S-82PX.

[246] *Id.*

policymakers concerning the uses of personal information they should encourage, discourage, or forbid."[247]

[76] But these definitional dilemmas are only part of the problem. Even if "privacy" and the corresponding FIPPs could be defined with greater academic and legal rigor, an equally thorny problem arises when determining how to translate these principles into a workable enforcement regime for IoT and wearable technology. First Amendment–related hurdles to privacy enforcement may also exist. Those two issues will be discussed next.

C. Limitations of the Traditional "Notice and Consent" Model for IoT

[77] By their very nature, IoT and wearable technologies are always on, always sensing, always collecting, and always communicating. This condition will create major challenges for traditional FIPPs-based policymaking efforts. As FTC Chairwoman Ramirez notes, "the difficulties will be exponentially greater with the advent of the Internet of Things, as the boundaries between the virtual and physical worlds disappear."[248] She goes on to ask a series of questions about the rise of IoT and its implications for privacy best practices:

> Will consumers understand that previously inert everyday objects are now collecting and sharing data about them? How can these objects provide just-in-time notice and choice if there is no user interface at all? And will we be

[247] Benjamin Wittes & Wells C. Bennett, *Databuse and A Trusteeship Model of Consumer Protection in the Big Data Era*, GOVERNANCE STUDIES AT BROOKINGS 1, 1 (June 2014), *available at* http://www.brookings.edu/research/papers/2014/06/04-databuse-trusteeship-consumer-protection-big-data-era-privacy, *archived at* http://perma.cc/8JN4-KEUX.

[248] Edith Ramirez, Chairwoman, U.S. Fed. Trade Comm'n, The Internet of Things: Privacy and Security in a Connected World 4 (Nov. 19, 2013), *available at* http://www.ftc.gov/public-statements/2013/11/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission, *archived at* http://perma.cc/68H2-YW8H.

> asking consumers to make an unreasonable number of decisions about the collection and use of their data?[249]

"The answers to these and other questions may not be simple," Ramirez says, "[b]ut in my mind the question is not *whether* the core principles of privacy by design, simplified choice, and transparency should apply to the Internet of Things. The question is *how* to adapt them to the Internet of Things."[250]

[78] Alas, Ramirez does not offer a clear roadmap for how to do so. Nor has the FTC in its recent January 2015 staff report on Internet of Things issues. Although the agency "believes that providing notice and choice remains important," it also noted that "offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface."[251] That is hardly surprising, however, because it is almost impossible to envision how a rigid application of traditional notice and choice procedures to IoT would work in practice. The Future of Privacy Forum notes that while FIPPs "are a valuable set of high-level guidelines for promoting privacy, . . . given the nature of the technologies involved, *traditional* implementations of the FIPPs may not always be practical as the Internet of Things matures."[252]

[79] For example, it is not even clear at the moment whether existing wearable technologies and mobile medical applications are in compliance with—or even need to be in compliance with—the Health Insurance Portability and Accountability Act (HIPAA),[253] which governs the use of

[249] *Id.*

[250] *Id.*

[251] THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 231, at v.

[252] FUTURE OF PRIVACY FORUM, *supra* note 204, at 3.

"individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information."[254] As consumers use their smartphones and tablets as medical monitoring devices to compile data about their health and fitness and then share it with medical professionals or others, it will raise a variety of questions about HIPAA compliance as well as traditional FDA medical device regulatory compliance more generally.[255]

[80] Enforcing privacy best practices in an age of increasing device miniaturization means that, in many cases, it also will not be possible for consumers to read an organization's privacy policy because many of these technologies will be too small to even have a display.[256] Moreover, the sophistication of many of these devices and the sheer amount of data they collect make it difficult to devise a workable notice and choice regime that

---

[253] *See* Anne Marie Helm & Daniel Georgatos, *Privacy and Mhealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 156 (2014).

[254] *Understanding Health Information Privacy*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/, *archived at* http://perma.cc/5UGT-AA3U (last visited Dec. 4, 2014).

[255] *See* Mark Sullivan, *Health Apps Could Be Heading into a HIPAA Showdown*, VENTUREBEAT (June 13, 2014, 9:56 AM), http://venturebeat.com/2014/06/13/health-apps-could-be-heading-into-a-hipaa-showdown, *archived at* http://perma.cc/Z7L7-485Q.

[256] The FDA has already struggled with this problem in the context of digital advertising for prescription drugs and medical devices. In doing so, the agency has actually discouraged the use of some social media sites, such as Twitter, if adequate disclosure is difficult. The draft guidance says, "If the firm concludes that adequate benefit and risk information, as well as other required information, cannot all be communicated within the same tweet, then the firm should reconsider using Twitter for the intended promotional message." FOOD & DRUG ADMIN., U.S. DEP'T HEALTH & HUM. SERVS., GUIDANCE FOR INDUSTRY: INTERNET/SOCIAL MEDIA PLATFORMS WITH CHARACTER SPACE LIMITATIONS — PRESENTING RISK AND BENEFIT INFORMATION FOR PRESCRIPTION DRUGS AND MEDICAL DEVICES 7 (June 2014), *available at* http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401087.pdf, *archived at* http://perma.cc/A69N-8Z6V.

can foresee every possible misuse. As the recent White House *Big Data* report noted,

> Big data technologies, together with the sensors that ride on the "Internet of Things," pierce many spaces that were previously private. Always-on wearable technologies with voice and video interfaces and the arrival of whole classes of networked devices will only expand information collection still further. This sea of ubiquitous sensors, each of which has legitimate uses, make the notion of limiting information collection challenging, if not impossible.[257]

The White House concluded, "[t]ogether, these trends may require us to look closely at the notice and consent framework that has been a central pillar of how privacy practices have been organized for more than four decades."[258] In an accompanying report, the President's Council of Advisors for Science and Technology concluded that, "[a]s a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data."[259]

[81] Many academics agree. Peppet says, "notice and choice is an ill fitting solution to these problems, both because Internet of Things devices may not provide consumers with inherent notice that data rights are implicated in their use and because sensor-device firms seem stuck in a notice paradigm designed for web sites rather than connected consumer goods."[260]

---

[257] EXEC. OFFICE OF THE PRESIDENT, *supra* note 232, 53–54.

[258] *Id.* at 54.

[259] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf, *archived at* http://perma.cc/BK4F-RS8A.

D. The Possible Move Toward Use Restrictions for IoT

[82] In light of these problems, various academics, government officials, and even private companies have suggested that it may be necessary to move away from a policy approach rooted in notice and choice and toward a new regime based on use restrictions.[261]

[83] Former FTC officials J. Howard Beales and Timothy J. Muris have argued that "government should base commercial privacy regulations and policies on the potential consequences for consumers of information use and misuse. This approach focuses attention on the relevant questions of benefits and costs, and offers a superior foundation for regulation," they say.[262] Similarly, Craig Mundie, a senior advisor at Microsoft, says, "[t]he time has come for a new approach: shifting the focus from limiting the collection and retention of data to controlling data at the most important point—the moment when it is used."[263] Finally, in a recent report on revising data protection principles, Fred H. Cate of Indiana University, Peter Cullen of Microsoft, and Viktor Mayer-Schönberger of Oxford University argue that

> As a practical matter, the evolution of data collection and data use necessitates an evolving system of information privacy protection. A revised approach should shift

[260] Peppet, *supra* note 4, at 148.

[261] *See* Bambauer, *supra* note 243, at 270–71 ("Laws prohibiting specific uses of personal information can achieve the goals of privacy law without significantly curtailing the flow of truthful information. If we have reason to believe that a particular use diminishes social welfare, we can and should craft prohibitions on those specific uses.").

[262] *See, e.g.*, J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 109 (2008).

[263] Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, 93 FOREIGN AFF., Mar./Apr. 2014, at 28, 29.

> responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtain individual consent. In addition, a revised approach should focus more on data use than on data collection because the context in which personal information will be used and the value it will hold are often unclear at the time of collection.[264]

[84] Policymakers appear ready to move in this direction. The Obama administration's recent *Big Data* report suggested that "in instances where the notice and consent framework threatens to be overcome—such as the collection of ambient data by our household appliances—we may need to re-focus our attention on the context of data use, a policy shift presently being debated by privacy scholars and technologists."[265] The White House argued that this sort of "responsible use framework" has many potential advantages:

> It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[266]

---

[264] FRED H. CATE, PETER CULLEN & VIKTOR MAYER-SCHÖNBERGER, DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES 8 (Dec. 2013), *available at* http://op.bna.com/pl.nsf/id/dapn-9gyjvw/$File/Data-Protection-Principles-for-the-21st-Century.pdf, *archived at* http://perma.cc/258D-44NQ.

[265] EXEC. OFFICE OF THE PRESIDENT, *supra* note 232, at 56.

[266] *Id.*

The FTC's January 2015 IoT staff report stopped short of endorsing a use-based approach, however. The agency said "staff has incorporated certain elements of the use-based model into its approach" but "has concerns . . . about adopting a pure use-based model for the Internet of Things."[267] The agency worried that "it is unclear who would decide which additional uses are beneficial or harmful" under a use-based approach and that it would "not address the privacy and security risks created by expansive data collection and retention" and "would not take into account consumer concerns about the collection of sensitive information."[268] The agency was, by contrast, much more focused on trying to make notice and choice work for the IoT, as well as pushing data minimization limitations on developers.[269]

[85] Nonetheless, many companies—including many large IoT players—have suggested they are open to a move toward use-based restrictions. The Transatlantic Computing Continuum Policy Alliance—which includes AT&T, General Electric, Intel Corporation, and Oracle Corporation—has filed comments with the FTC arguing as follows:

> We need to move away from an approach centered on the collection of data to focus in practical terms on what happens to that data and how it's used, bearing in mind the real world harms and consequences. That does not mean that there is no role for notice and choice, but rather that we must review the context of the implementation and potential societal benefits from how the information may be used to determine what controls are needed to protect privacy within the circumscribed use. We need to think through how we manage notice and choice—not to change

[267] THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 231, at vi.

[268] *Id*., at vi–vii.

[269] *See id*., at 33.

> existing privacy principles, but to provide more guidance about how to apply the existing principles in this new IoT environment.[270]

Such a move away from notice and consent and toward use-based limitations seems likely as IoT and wearable technologies evolve and make older enforcement methods less effective.[271] For technologies such as Google Glass and other wearables, it would be impossible for users to obtain notice and consent from every individual they randomly passed by on a sidewalk or at an event. By contrast, it might be possible to impose some limited use-based restrictions of wearables to achieve privacy or safety goals.

[86] For example, the use of wearables in certain sensitive environments (such as bathrooms or locker rooms) could be prohibited. Use-based restrictions might also be imposed for safety-related reasons as well. A state senator in Illinois recently introduced a bill that would prohibit drivers from wearing Google Glass while operating a vehicle.[272] Even if that measure does not pass, it is easy to imagine comparable

[270] Letter from Daniel W. Caprio, Jr., Senior Strategic Advisor, Transatlantic Computing Continuum Policy Alliance, to Donald S. Clark, Sec'y, U.S. Fed. Trade Comm'n 3 (Jan. 10, 2014), *available at* http://cppionline.org/docs/Letter-to-Secretary_Clark_final.pdf, *archived at* http://perma.cc/5JL6-23K3.

[271] *See* Jill Valenstein, *Will Individual Notice and Consent Become a Relic of the Past? The White House Report on Big Data Suggests Privacy Regulation Should Focus on Data Use, Rather Than Data Collection*, PRIVACY & SEC. L. BLOG (May 20, 2014), http://www.privsecblog.com/2014/05/articles/main-topics/marketing-consumer-privacy/will-individual-notice-and-consent-become-a-relic-of-the-past-the-white-house-report-on-big-data-suggests-privacy-regulation-should-focus-on-data-use-rather-than-data-collection, *archived at* http://perma.cc/7Q94-XM98.

[272] *See* John Byrne, *Illinois Lawmaker Wants to Outlaw Wearing Google Glass While Driving*, CHI. TRIB. (May 20, 2014), http://articles.chicagotribune.com/2014-05-20/news/chi-illinois-google-glass-law-driving-20140520_1_google-glass-illinois-lawmaker-silverstein, *archived at* http://perma.cc/Z8AK-YDMN.

restrictions being imposed on the use of wearables while driving or operating heavy machinery.

E. The Problem of "Privacy Paternalism" and the Limits of Privacy "Harm"

[87] In crafting use-based restrictions, however, policymakers must exercise caution. Overly broad restraints could end up being tantamount to a de facto ban on *all* uses of certain IoT or wearable technologies. Moreover, policymakers must avoid converting their preferences—or the preferences of just a small but vocal group of regulation advocates—into paternalistic policies that limit individual autonomy.[273] The goal of privacy policy should not be to prevent people from making choices that others feel are unwise.

[88] Privacy scholar Daniel J. Solove of the George Washington University School of Law has warned about privacy law's "paternalism" problem.[274] "Privacy regulation," he notes, "risks becoming too paternalistic. Regulation that sidesteps consent denies people the freedom to make choices. The end result is that either people have choices that are not meaningful or people are denied choices altogether."[275]

[89] Privacy is too subjective to have policymakers or academics dictating outcomes on the basis of their own preferences.[276] As Solove

[273] *See* Adam Thierer, *Is Privacy an Unalienable Right? The Problem with Privacy Paternalism*, TECH. LIBERATION FRONT (Jan. 27, 2014), http://techliberation.com/2014/01/27/is-privacy-an-unalienable-right-the-problem-with-privacy-paternalism/, *archived at* http://perma.cc/3MUS-8GEH.

[274] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1895–96 (2013).

[275] *Id.* at 1894.

[276] *See* Thierer, *supra* note 244, at 414–21; Thomas M. Lenard & Paul H. Rubin, The Big Data Revolution: Privacy Considerations 24 (Dec. 2013) (unpublished manuscript), *available at* http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconside

notes, "the correct choices regarding privacy and data use are not always clear. For example, although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively."[277] Generally speaking, barring a clear showing of actual—not prospective or hypothetical—harm,[278] U.S. culture has rejected the paternalistic idea that law must "save us from ourselves" (i.e., from citizens' own irrationality or mistakes).[279] Importantly, the term *harm* in this context has usually been narrowly defined as action that poses a direct threat to human well-being, personal property, or the home.[280] This is not to say emotional or psychic harm associated with privacy violations are ignored completely under U.S. law,[281] merely that a much higher bar

rations.pdf, *archived at* http://perma.cc/2BQE-HCG5 (worrying that "many of the privacy advocates and writers on the subject do not trust the consumers for whom they purport to advocate").

[277] Solove, *supra* note 274, at 1895.

[278] *See id.* at 1897 ("The law generally does not override consent, even with potentially dangerous activities . . . . As a general matter, the law refrains from restricting transactions that appear on the surface to be consensual, and the law will tolerate a substantial amount of manipulation and even coercion before it deems a transaction to be nonconsensual.").

[279] *See id.* ("People make decisions all the time that are not in their best interests. People relinquish rights and take bad risks, and the law often does not stop them.").

[280] *See* PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 15, (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf, *archived at* http://perma.cc/5YHW-Z6EB ("Prescriptive regulation may be called for where there is significant risk to human life or health because the injuries people may suffer are irreversible or deadly. This makes compensation after the fact impossible or insufficient. Though suffering a privacy violation can be devastating, information policy can not be fairly characterized as an area of significant danger to human life or health.").

[281] *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011); Daniel Solove, *Privacy and Data Security Violations: What's the Harm?*, LINKEDIN (June 25, 2014), https://www.linkedin.com/today/post/article/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm, *archived at* https://perma.cc/5X89-RD6A.

exists when attempting to make the case that those harms should be legally actionable.[282]

[90] That approach generally makes sense in light of both how subjective privacy can be and the high value Americans place on privacy in balancing it against other values, such as freedom of speech and journalistic freedoms (which will be discussed in the next section), as well as economic innovation and consumer choice. "We have fallen in love with this always-on world," note Hal Abelson, Ken Ledeen, and Harry Lewis, authors of *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*.[283] "We accept our loss of privacy in exchange for efficiency, convenience, and small price discounts."[284] Although many privacy advocates are loath to hear it, the reality is that "[w]e give away information about ourselves—voluntarily leave visible footprints of our daily lives—because we judge, perhaps without thinking about it very much, that the benefits outweigh the costs. To be sure, the benefits are many," argue Abelson, Ledeen, and Lewis.[285]

[91] This is why America's privacy torts typically involve a careful weighing of competing values and why courts usually try to strike a balance among them. "Reasonable minds are bound to differ when deciding whether the likely psychic harms outweigh the social gains," notes Jane Yakowitz Bambauer of the University of Arizona College of Law.[286] "The values on both sides of the scale are inordinately difficult to measure."[287]

---

[282] *See* Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467, 473–77 (2014) [hereinafter *Precautionary Principle*].

[283] ABELSON ET AL., *supra* note 10, at 20.

[284] *Id.*

[285] *Id.* at 36.

[286] Bambauer, *supra* note 243, at 261.

[287] *Id.*

[92] For those reasons, use-based restrictions should not be converted into a regulatory straitjacket that uniformly mandates data collection and use practices according to a static, one-size-fits-all blueprint. The need for flexibility and adaptability will be paramount if innovation is to continue in this space.[288]

[93] For example, if policymakers attempt to craft a use-based restriction that prohibits the use of wearable data on grounds that it could be used to discriminate against users, lawmakers should narrowly tailor that rule to address truly invidious forms of racial, sexual, or religious discrimination.[289] Of course, many antidiscrimination laws that might make such practices illegal anyway already exist.[290] But the term *discrimination* should not be construed to include any form of service differentiation, such as tailored product offerings that help expand the range of consumer services.[291] In the future, some IoT developers might

[288] *See* FUTURE OF PRIVACY FORUM, *supra* note 204, at 6 ("Even in circumstances where traditional [privacy policy] implementations may seem appropriate, however, flexibility is needed.").

[289] *See* Sam Pfeifle, *How Big Data Discriminates*, INT'L ASS'N PRIVACY PROFS. (June 24, 2014), https://www.privacyassociation.org/publications/how_big_data_discriminates, *archived at* https://perma.cc/2UED-U2VK.

[290] *See* Bambauer, *supra* note 243, at 271 ("Antidiscrimination laws are prime examples of narrow use restrictions. Antidiscrimination laws restrict the use of race, age, sex, or medical information for hiring, housing, and lending decisions because the biases that result from use of this information, whether statistically rational or not, run against the public interest. These laws work well on the risk-utility calculator because they allow information to be exploited for all purposes except the ones that have been determined to be harmful or risky. The large, rich scholarship on discrimination law explores and debates the soundness of anti-discrimination measures. Curiously, the privacy and discrimination fields often work in isolation, without overt awareness that regulations called 'privacy laws' and those called 'antidiscrimination laws' often aim to prevent the same harms." (internal citations omitted)).

[291] *See* Hal Varian, *Price Discrimination*, *in* 1 HANDBOOK OF INDUSTRIAL ORGANIZATION 597, 598 (Richard Schmalensee & Robert Willig eds., 1989), *available at*

craft creative data sharing policies that provide consumers with a wide variety of unanticipated benefits. Serendipitous discoveries and data-driven innovation can materialize only in a policy environment that embraces trial-and-error experimentation.[292] That is why flexible data collection and use proposals and evolving best practices will ultimately serve consumers better than one-size-fits all, top-down regulatory edicts.

[94] Even well-intentioned regulation can create complex and sometimes quite costly tradeoffs.[293] Data collection has fueled a remarkable amount of the innovation in the modern economy.[294] Privacy-

http://www.sciencedirect.com/science/handbooks/1573448X/1, *archived at* http://perma.cc/ZL85-Y7FU (discussing the benefits of price discrimination).

[292] *See* PERMISSIONLESS INNOVATION, *supra* note 7, at 1, 17, 81; Letter from Daniel Castro to Nicole Wong, *supra* note 15 ("The federal government can play a major role in maximizing the potential benefits of big data, but it must above all encourage use and reuse of data. This means allowing data to be collected and retained for serendipitous future applications that were not foreseen at the time of collection, while restricting harmful applications.").

[293] *See A Framework*, *supra* note 204, at 1082–83.

[294] *See* JOHN DEIGHTON & PETER A. JOHNSON, THE VALUE OF DATA: CONSEQUENCES FOR INSIGHT, INNOVATION & EFFICIENCY IN THE U.S. ECONOMY 5–6 (DMA Oct. 18, 2013), *available at* http://thedma.org/wp-content/uploads/The_Value_of_Data_Consequences_for_Insight_Innovation_and_Efficiency_in_the_US_Economy_WEB.pdf, *archived at* http://perma.cc/8RBD-9VFM (finding that data-driven marketing added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012); JAMES MANYIKA ET AL., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 97–102 (McKinsey Global Institute May 2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation, *archived at* http://perma.cc/4L9K-85CP; ROBERT J. SHAPIRO, THE U.S. SOFTWARE INDUSTRY: AN ENGINE FOR ECONOMIC GROWTH AND EMPLOYMENT 1–5 (Sonecon Sept. 2014), *available at* http://www.sonecon.com/docs/studies/Report_for_SIIA-Impact_of_Software_on_the_Economy-Robert_Shapiro-Sept2014-Final.pdf, *archived at* http://perma.cc/XE7B-CVRS; Press Release, Gartner, Gartner Says Big Data Will Drive $28 Billion of IT Spending in 2012 (Oct. 17, 2012), *available at*

related mandates that propose curtailing the use of data could have several deleterious effects, including higher costs for consumers, a decrease in the content and services supported by that data collection and advertising, increased costs for smaller operators and new start-ups (meaning less competition overall), and perhaps even a decrease in America's global competitive advantage in the digital economy.[295]

[95] All these considerations and tradeoffs apply equally to IoT and wearable technologies. Health and fitness application providers already collect and sell a certain amount of user information to advertisers so they can create richer user profiles and deliver more relevant ads.[296] Some users may find that creepy, but this process is what ensures the cost of such services remains low or even altogether free of charge. And users are always free to avoid such services completely if they fear such data collection practices.

[96] Instead of imposing these FIPPs in a rigid regulatory fashion, therefore, these privacy and security best practices will need to evolve gradually to new realities and be applied in a more organic and flexible fashion, often outside the realm of public policy. For example, providing consumers with adequate information about various data collection practices remains a sensible best practice for developers to follow, even if it proves difficult to enforce by law. Likewise, IoT developers would be wise to be highly transparent about their data use policies and also limit the amount of overall data collection to core functions as much as possible. Finally, they should limit retention of that data, limit sharing with too many third parties, and safeguard the data they collect against unauthorized interception or data breaches.

---

http://www.gartner.com/newsroom/id/2200815, *archived at* http://perma.cc/XY3C-4MDX.

[295] *See* Testimony before the Senate, *supra* note 205, at 2–3.

[296] *See* Thorin Klosowski, *Lots of Health Apps Are Selling Your Data: Here's Why*, LIFEHACKER (May 9, 2014, 10:00 AM), http://lifehacker.com/lots-of-health-apps-are-selling-your-data-heres-why-1574001899, *archived at* http://perma.cc/N7Y5-RGFB.

[97] The key takeaway from this discussion is that no silver-bullet solution to these complex privacy issues exists. As analysts with Morrison Foerster have argued, "threats to security and privacy vary considerably and the breadth of challenges presented means that a one-size-fits-all approach to policy and/or regulation is unlikely to work."[297] What is needed is a layered approach. Some potential responses will be outlined in section VI of this paper. But one additional complication needs to be discussed first: the First Amendment.

F. First Amendment–Related Hurdles to the Regulation of IoT and Wearable Technology

[98] To the extent that wearable technologies are used by individuals to record and gather video, audio, and other data, First Amendment rights may be implicated. There has long existed a tension between privacy and free speech rights, which will be greatly exacerbated by the rise of these IoT technologies.

[99] Legal scholar Rodney A. Smolla notes that "strong First Amendment doctrines stand in the way of many of the most meaningful privacy reforms."[298] In particular, legal scholars have long noted that press rights are also affected by stronger commercial privacy controls. Philosopher Judith Jarvis Thomson argues that "even if there is a right to not be caused distress by the publication of personal information, it is mostly, if not always, overridden by what seems to me a more stringent right, namely the public's right to a press which prints any and all information, personal or impersonal, which it deems newsworthy. . . ."[299]

[100] But more than just journalistic freedoms are at stake here. The First Amendment protects the right of all citizens to observe and freely

[297] Collins et al., *supra* note 175, at 2.

[298] Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1138 (1999).

[299] Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 310 (1975).

gather information about the world around them and to use various technologies to help them do so. As the Seventh Circuit explained in its 2012 decision in *ACLU v. Alvarez*,

> The act of *making* an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording. The right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of *making* the recording is wholly unprotected, as the State's Attorney insists. By way of a simple analogy, banning photography or note-taking at a public event would raise serious First Amendment concerns; a law of that sort would obviously affect the right to publish the resulting photograph or disseminate a report derived from the notes. The same is true of a ban on audio and audiovisual recording.[300]

Although some privacy theorists argue that data and data collection are not protected speech deserving First Amendment protection,[301] other scholars recognize that restrictions on data collection are restrictions on the free flow of information, which implicate the First Amendment.[302] This reasoning is supported by the Supreme Court's 2011 decision in *Sorrell v. IMS Health Inc.*, which struck down a state law prohibiting data aggregators from selling personal information to pharmaceutical

[300] ACLU v. Alvarez, 679 F.3d 583, 595–96 (7th Cir. 2012).

[301] *See, e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1173–75 (2005); *see also* Tim Wu, Op-Ed., *Free Speech for Computers?*, N.Y. TIMES, June 20, 2012, at A29, *available at* http://www.nytimes.com/2012/06/20/opinion/free-speech-for-computers.html, *archived at* http://perma.cc/HK9M-KCKX.

[302] *See, e.g.*, Jane Yakowitz Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 57 (2014) ("Data privacy laws regulate minds, not technology. Thus, for all practical purposes, and in every context relevant to the privacy debates, data is speech.").

companies, which in turn use the data to customize their marketing pitches to doctors.[303] In line with a lower court ruling, the Supreme Court found that the regulation violated the First Amendment "because it restricts the speech rights of data miners without directly advancing legitimate state interests."[304] The Court's ruling means that restrictions on the sale, disclosure, and use of personally identifying information will be subject to heightened judicial scrutiny in the future.

[101] This makes it clear how the First Amendment might pose a serious roadblock to more comprehensive regulation of IoT and wearable technologies—regardless of whether these devices and services are being used for commercial or noncommercial purposes. For example, consider technologies such as Google Glass and wearable clip-on cameras, which were discussed earlier. When individuals use these technologies in public spaces, it is likely that their First Amendment rights to record information and interactions would trump most privacy considerations.[305] "Current U.S. privacy law recognizes only a very limited right of privacy in public, one that would likely not bar citizens from . . . gathering information through augmented-reality spectacles," says Daxton "Chip" Stewart of Texas Christian University's College of Communication.[306] That will be equally true for many other IoT and wearable technologies.

---

[303] *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2672 (2011).

[304] Yara Tercero-Parker, *U.S. Supreme Court Questions State Drug Data Restrictions*, BIOETHICS INT'L (Apr. 27, 2011), http://www.bioethicsinternational.org/blog/2011/04/27/us-supreme-court-questions-state-drug-data-restrictions, *archived at http://perma.cc/3LKP-SCL7*; *see also Sorrell*, 131 S. Ct. at 2672.

[305] *See* Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 398 (2011) ("Once we recognize that image capture is protected by principles of free expression, proposals to impose liability without observing the established limitations of privacy torts—either by common law innovation or by statute—raise serious constitutional questions. Such liability would facilitate interference with efforts by private individuals to preserve their observations for future review, reflection, and dissemination without any actual demonstration to a court of substantial countervailing privacy interests.").

[102] Thus, when considering the application of traditional FIPPs in this context, policymakers would be wise to remember law professor Eugene Volokh's observation:

> We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits . . .), whether the communication is "fair" or not.[307]

This does not mean that government is completely powerless to impose privacy-related restrictions on some information-gathering efforts. As will be noted in section VI, some targeted statutes already exist that limit information gathering in highly sensitive contexts outside the scope of First Amendment protection.[308] For example, though citizens have broad liberties to use cameras and recording devices in public, privacy torts and "peeping Tom" laws prohibit intrusive or surreptitious recording in private spaces or even in many public places. Also, the use of wearables in private spaces could be constrained by private contracts and property rights considerations, although enforcement challenges will be evident in this context, too. In other words, although limiting data collection proves challenging (either because of the practicality of doing so or because of First Amendment considerations), it might be possible to impose some limits or penalties on data dissemination after the fact.

[103] In sum, more expansive regulatory efforts aimed at clamping down on information collection efforts using IoT and wearable technologies are

[306] Stewart, *supra* note 130, at 455–56.

[307] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000).

[308] *See, e.g.*, Bambauer, *supra* note 243, at 267–68.

bound to face formidable First Amendment–related challenges.[309] Policymakers will need to narrowly tailor privacy-related measures if they hope to avoid these complications.

V. THE ROLE OF RESILIENCY AND GRADUAL SOCIAL ADAPTATION

[104] Before discussing some of the ways that the public and policymakers might constructively address concerns about IoT and wearable technology, it is worth discussing the important—and quite often overlooked—role that social and individual adaptation plays with regard to new inventions.[310]

A. From Resistance to Resiliency

[105] Citizen attitudes about these technologies will likely follow a cycle that has played out in countless other contexts; and "[t]hat cycle typically witnesses initial *resistance*, gradual *adaptation*, and then eventual *assimilation* of a new technology into society."[311] Some citizens will begin their relationship with these new technologies in a defensive crouch. In the extreme, if there is enough of a backlash, the initial resistance to these technologies might take the form of a full-blown "technopanic."[312]

---

[309] *See, e.g.*, Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 51 (2002) ("[T]o the extent that privacy laws restrict expression, even if that expression is commercial, the First Amendment imposes a considerable burden on the government to demonstrate the need and effectiveness of those laws.").

[310] *See* Adam Thierer, *Muddling Through: How We Learn to Cope with Technological Change*, TECH. LIBERATION FRONT (June 17, 2014), http://techliberation.com/2014/06/17/muddling-through-how-we-learn-to-cope-with-technological-change, *archived at* http://perma.cc/WD4U-KZRN.

[311] *See* PERMISSIONLESS INNOVATION, *supra* note 7, at 53.

[312] *See* Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J.L. SCI. & TECH. 309, 311 (2013).

[106] Over time, however, citizens tend to learn how to adapt to new technologies or at least become more resilient in the face of new challenges posed by modern technological advances. Andrew Zolli and Ann Marie Healy, authors of *Resilience: Why Things Bounce Back*, define *resilience* as "the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances."[313] They continue,

> To improve your resilience is to enhance your ability to resist being pushed from your preferred valley, while expanding the range of alternatives that you can embrace if you need to. This is what researchers call *preserving adaptive capacity*—the ability to adapt to changed circumstances while fulfilling one's core purpose—and it's an essential skill in an age of unforeseeable disruption and volatility.[314]

Consequently, they note, "by encouraging adaptation, agility, cooperation, connectivity, and diversity, resilience-thinking can bring us to a different way of being in the world, and to a deeper engagement with it."[315]

[107] Those who propose more precautionary solutions to challenging social problems often ignore this uncanny ability of individuals and institutions to "bounce back" from technological disruptions and become more resilient in the process. Part of the reason precautionary thinking sometimes dominates discussions about emerging technologies is that many people hold a deep-seated pessimism about future developments and a belief that, with enough preemptive planning, they can anticipate and overcome any number of hypothetical worst-case scenarios.

[313] ANDREW ZOLLI & ANN MARIE HEALY, RESILIENCE: WHY THINGS BOUNCE BACK 7 (2012).

[314] *Id.* at 7–8.

[315] *Id.* at 16.

Consequently, their innate tendency not only to be pessimistic but also to want greater certainty about the future means that "the gloom-mongers have it easy," notes author Dan Gardner.[316] "Their predictions are supported by our intuitive pessimism, so they *feel* right to us. And that conclusion is bolstered by our attraction to certainty."[317] Clive Thompson, a contributor to *Wired* and the *New York Times Magazine*, also notes that

> [D]ystopian predictions are easy to generate. . . . [and] doomsaying is emotionally self-protective: If you complain that today's technology is wrecking the culture, you can tell yourself you're a gimlet-eyed critic who isn't hoodwinked by high-tech trends and silly, popular activities like social networking. You seem like someone who has a richer, deeper appreciation for the past and who stands above the triviality of today's life.[318]

[108] Luckily, as science reporter Joel Garreau reminds readers, "[t]he good news is that end-of-the-world predictions have been around for a very long time, and none of them has yet borne fruit."[319] Doomsayers have a bad track record because they typically ignore how "humans shape and adapt [technology] in entirely new directions."[320] "Just because the problems are increasing doesn't mean solutions might not also be increasing to match them," Garreau correctly notes.[321]

---

[316] DAN GARDNER, FUTURE BABBLE: WHY EXPERT PREDICTIONS FAIL—AND WHY WE BELIEVE THEM ANYWAY 141 (2010).

[317] *Id.*

[318] CLIVE THOMPSON, SMARTER THAN YOU THINK: HOW TECHNOLOGY IS CHANGING OUR MINDS FOR THE BETTER 283 (2013).

[319] GARREAU, *supra* note 150, at 148.

[320] *Id.* at 95.

[321] *Id.* at 150–51.

[109] In their 2001 "Response to . . . Doom-and-Gloom Technofuturists," John Seely Brown and Paul Duguid note that "technological and social systems shape each other. . . . [They] are constantly forming and reforming new dynamic equilibriums with far-reaching implications."[322] "Social and technological systems do not develop independently," rather, "the two evolve together in complex feedback loops, wherein each drives, restrains, and accelerates change in the other."[323]

[110] This is how humans become more resilient and prosper, even in the face of sweeping technological change. Wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures while both developing new technologies and learning how to live with them.[324] Citizens should remain open to new forms of technological change not only because doing so provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve—and to learn from that change. More often than not, citizens find creative ways to adapt to technological change by using a variety of coping mechanisms, new norms, or other creative fixes. Although some things are lost in the process, something more is typically gained, including lessons about how to deal with subsequent disruptions.

B. Case Study: The Rise of Public Photography

[111] Consider the jarring impact that the rise of the camera and public photography had on American society in the late 1800s.[325] This case

[322] John Seely Brown & Paul Duguid, *A Response to Bill Joy and the Doom-and-Gloom Technofuturists*, *in* AAAS SCIENCE AND TECHNOLOGY POLICY YEARBOOK 2001 77, 79, 82 (Albert H. Teich, Stephen D. Nelson, Celia McEnaney & Stephen J. Lita eds., 2001).

[323] *Id.* at 83.

[324] *See* PERMISSIONLESS INNOVATION, *supra* note 7, at viii.

[325] *See* Robert E. Mensel, *Kodakers Lying in Wait: Amateur Photography and the Right of Privacy in New York, 1885–1915*, 43 AMER. QUAR. 24, 25, 28 (1991).

study has implications for the debate over wearable technologies. Plenty of critics existed, and many average citizens were probably outraged by the spread of cameras[326] because "[f]or the first time photographs of people could be taken without their permission—perhaps even without their knowledge," notes Lawrence M. Friedman in his 2007 book, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*.[327]

[112] In fact, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay "The Right to Privacy," decries the spread of public photography. The authors lament that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claim that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[328]

[113] Despite the profound disruption caused by cameras and public photography, personal norms and cultural attitudes evolved quite rapidly as cameras became a central part of the human experience. In fact, instead of shunning cameras, most people quickly looked to buy one! At the same time, social norms and etiquette evolved to address those who would use cameras in inappropriate or privacy-invasive ways. In other words, citizens bounced back and became more resilient in the face of technological adversity.

[114] Although some limited legal responses were needed to address the most egregious misuses of cameras, for the most part the gradual evolution of social norms, public pressure, and other coping mechanisms combined

[326] *See id.* at 29 (discussing of the anxieties caused by photography during this time).

[327] LAWRENCE M. FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 214 (2007).

[328] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

to solve the "problem" of public photography. As will be noted in the next section, in much the same way IoT and wearable technology will likely see a similar combination of factors at work as individuals and society slowly adjust to the new technological realities of the time. The public will likely develop coping mechanisms to deal with the new realities of a world of wearable technologies and become more resilient in the process.

[115] That being said, resiliency should not be equated with complacency or a "just-get-over-it" attitude toward privacy and security issues. With time, it may very well be the case that people "get over" *some* of the anxieties they might hold today concerning these new technologies, but in the short run, IoT and wearable technologies will create serious social tensions that deserve serious responses.[329] This paper will turn to some of those potential responses next.

VI. CONSTRUCTIVE SOLUTIONS TO COMPLEX PROBLEMS

[116] Even if it is true that precautionary regulation will be costly, counterproductive, or potentially ineffective—and should therefore be avoided if possible—this does not mean the various privacy and security challenges associated with IoT and wearable technologies can be ignored.

[117] As noted already, there are no silver-bullet solutions that can instantly or easily solve these complex problems. Instead, what is needed is a *layered* approach to addressing these concerns that incorporates many different solutions. This section outlines a variety of constructive approaches that can be tapped to address the various privacy and security concerns associated with these new innovations.

[329] *See* Adam Thierer, *Can We Adapt to the Internet of Things?*, INT'L ASS'N PRIVACY PROFS. (June 19, 2013), https://www.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things, *archived at* https://perma.cc/V3Q9-2QET.

A. Digital Literacy: How Education and Etiquette Can Help

[118] One solution to the privacy, security, and safety concerns raised by IoT and wearable technologies is to better educate the public about the potential downsides associated with these technologies, as well as their proper and improper uses.[330] This can be accomplished with a variety of education and awareness-building efforts.[331]

[119] Such efforts are already the primary means of dealing with concerns about online child safety.[332] Much like today's policy debates over online privacy, early policy debates over online child safety focused on top-down regulatory solutions, including efforts to censor objectionable content.[333] These efforts to devise legislative and regulatory responses to online safety concerns immediately faced both technical and legal challenges. Technically speaking, devising workable filtering mechanisms for a medium such as the Internet proved elusive. In terms of the law, at least in the United States, various First Amendment–based constraints made it impossible to devise constitutionally permissible restrictions.[334]

[120] After many years of trying and failing to impose such restrictions, policymakers and online safety experts instead turned their attention to educational and empowerment-based solutions.[335] The educational

[330] *See Precautionary Principle*, *supra* note 282, at 480.

[331] *See* Howard Beales, Richard Craswell & Steven C. Salop, *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 531 (1981) ("Consumer education is often overlooked as a means of dealing with incomplete information.").

[332] *See generally* ADAM THIERER, PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS AND METHODS 11–14 (Version 4.0) (Progress & Freedom Found. Summer 2009), *available at* http://www.pff.org/parentalcontrols/, *archived at* http://perma.cc/E2QH-D7PG (explaining the importance of parental controls).

[333] *See Precautionary Principle*, *supra* note 282, at 479–82.

[334] *See* Reno v. ACLU, 521 U.S. 844, 874–79, 885 (1997).

approaches that they tapped—which focused on media literacy strategies, critical thinking skills, and "digital citizenship"—are equally relevant in the context of online privacy.[336] Digital citizenship efforts stress the importance of teaching both children and adults better online behavior, or "netiquette" (proper behavior toward others), which can promote both online safety and digital privacy goals.[337] Digital literacy and digital citizenship efforts can help individuals understand the potential perils of oversharing information about themselves and others while simultaneously encouraging consumers to occasionally delete unnecessary

[335] *See* Adam Thierer, *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, 16 PROGRESS ON POINT, July 2009, at 1–2, *available at* http://www.pff.org/issues-pubs/pops/2009/pop16.13-five-online-safety-task-forces-agree.pdf, *archived at* http://perma.cc/P5R6-8GNR (discussing how online safety task forces agree that education is the primary solution to online child safety concerns); ONLINE SAFETY & TECH. WORKING GRP., YOUTH SAFETY ON A LIVING INTERNET: REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP 1–2 (June 4, 2010), *available at* http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf, *archived at* http://perma.cc/YG8W-NTSF (discussing the findings of the Online Safety and Technology Working Group in reviewing the status of industry efforts to promote online safety through educational efforts).

[336] COMMON SENSE MEDIA, DIGITAL LITERACY AND CITIZENSHIP IN THE 21ST CENTURY: EDUCATING, EMPOWERING, AND PROTECTING AMERICA'S KIDS 1 (June 2009), *available at* https://www.itu.int/council/groups/wg-cop/second-meeting-june-2010/CommonSenseDigitalLiteracy-CitizenshipWhitePaper.pdf, *archived at* https://perma.cc/YTX4-YL73.

[337] *See generally* Anne Collier, *From Users to Citizens: How to Make Digital Citizenship Relevant*, NETFAMILYNEWS (Nov. 16, 2009), http://www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html, *archived at* http://perma.cc/V52V-FBZY (suggesting that digital citizens should read the terms of service, seek social media service support that that parents and educators should educate children about digital citizenship); *see also* Larry Magid, *We Need to Rethink Online Safety*, HUFFINGTON POST (Mar. 24, 2010, 5:12 AM), http://www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html, *archived at* http://perma.cc/T3N4-6A5X (stressing the importance of Internet safety education).

online information and cover their digital footprints in other ways.[338] "We live in what one might call the Peeping Tom society," argues Stanford law professor Lawrence M. Friedman, in that "[n]ew technology puts powerful tools for invading privacy into the hands of ordinary people."[339] Digital literacy and digital citizenship efforts can help address that problem.

[121] The Obama administration's *Big Data* report included a short section on the need to "[r]ecognize digital literacy as an important 21st century skill," noting,

> In order to ensure students, citizens, and consumers of all ages have the ability to adequately protect themselves from data use and abuse, it is important that they develop fluency in understanding the ways in which data can be collected and shared, how algorithms are employed and for what purposes, and what tools and techniques they can use to protect themselves. Although such skills will never replace regulatory protections, increased digital literacy will better prepare individuals to live in a world saturated by data. Digital literacy—understanding how personal data is collected, shared, and used—should be recognized as an essential skill in K-12 education and be integrated into the standard curriculum.[340]

[122] In 2013, scholars affiliated with the Center on Law and Information Policy at the Fordham University School of Law released a good model for how to operationalize this vision. They launched a privacy education program "aimed at engaging middle school students in

[338] Brian O'Neill & Yiannis Laouris, *Teaching Internet Safety, Promoting Digital Literacy: The Dual Role of Education and Schools*, TOWARDS A BETTER INTERNET FOR CHILDREN? POLICY PILLARS, PLAYERS AND PARADOXES 193 (Brian O'Neill, Elisabeth Staksrud & Sharon McLaughlin eds., 2013).

[339] FRIEDMAN, *supra* note 327, at 259, 269.

[340] EXEC. OFFICE OF THE PRESIDENT, *supra* note 232, at 64.

discussions about privacy and its relevance in their lives."[341] The resulting Volunteer Privacy Educators Program offered students some lessons about how to deal with social media and how to actively manage their digital reputation, as well as how to establish strong passwords and avoid behavioral advertising, if they were so inclined.[342]

[123] Governments can play an important role in facilitating education and awareness-building approaches. The FTC notes, "Consumer and business education serves as the first line of defense against fraud, deception, and unfair practices."[343] Toward that end, the FTC already partners with over a dozen other federal agencies to provide OnGuardOnline, a website that offers wide-ranging security, safety, and privacy tips for both consumers and businesses.[344] Also, the FTC has created a YouTube page featuring informational videos on these issues.[345]

---

[341] *Volunteer Privacy Educators Program*, FORDHAM CTR. ON LAW & INFO. POLICY, *available at* http://law.fordham.edu/center-on-law-and-information-policy/30317.htm, *archived at* http://perma.cc/M8SA-SDML (last visited Dec. 1, 2014).

[342] *See* FORDHAM CTR. ON LAW & INFO. POLICY, FORDHAM CLIP VOLUNTEER PRIVACY EDUCATORS PROGRAM (2013), *available at* http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Complete.pdf, *archived at* http://perma.cc/65EC-3BAY.

[343] U.S. FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2009 TO 2014 4 (Sept. 2009), *available at* http://www.ftc.gov/opp/gpra/spfy09fy14.pdf, *archived at* http://perma.cc/L4VV-MEUB ("Most FTC law enforcement initiatives include a consumer and/or business education component aimed at preventing consumer injury and unlawful business practices, and mitigating financial losses. From time to time, the agency conducts pre-emptive consumer and business education campaigns to raise awareness of new or emerging marketplace issues that have the potential to cause harm. The agency creatively uses new technologies and private and public partnerships to reach new and under-served audiences, particularly those who may not seek information directly from the FTC.").

[344] *See About Us*, ONGUARD ONLINE, *available at* http://www.onguardonline.gov/about-us, *archived at* http://perma.cc/DJJ8-DKRH (last visited Jan. 29, 2015).

[345] *See Federal Trade Commission*, YOUTUBE, https://www.youtube.com/user/FTCvideos, *archived at* https://perma.cc/N35M-9L5Y (last visited Jan. 29, 2015).

As part of its recent staff IoT report, the FTC said it "will develop new consumer and business education materials in this area" in coming months and years.[346] The Federal Communications Commission also offers smartphone security advice on its website.[347] Many privacy activists and privacy professionals already offer extensive educational programs and advice.[348]

B. Best Practices and Self-Regulation: Privacy and Security "By Design"

[124] Privacy and data security policies for IoT and wearable technology can also be governed by self-regulatory efforts.[349] Developers have a vested interest in adopting best practices and codes of conduct because "only by developing solutions that are clearly respectful of people's privacy, and devoting an adequate level of resources for disseminating and explaining the technology to the mass public" can companies expect to achieve widespread adoption of IoT technologies.[350]

---

[346] THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 231, at 53.

[347] *See FCC Smartphone Security Checker*, FCC.GOV, http://www.fcc.gov/smartphone-security, *archived at* http://perma.cc/G67V-GUXL (last visited Jan. 15, 2015).

[348] *See* David Hoffman, *What's One Way Organizations Can Be More Accountable? Privacy Education*, INT'L ASS'N PRIVACY PROFS. (Apr. 2, 2013), https://www.privacyassociation.org/privacy_perspectives/post/whats_one_way_organizations_can_be_more_accountable_educate_educate_educate, *archived at* https://perma.cc/GRM5-T7ZT; Sacco, *supra* note 224 (discussing the Symantic Security Response team's findings regarding security concerns of wearable fitness trackers).

[349] *See* Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, INT'L ASS'N PRIVACY PROFS. (June 24, 2014), https://www.privacyassociation.org/publications/will_industry_self_regulation_be_privacys_way_forward, *archived at* https://perma.cc/RK7R-43AE.

[350] INFSO D.4 NETWORKED ENTERPRISE & RFID INFSO G.2 MICRO & NANOSYSTEMS, *supra* note 52, at 21.

[125] "Compared to traditional government regulation," notes FTC Commissioner Maureen Ohlhausen, "self-regulation has the potential to be more prompt, flexible, and responsive when business models or technologies change."[351] Ohlhausen itemizes other advantages of self-regulation as follows:

- It is "easier to reconfigure than major regulatory systems that must be adjusted via legislation or agency rulemaking."
- It "can also be well attuned to market realities where self-regulatory organizations have obtained the support of member firms. Their accumulated judgment and hands-on experience in their industries help create rules that are workable for companies."
- It "also helps prompt compliance by allowing corporations to 'buy-in' to the process."
- It "may also offer a less adversarial, more efficient dispute resolution mechanism than formal legal procedures."
- It is "a useful option to resolve consumer concerns, so that government enforcement resources can be preserved for the most egregious cases of consumer harm."
- "[T]he cost burden of a self-regulatory process falls on industry participants rather than American taxpayers."[352]

[126] Importantly, Ohlhausen notes that "[s]elf-regulation may also be the only option for certain types of activity where government intervention is limited by the First Amendment."[353] For the reasons stated in section IV, this consideration is of obvious relevance to the use of wearable

[351] Maureen K. Ohlhausen, Comm'r, U.S. Fed. Trade Comm'n, Success in Self-Regulation: Strategies to Bring to the Mobile and Global Era, Address to the Better Business Bureau Self-Regulation Conference 3 (June 24, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/410391/140624bbbself-regulation.pdf, *archived at* http://perma.cc/957C-ZU67.

[352] *Id.*

[353] *Id.*

technologies, which could be protected from regulation on free speech grounds.

[127] Industry self-regulation in this space can take the form of what is known as *privacy by design* and *security by design*.[354] These terms generally refer to efforts by developers to "bake in" certain privacy and security practices and protections as they are designing and deploying new technologies.[355] The Future of Privacy Forum has compiled a centralized resource of current standards and best practices to help firms address a wide variety of privacy concerns (e.g., app development, children's privacy, locational privacy and mobile services, and online ads)[356] and has also developed a blueprint to help organizations conduct privacy impact assessments for data-oriented innovations.[357] The Council of Better Business Bureaus has also produced detailed best-practice guidelines for data security[358] and data privacy for small businesses.[359] Finally, privacy

[354] *See* ANN CAVOUKIAN, PRIVACY BY DESIGN AND THE EMERGING PERSONAL DATA ECOSYSTEM 4 (Privacy by Design Oct. 2012), *available at* http://www.ipc.on.ca/images/Resources/pbd-pde.pdf, *archived at* http://perma.cc/K6QJ-2ND3.

[355] *See, e.g.*, Letter from Daniel W. Caprio, Jr. to Donald S. Clark, *supra* note 270, at 4 ("These context-specific [privacy and security] choices are something engineers, working alongside privacy and security professionals, can help bake into products."). Efforts aimed at "baking in" security best practices have been under way for many years. *See* Heather Havenstein, *Baked-In Security*, COMPUTERWORLD (Mar. 21, 2005, 12:00 AM), http://www.computerworld.com/s/article/100443/Baked_In_Security, *archived at* http://perma.cc/ZF58-6URF (urging the need for developers to build in security features to applications).

[356] *See Best Practices*, FUTURE PRIVACY F., http://www.futureofprivacy.org/resources/best-practices, *archived at* http://perma.cc/6QMT-7MLV (last visited Dec. 19, 2014).

[357] *See* JULES POLONETSKY, OMER TENE & JOSEPH JEROME, BENEFIT-RISK ANALYSIS FOR BIG DATA PROJECTS 1 (Future of Privacy Forum Sept. 2014), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf, *archived at* http://perma.cc/3TT3-MCK5.

expert Daniel Solove created TeachPrivacy, an educational resource to help train employees about privacy and data security matters.[360]

[128] What do privacy and security by design entail? There are several practical steps that developers of IoT and wearable technologies can take, including the following:

- **Proper use guidelines:** Developers should include clear warnings in their packaging materials that explain to new owners the dangers associated with inappropriate use of their technologies. Many of them already do so.
- **Transparency:** Giving consumers more and better information about their digital tools is one of the key objectives of best practice efforts.[361] "Transparency is crucial," argues FTC Chairwoman Edith Ramirez, "As more and more of our devices become smarter and smarter, it is essential we know as much about them as they know about us—that we understand what information the devices are collecting and how it is being used or shared."[362] Her colleague, FTC Commissioner Julie Brill, argues, "Manufacturers should deploy signals or consumer-friendly online dashboards that

[358] *See Data Security Made Simpler*, COUNCIL BETTER BUS. BUREAUS, http://www.bbb.org/data-security, *archived at* http://perma.cc/3Y9A-4JZA (last visited Dec. 19, 2014).

[359] *See Data Privacy for Small Businesses*, COUNCIL BETTER BUS. BUREAUS, http://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses, *archived at* http://perma.cc/6S36-JUWL (last visited Dec. 19, 2014).

[360] *See* TEACHPRIVACY, http://www.teachprivacy.com, *archived at* http://perma.cc/QM4K-KEV5 (last visited Dec. 19, 2014).

[361] *See* FUTURE OF PRIVACY FORUM, *supra* note 204, at 13 ("Transparency can also be vital to the development of the Internet of Things. Industry must ensure that consumers understand how they will benefit from the Internet of Things and see that measures are in place to promote consumer privacy and security.").

[362] Ramirez, *supra* note 248, at 4.

explain—through sounds, pictures, or graphs—the data the device collects about consumers, the uses of the data, and who else might see it."[363] On their websites, developers should also clearly disclose how the data their devices collect are retained, if at all, by the company, or who else such data might be shared with, if anyone.

- **Data transfer or data minimization:** Developers should also make it easier to transfer or delete data when users so request. Developers should also look to minimize or delete unnecessary datasets that could open future privacy or security vulnerabilities.
- **Ongoing security notices and updates:** Ongoing software updates will be essential to ensure that vulnerabilities are patched as quickly as possible so that IoT does not become "the hacker's new playground."[364]
- **Better security through encryption:** Encryption, anonymization, and data *de-identification*—a term that refers to "storing and sharing the data without revealing the identity of the individuals involved"[365]—will also be important, even if imperfect.[366]

[363] Julie Brill, Comm'r, U.S. Fed. Trade Comm'n, Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data, Address Before the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection and Competition in the Digital Age 9 (June 2, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf, *archived at* http://perma.cc/D9S7-URR4.

[364] Arik Hesseldahl, *The Internet of Things Is the Hackers' New Playground*, RE/CODE (July 29, 2014, 5:49 AM), http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/, *archived at* http://perma.cc/C5ZZ-8WTB.

[365] ANN CAVOUKIAN & DANIEL CASTRO, BIG DATA AND INNOVATION, SETTING THE RECORD STRAIGHT: DE-IDENTIFICATION DOES WORK 1 (June 16, 2014), *available at* http://www2.itif.org/2014-big-data-deidentification.pdf, *archived at* http://perma.cc/7TBK-KGPX.

[366] *See* Daniel C. Barth-Jones, *Does De-identification Work or Not?*, FIERCE BIG DATA (June 23, 2014), http://www.fiercebigdata.com/node/35502156, *archived at* http://perma.cc/AC68-2PXE; *see also* Arvind Narayanan & Edward W. Felten, No Silver Bullet: De-identification Still Doesn't Work 8 (July 9, 2014) (unpublished manuscript)

Why would developers adopt such best practices or codes of conduct voluntarily? Fear of legal liability and pressure from government officials are two possible explanations. But, in most cases, it comes down to good business. Many potential customers will care deeply about the privacy and security of their IoT and wearable devices and services.[367] "The signs are already beginning to appear," says Ann Cavoukian—who is widely credited with coining the term *privacy by design*—that "market leaders are embracing *Privacy by Design*, and are, in turn, reaping the benefits."[368]

[129] The last thing that developers want on their hands is consumer backlash or unwanted press attention because of failures related to privacy or data security.[369] Such failures could have profound consequences. "Not only should privacy protection be built in from the start, it also has to be communicated effectively to all stakeholders throughout the process," says David Hoffman, director of Intel's Security Policy and Global

(on file with author), *available at* http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf, *archived at* http://perma.cc/82Y8-MQW7.

[367] *See The Internet of Things (To Be Hacked)*, ECONOMIST, July 12, 2014, *available at* http://www.economist.com/news/leaders/21606829-hooking-up-gadgets-web-promises-huge-benefits-security-must-not-be, *archived at* http://perma.cc/3D4C-9369 ("Wrongdoers should be punished, but the best prompt for securing the internet of things is competition. Either tech firms will find ways to make web-connected gadgets more dependable, or people will decide they can live without them."); *see also* Larry Magid, *Safety, Security and Privacy Risks of Fitness Tracking and "Quantified Self,"* FORBES (July 31, 2014, 2:45 PM), http://www.forbes.com/sites/larrymagid/2014/07/31/safety-security-and-privacy-risks-of-fitness-tracking-and-quantified-self, *archived at* http://perma.cc/M69D-H25H.

[368] Ann Cavoukian, *2011: The Decade of Privacy by Design Starts Now*, ITBUSINESS (Jan. 15, 2011), http://blogs.itbusiness.ca/2011/01/2011-the-decade-of-privacy-by-design-starts-now, *archived at* http://perma.cc/439Y-V9QH.

[369] *See, e.g.*, Danny Yadron, *Corporate Boards Race to Shore Up Cybersecurity*, WALL ST. J. (June 29, 2014, 7:55 PM), http://online.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146, *archived at* http://perma.cc/Q2HQ-PCEZ.

Privacy Office.[370] "Failure to do so may incur financial implications," he believes.[371]

[130] In essence, self-regulation comes down to organizations' being good stewards of the information they gather and use.[372] Wittes and Bennett argue that this is "a relationship best seen as a form of trusteeship."[373]

> A user's entrusting his or her personal data to a company in exchange for a service, we shall argue, conveys certain obligations to the corporate custodians of that person's data: obligations to keep it secure, obligations to be candid and straightforward with users about how their data is being exploited, obligations not to materially misrepresent their uses of user data, and obligations not to use them in fashions injurious to or materially adverse to the users' interests without their explicit consent. These obligations show up in nearly all privacy codes, in patterns of government enforcement, and in the privacy policies of the largest internet companies.[374]

[370] Interview with David Hoffman, Dir., Intellectual Sec. Policy and Global and Privacy Office (May 23, 2014, 3:50 PM), *available at* http://www.darkreading.com/why-is-privacy-important-to-security-practitioners-and-professionals/a/d-id/1269187?, *archived at* http://perma.cc/T5V8-D2TP.

[371] *Id.*

[372] *See, e.g.*, Letter from Ken Wasch, *supra* note 208, at 8 ("[T]o maximize the opportunities presented by the Internet of Things and data-driven innovation, policies should take a more practical approach, shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability.").

[373] Wittes & Bennett, *supra* note 247, at 2.

[374] *Id.*

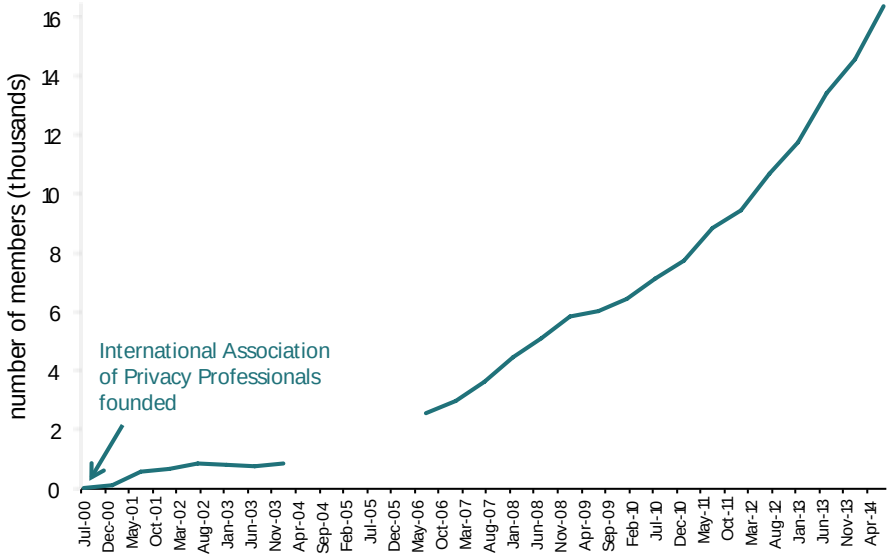
The rise of privacy and security professionals is having an important influence on how privacy and security by design work in practice today. Privacy professionals come in many flavors, with titles such as chief privacy officer, chief information officer, chief data officer, data architect, and data ethicist.[375] Daniel Solove notes that these privacy professionals "educate personnel to be mindful of privacy and influence software, product, and service design to be more privacy friendly. Privacy self-management thus has the salutary effect of creating beneficial structural privacy protections and accountability inside institutions."[376] Nothing better illustrates the growing role that these privacy professionals play today than the swelling membership ranks of the International Association of Privacy Professionals (IAPP), which trains and certifies privacy professionals. Membership in the IAPP, which was founded in 2000, grew to more than 15,000 by the end of 2013, up from 10,000 in March 2012 (see Figure 2).[377]

[375] *See* Brad Peters, *Meet the CDO*, FORBES (Dec. 20, 2013, 2:00 PM), http://www.forbes.com/sites/bradpeters/2013/12/20/meet-the-cdo, *archived at* http://perma.cc/KQ2E-FNVB.

[376] Solove, *supra* note 274, at 1900.

[377] *See* Omer Tene, *2013: The Year of Privacy*, INT'L ASS'N OF PRIVACY PROF'L (Dec. 19, 2013), https://privacyassociation.org/news/a/2013-the-year-of-privacy-2/, *archived at* https://perma.cc/DQ2Z-ZCRK.

Figure 2. The Explosion of Privacy Professionals: International Association of Privacy Professionals Membership, 2000–2014



Source: International Association of Privacy Professionals.
Note: Data for 2004 and 2005 are unavailable.

[131] The reason all this activity by privacy professionals is so important is that, as Berkeley Law School professors Kenneth A. Bamberger and Deirdre K. Mulligan note, it is increasingly what happens "on the ground"—that is, the day-to-day management of privacy decisions through the interaction of privacy professionals, engineers, outside experts, and regular users—that is perhaps most important for protecting consumers' privacy.[378] They suggest that "governing privacy through flexible principles" may be optimal, or at least more feasible, when compared to other regulatory efforts.[379] As more technology firms bring

[378] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249–50 (2011).

[379] *Id.* at 253.

on privacy and security professionals, this process of "baking in" best practices becomes more routine, and compliance becomes easier over time.

[132] Of course, as the FTC's Ohlhausen also observes, "self-regulation is not a perfect solution, nor can it be a complete substitute for traditional regulation."[380] She argues that "it's important that self-regulation is backed up by enforcement. . . . If a company makes a promise publicly and it doesn't adhere to that, we can bring an enforcement action."[381] In this regard, the FTC's important regulatory backstop role will be discussed later in this paper.

[133] Regardless of whether they will be enforced internally by firms or by ex post FTC enforcement actions, best practices must not become a heavy-handed, quasi-regulatory straitjacket. A focus on security and privacy by design does not mean those are the only values and design principles that developers should focus on when innovating. Cost, convenience, choice, and usability are all important values too. In fact, many consumers will prioritize those values over privacy and security—even as activists, academics, and policymakers simultaneously suggest that more should be done to address privacy and security concerns.

[134] Finally, best practices for privacy and security issues will need to evolve as social acceptance of various technologies and business practices evolve. For example, had "privacy by design" been interpreted strictly when wireless geolocation capabilities were first being developed, these technologies might have been shunned because of the privacy concerns they raised. With time, however, geolocation technologies have become a better understood and more widely accepted capability that consumers

[380] Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, *Success in Self-Regulation: Strategies to Bring to the Mobile and Global Era*, Speech at the BBB Self-Regulation Conference 4 (June 24, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/410391/140624bbbself-regulation.pdf, *archived at* http://perma.cc/JU7Y-TLAB.

[381] Bracy, *supra* note 349.

have come to expect will be embedded in many of their digital devices.[382] Those geolocation capabilities enable services that consumers now take for granted, such as instantaneous mapping services and real-time traffic updates.

[135] This is why flexibility is crucial when interpreting the privacy and security best practices.

C. Empowerment Solutions

[136] Although IoT innovation is occurring at a breakneck pace, it may nonetheless be possible that technological self-help solutions will emerge to help individuals and organizations better protect their privacy and security.[383] More robust, end-to-end encryption will certainly be a major part of the solution. As Gershenfeld and Vasseur conclude,

> [P]rivacy can be protected on the Internet of Things. Today, privacy on the rest of the Internet is safeguarded through cryptography, and it works: recent mass thefts of personal information have happened because firms failed to encrypt their customers' data, not because the hackers broke through strong protections. By extending cryptography down to the level of individual devices, the owners of those devices would gain a new kind of control over their personal information. Rather than maintaining secrecy as an absolute good, it could be priced based on the value of sharing. Users could set up a firewall to keep private the Internet traffic coming from the things in their homes—or they could share that data with, for example, a

[382] *See* Bambauer, *supra* note 243, at 238.

[383] *See generally* Kashmir Hill, *Forget Glass: Here Are Wearables That Protect Your Privacy*, FORBES (July 29, 2014, 11:20 AM), http://www.forbes.com/sites/kashmirhill/2014/07/29/forget-glass-here-are-wearables-that-protect-your-privacy, *archived at* http://perma.cc/EB62-6XQJ (describing different wearables that protect privacy).

> utility that gave a discount for their operating their dishwasher only during off-peak hours or a health insurance provider that offered lower rates in return for their making healthier lifestyle choices.[384]

Other creative solutions will likely emerge as problems develop. Roger A. Grimes, a security expert with Microsoft, argues that "what we need is device identity. In order for us to begin securing IoT, we have to be able to reliably authenticate devices and apply the appropriate security controls to those devices—and be able to identify misbehaving devices and remediate them."[385] "The real way to decrease Internet crime is to make it harder for the bad guys to get away with malicious hacking. Once the bad guys realize that they're likely to get caught—and those who get away with it don't make much money—Internet crime will decrease," he argues.[386]

[137] Better device authentication mechanisms could help address this. Computer scientists at the University of California, San Diego, recently announced the development of a tool that "tags critical pieces in a hardware's security system and tracks them."[387] This tool will help IoT developers and users detect security vulnerabilities that can compromise a device's security and address them before problems develop. "IoT isn't a frightening giant ogre," argues security consultant Jim O'Reilly, "[i]f we stop admiring how big it is and realize the devil is in the details, we should be able to handle IoT just fine."[388]

---

[384] Gershenfeld & Vasseur, *supra* note 18.

[385] Roger A. Grimes, *The Right Way to Secure The Internet of Things*, INFOWORLD (Apr. 15, 2014), http://www.infoworld.com/d/security/the-right-way-secure-the-internet-of-things-240486, *archived at* http://perma.cc/47EB-EFG5.

[386] *Id.*

[387] *Computer Scientists Develop Tool to Make the Internet of Things Safer*, PHYS.ORG (June 2, 2014), http://phys.org/news/2014-06-scientists-tool-internet-safer.html#jCp, *archived at* http://perma.cc/3C8E-Y7JK.

[138] An extensive array of privacy-enhancing technologies and consumer information is already available on the market today to help users block or limit data collection or help them achieve a more anonymous browsing experience.[389] Some of those tools can help users protect their privacy as they start using more IoT and wearable technologies.

[139] Other technological empowerment fixes will emerge spontaneously to address new IoT-related challenges as they develop. For example, *Wired* recently profiled a Berlin artist who wrote a simple program to detect any Google Glass device attempting to connect to a Wi-Fi network and alert those in the area that someone is using Glass nearby.[390] The program could even send a "deauthorization" command, cutting the Wi-Fi connection for the headset.[391]

[140] As noted next, firms have a powerful incentive to handle security concerns preemptively to avoid liability and negative press attention down the road. Industry consortia can help achieve security in a more collective fashion through best practices. For example, in early 2014, the Industrial Internet Consortium was established to "further the development, adoption, and wide-spread use of interconnected machines, intelligent

[388] Jim O'Reilly, *The Internet of Things: Not so Scary*, INFO. WEEK NETWORK COMPUTING (May 23, 2014, 7:00 AM), http://www.networkcomputing.com/wireless-infrastructure/the-internet-of-things-not-so-scary/a/d-id/1269152?, *archived at* http://perma.cc/NR9T-LU69.

[389] *See, e.g.*, *Privacy, Security, and Human Dignity*, *supra* note 244, at 440–46.

[390] *See* Andy Greenberg, *Cut Off Glassholes' Wi-Fi with This Google Glass Detector*, WIRED (June 3, 2014, 2:55 PM), http://www.wired.com/2014/06/find-and-ban-glassholes-with-this-artists-google-glass-detector, *archived at* http://perma.cc/WGL3-BEPW.

[391] *Id.*

analytics, and people at work,"[392] and "[b]uild confidence around new and innovative approaches to security."[393] Founding members include AT&T, Cisco, IBM, Intel, and General Electric.[394] As firms investigate and establish innovative approaches to security in web-connected industrial gear, eventually those best practices will be applied to consumer devices and systems as well.[395]

D. Common-Law Solutions, Evolving Liability Standards, and Other Legal Recourses

[141] Torts and other legal mechanisms will also continue to play a role in protecting privacy and data security.[396] Privacy torts evolved fairly recently compared to other common-law torts, but it is probable that—like other torts—they will continue to evolve in response to technological change and provide more avenues of recourse to plaintiffs seeking to protect their privacy rights.[397] The four privacy torts are public disclosure

[392] *Executive Summary*, INDUSTRIAL INTERNET CONSORTIUM 6–7, http://www.iiconsortium.org/docs/Industrial_Internet_Consortium-Introductory_White_Paper.pdf, *archived at* http://perma.cc/7PQW-MZLC (last visited Jan. 15, 2015).

[393] *The Industrial Internet Consortium™: A Global Nonprofit Partnership of Industry, Government and Academia*, INDUSTRIAL INTERNET CONSORTIUM, http://www.iiconsortium.org/about-us.htm, *archived at* http://perma.cc/3VRF-ZYAB (last visited Jan. 28, 2015).

[394] *See id.*

[395] *See, e.g.*, *Prevention Is Better Than Cure*, ECONOMIST, July 12, 2014, *available at* http://www.economist.com/news/special-report/21606424-more-vigilance-and-better-defences-can-make-cyberspace-lot-safer-prevention-better, *archived at* http://perma.cc/B44P-LK3V.

[396] *See, e.g.*, PRIVACILLA.ORG, *supra* note 280 at 2.

[397] *See, e.g.*, Bambauer, *supra* note 243, at 273 ("Tort law holds the solution to vexing problems in privacy law. Yet it has been neglected by privacy law scholars, who are on a misguided quest to constrain the quantity, spread, and repurposing of personal data. The

of private facts, intrusion upon seclusion, false light, and appropriation of name or likeness.[398]

[142] The tort of intrusion upon seclusion may evolve in response to some of the specific technological changes outlined in this paper and in the process provide additional remedies to perceived privacy harms.[399] This tort states, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[400] Cases flowing from this tort have dealt with involuntary exposure in public[401] and "overzealous" surveillance[402] activities, as well as entering a person's home under false pretenses and recording their activities.[403] It would not be surprising to see future privacy-related controversies give rise to more legal actions involving the tort of intrusion upon seclusion because, as Bambauer notes, it "offers the best theory to target legitimate privacy harms in the information age."[404]

extensive regulations they propose come into direct conflict with traditional American normative commitments to the free flow of information.").

[398] *See, e.g.*, PRIVACILLA.ORG, *supra* note 280, at 5–7.

[399] *See, e.g.*, Bambauer, *supra* note 243, at 275.

[400] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[401] *See, e.g.*, Daily Times Democrat v. Graham, 162 So. 2d 474, 476–78 (Ala. 1964).

[402] *See, e.g.*, Nader v. General Motors Corp., 255 N.E.2d 765, 770–71 (N.Y. 1970).

[403] *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245, 246–47 (9th Cir. 1971).

[404] Bambauer, *supra* note 243, at 205 ("The tort of intrusion upon seclusion offers the best theory to target legitimate privacy harms in the information age.").

[143] Other federal and state laws already exist that could address privacy concerns.[405] Property law already addresses trespass, and future court rulings could see property norms extended to cover new types of harms involving wearable technologies.[406] State Peeping Tom laws that prohibit peering into individual homes or even surreptitious spying in public also exist.[407] The Video Voyeurism Prevention Act imposes fines and even jail time on those who have an "intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy."[408] The Fair Credit Reporting Act also already offers consumers access and correction remedies for their credit records, and its provisions may apply to some of the records created through new IoT technologies.[409]

[144] Contract law can also act as a powerful deterrent to the misuse of IoT and wearable technologies, not only in the workplace, but in many other formal relationships. State officials—state attorneys general in

[405] *See, e.g.*, Micah Singleton, *Defining Privacy in the Age of Wearable Cameras*, KERNEL (Sept. 14, 2014), http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10248/glass-wearable-cameras-legal-privacy, *archived at* http://perma.cc/2UD7-WJ2S ("Perhaps, though, instead of a surge of new laws, we may witness current laws against recording people without consent enforced more actively, as wearables continue to get smaller and more advanced.").

[406] *See, e.g.*, Jim Harper, CATO Institute, Consumer Online Privacy, Remarks at the Committee on Commerce, Science, and Transportation (July 27, 2010), *available at* http://www.cato.org/publications/congressional-testimony/consumer-online-privacy, *archived at* http://perma.cc/7GVT-ZR4D ("Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within.").

[407] *See, e.g.*, VA. CODE ANN. § 18.2–130 (2014) (Peeping or spying into dwelling or enclosure).

[408] Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (2012).

[409] *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681, 1681n, 1681o (2012).

particular—also continue to push for new policies addressing privacy and data security, many of which are often more stringent than federal law.[410]

[145] Ironically, the fact that IoT and wearable technology developers may be collecting massive volumes of new data could open those developers up to new forms of liability. In the context of intelligent vehicle technology, for example, Bryant Walker Smith of Stanford Law School notes that liability norms will likely be affected by the level of knowledge and control that manufacturers have over those systems.[411] "A seller who can, does, or should know more about the products it sells may be expected to foresee a wider range of product-related uses, misuses, and harms," he argues.[412] In other words, as IoT and wearable technology application developers come to possess a greater volume of data about what users are doing with their devices and services, liability could expand over time for those developers.[413] These developers could become what economists refer to as the "least cost avoider" or the party who is in the

[410] *See, e.g.*, CHRISTOPHER WOLF, BUREAU OF NAT'L AFFAIRS, INC., TARGETED ENFORCEMENT AND SHARED LAWMAKING AUTHORITY AS CATALYSTS FOR DATA PROTECTION IN THE U.S., PRIVACY & SECURITY LAW REPORT 2 (2010), *available at* http://www.hldataprotection.com/uploads/file/PDFArtic.pdf, *archived at* http://perma.cc/V6SV-89W5 ("At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws . . . as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data.").

[411] *See* Bryant Walker Smith, *Proximity-Driven Liability*, 102 GEO. L.J. 1777, 1779 (2014).

[412] *Id.* at 1799.

[413] *See id.* ("Since a product use or misuse that should be known to the seller is likely to be foreseeable, this information can also expand the content of other duties.").

best position to minimize risk at the lowest cost.[414] Smith refers to this as "proximity-driven liability."[415]

[146] This observation will likely also be true for other smart systems as new legal standards and responsibilities evolve gradually through a body of common-law cases, as they have for many other technologies. Brookings Institution scholar John Villasenor notes that

> [W]hen confronted with new, often complex, questions involving products liability, courts have generally gotten things right. . . . Products liability law has been highly adaptive to the many new technologies that have emerged in recent decades, and it will be quite capable of adapting to emerging autonomous vehicle technologies as the need arises.[416]

Thus, instead of trying to micromanage the development of IoT technologies in an attempt to plan for every hypothetical risk scenario, policymakers should be patient while the common law evolves and liability norms adjust.[417] Traditionally, the common law has dealt with products liability and accident compensation in an evolutionary way through a variety of mechanisms, including strict liability, negligence, design defects law, failure to warn, and breach of warranty.[418] There is no

---

[414] STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 189 (Belknap Press of University of Harvard Press, 2004).

[415] *See generally* Smith, *supra* note 411, at 1779–80 (setting forth the general concept of "proximity-driven liability").

[416] John Villasenor, *Who Is at Fault When a Driverless Car Gets in an Accident?*, ATLANTIC (Apr. 25, 2014, 4:15 PM), http://www.theatlantic.com/business/archive/2014/04/who-is-at-fault-when-a-driverless-car-gets-in-an-accident/361250, *archived at* http://perma.cc/NWV9-2RWR.

[417] *See, e.g.*, *The Internet of Things (To Be Hacked)*, *supra* note 367 ("[Governments] should make clear that web-connected gadgets are covered by existing safety laws and existing product-liability regimes.").

reason to think that the common law will not adapt to new technological realities, including IoT and wearable technologies, especially since firms have powerful incentives to improve the security of their systems and avoid punishing liability, unwanted press attention, and lost customers.[419]

E. Federal Trade Commission Oversight and Enforcement

[147] The FTC has already played a major role in addressing concerns about privacy and security for today's leading online technologies. The agency has used its broad authority under section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[420] Section 5 gives the FTC remarkably broad authority to address alleged violations of data privacy and security standards. Bamberger and Mulligan note that "since 1996 the FTC has actively used its broad authority under section 5 . . . to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer

[418] *See* JOHN VILLASENOR, PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION 7–14 (2014), *available at* http://www.brookings.edu/research/papers/2014/04/products-liability-driverless-cars-villasenor, *archived at* http://perma.cc/UH34-9C4R.

[419] *See, e.g.*, Eli Dourado, *Internet Security Without Law: How Service Providers Create Order Online* 12–13 (Mercatus Center at George Mason Univ., Working Paper No. 12–19, 2012), *available at* http://mercatus.org/sites/default/files/ISP_Dourado_WP1219.pdf, *archived at* http://perma.cc/F2WB-A86U; *see also* Letter from William L. Kovacs, Senior Vice President, Env't, Tech. & Regulatory Affairs, to Donald S. Clark, Sec'y, Fed. Trade Comm'n 3 (Jan. 10, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00011-88248.pdf, *archived at* http://perma.cc/RNF7-U8MD ("In this tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Successful companies work to ensure that their products and services are deemed trustworthy by their customers. If a company has failed to meet customers' privacy and security expectations, then oftentimes the marketplace and public relations consequences will be swift and decisive, forcing the company to quickly align its business practices with consumer expectations.").

[420] 15 U.S.C. § 45(a) (2012).

information, to bringing enforcement actions challenging information practices alleged to cause consumer injury."[421]

[148] In recent years, for example, the FTC has brought privacy-related and data-security-oriented enforcement actions against a wide variety of information technology companies, including Google,[422] Facebook,[423] Apple,[424] Twitter,[425] MySpace,[426] HTC,[427] Lookout,[428] Path,[429]

[421] Bamberger & Mulligan, *supra* note 378, at 273.

[422] *See, e.g.*, Complaint at 5–6, *In re* Google Inc., No. C–4336 (F.T.C. Oct. 16, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf, *archived at* http://perma.cc/EK5G-ALX7; *see also* Alex Howard, *Google Reaches Agreement with FTC on Buzz Privacy Concerns*, GOVFRESH (Mar. 30, 2011), https://web.archive.org/web/20130502214829/http://gov20.govfresh.com/google-reaches-agreement-with-ftc-on-buzz-privacy-concerns/, *archived at* https://perma.cc/E9TA-8YEH.

[423] *See, e.g.*, Complaint at 6–7, 9–11, 14–17, *In re* Facebook, Inc., No. C–4365 (F.T.C. July 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf, *archived at* http://perma.cc/3D8V-JRR7; *see also* Brent Kendall, *Facebook Reaches Settlement with FTC on Privacy Issues*, WALL ST. J. (Nov. 29, 2011, 1:29 PM), *available at* http://online.wsj.com/article/BT-CO-20111129-710865.html, *archived at* http://perma.cc/5STF-7CGS.

[424] *See, e.g.*, Press Release, F.T.C., Apple Inc. Will Provide Full Consumer Refunds of at Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million, *archived at* http://perma.cc/KZ9Q-6XPH.

[425] *See, e.g.*, Complaint at 5, *In re* Twitter, Inc., No. C–4316 (F.T.C. Mar. 2, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf, *archived at* http://perma.cc/SPT8-EGAT.

[426] *See, e.g.*, Complaint at 5–6, *In re* Myspace L.L.C., No. C–4369 (F.T.C. Aug. 30, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf, *archived at* http://perma.cc/6SD6-XTK8.

Snapchat,[430] Fandango,[431] and Credit Karma,[432] among many others.[433] In testimony delivered in May 2014, an FTC official noted that it had pursued 53 data-security-related cases, which "examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic."[434]

---

[427] *See, e.g.*, Complaint at 2, *In re* HTC America Inc., No. C–4406 (F.T.C. Mar. 2, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf, *archived at* http://perma.cc/85GJ-T98B.

[428] *See, e.g.*, Complaint at 2–4, Lookout Services, Inc., No. C–4326 (F.T.C. June 15, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615lookoutcmpt.pdf, *archived at* http://perma.cc/YMT2-ZK4B.

[429] *See, e.g.*, Complaint at 1–2, 8–9, Path, Inc., No. C–130448 (N.D. Cal. Jan. 31, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf, *archived at* http://perma.cc/XST3-WXN5.

[430] *See, e.g.*, Complaint at 4–8, *In re* Snapchat, Inc., No. 132 3078 (F.T.C. May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf, *archived at* http://perma.cc/3J9B-53NS.

[431] *See, e.g.*, Complaint at 3–4, *In re* Fandango, L.L.C., No. C–4481 (F.T.C. Aug. 19, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf, *archived at* http://perma.cc/LQM9-PHBD.

[432] *See, e.g.*, Complaint at 3–5, *In re* Credit Karma, Inc., No. C–4480 (F.T.C. Aug. 13, 2014), http://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf, *archived at* http://perma.cc/H5KF-VYV6.

[433] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 610 (2014) (stating that the FTC has issued over 170 privacy-related complaints).

[434] Maneesha Mithal, Assoc. Dir. of the Div. of Privacy and Identity Prot., Fed. Trade Comm'n, Statement of the Federal Trade Commission on Emerging Threats in the Online Advertising Industry Before the S. Comm. on Homeland Sec. and Governmental Affairs Permanent Subcomm. on Investigations (May 15, 2014), *available at*

[149] Companies fear such FTC enforcement actions because they can bind a company to lengthy, twenty-year privacy audits[435] and open it up to potential liability of up to $16,000 per customer harmed per violation.[436] Moreover, firms take a reputation hit with the press and the general public when such enforcement actions are handed down.

[150] Leading privacy scholars have argued that "the principles that emerge from FTC privacy 'common law' [demonstrate] that the FTC's privacy jurisprudence is quite thick."[437] At a minimum, these enforcement actions make it clear that the agency already possesses plenary authority under section 5 to "make sure companies live up to the privacy promises they make to consumers."[438]

[151] The agency has also released industry best-practice guidance for mobile app data collection and privacy practices,[439] digital advertising

http://www.ftc.gov/system/files/documents/public_statements/309891/140515emergingthreatsonline.pdf, *archived at* http://perma.cc/ZZ7S-FR4R.

[435] *See* Kashmir Hill, *So, What Are These Privacy Audits That Google and Facebook Have to Do for the Next 20 Years?*, FORBES (Nov. 30, 2011, 2:29 PM), http://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years, *archived at* http://perma.cc/NVP8-EDTN.

[436] *See* Daniel J. Solove & Woodrow Hartzog, Snapchat and FTC Privacy and Security Consent Orders, LINKEDIN (May 12, 2014), https://www.linkedin.com/today/post/article/20140512053224-2259773-the-anatomy-of-an-ftc-privacy-and-data-security-consent-order, *archived at* https://perma.cc/6QCL-EPC6.

[437] Solove & Hartzog, *supra* note 433, at 583*; see also* WOLF, *supra* note 410, at 3.

[438] Press Release, Fed.Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived, *archived at* http://perma.cc/KNF8-NWTJ.

disclosures,[440] facial recognition technologies,[441] and other things that may be relevant to IoT and wearable technologies. It is likely that the agency will continue to actively monitor this marketplace to ensure that privacy and data security remain top priorities.[442] In fact, the FTC has already brought an enforcement action against TRENDnet, a maker of Internet-connected home video cameras, for "lax security practices [that] exposed the private lives of hundreds of consumers to public viewing on the Internet."[443]

[152] Importantly, however, the FTC has acknowledged limits to its enforcement powers. "Through these settlements, the Commission has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect

[439] *See* Press Release, Fed.Trade Comm'n, FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles (Sept. 5, 2012), http://www.ftc.gov/opa/2012/09/mobileapps.shtm, *archived at* http://perma.cc/3VUH-PJUZ.

[440] *See* FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING i (2013), *available at* http://www.ftc.gov/os/2013/03/130312dotcomdisclosures.pdf, *archived at* http://perma.cc/YR2L-9W2J.

[441] *See* Press Release, Fed. Trade Comm'n, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), *available at* http://www.ftc.gov/opa/2012/10/facialrecognition.shtm, *archived at* http://perma.cc/2CYT-PDN3.

[442] *See FTC Enters "Internet of Things" Arena with TRENDnet Proposed Settlement*, INFORMATION LAW GROUP (Sept. 9, 2013), http://www.infolawgroup.com/2013/09/articles/ftc/trendnet-settlement, *archived at* http://perma.cc/AK2W-KJJB.

[443] Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' *Privacy* (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles, *archived at* http://perma.cc/KEX3-Y6E4.

security; and that the mere fact that a breach occurred does not mean that a company has violated the law."[444] Such enforcement constraint and flexibility will be essential if IoT and wearable technologies are to realize their full potential.

F. Social Norms, Pressure, and Sanctions

[153] Norms—"social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done"[445]—can play a powerful role in curbing potentially problematic behavior by both the developers of IoT and its users. Indeed, the power of social norms in this context could become a crucial determinant of the popularity of many wearable technologies.

[154] Sometimes cultural norms, public pressure, and spontaneous social sanctions form a far more powerful "regulator" of innovations and how people use new tools than do laws and regulations.[446] Cristina Bicchieri, a leading behavioral ethicist, calls social norms "the grammar of society" because,

> [L]ike a collection of linguistic rules that are implicit in a language and define it, social norms are implicit in the operations of a society and make it what it is. Like a grammar, a system of norms specifies what is acceptable and what is not in a social group. And analogously to a grammar, a system of norms is not the product of human design and planning.[447]

[444] Mithal, *supra* note 434, at 12.

[445] Cass Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 914 (1996).

[446] PERMISSIONLESS INNOVATION, *supra* note 7, at 57–58.

[447] CRISTINA BICCHIERI, *Preface to* The GRAMMAR OF SOCIETY: THE NATURE AND DYNAMICS OF SOCIAL NORMS ix (Cambridge Univ. Press 2006).

Indeed, social pressure and constraints on the use and misuse of technology often develop in an organic, bottom-up fashion. For example, social norms continue to evolve to deal with smartphone usage in various environments, such as in some restaurants, most movie theaters, and gym locker rooms, where their use is frowned upon or actively discouraged. In some cases, social norms and constraints take the form of formal restrictions imposed by establishments themselves. Other times, however, social pressure develops more spontaneously from other people in the vicinity. For example, theaters use preshow messaging to pressure patrons to mute or turn off electronic devices, but other moviegoers are equally likely to make their displeasure with interruptions known to offending parties. Likewise, some passenger trains include "quiet cars," where phone conversations are prohibited, and other riders often scold passengers who ignore those rules.[448] Finally, while fitness centers often post signs disallowing the use of smartphones in locker rooms, anyone attempting to use them to take pictures would likely quickly meet the wrath of offended patrons.

[155] In a similar way, it is likely that social norms and pressures will influence the development and use of wearable computing technologies, such as Google Glass and other wearable devices.[449] "I can imagine social norms emerging on when it's appropriate to wear a camera, and when it isn't appropriate," says privacy lawyer Kurt Wimmer.[450] Advice columns are already being written about "Google Glass etiquette." Their recommendations include taking Google Glass off when first meeting

[448] *See, e.g.*, Vincent M. Mallozzi, *On Train, a Fight Between Silent and Merely Quiet*, N.Y. TIMES, Jan. 10, 2011, at A17, *available at* http://www.nytimes.com/2011/01/10/nyregion/10quiet.html, *archived at* http://perma.cc/3G59-3RQW.

[449] *See, e.g.*, Jared Newman, *The Real Privacy Implications of Google Glass*, TIME, (May 2, 2013,) http://techland.time.com/2013/05/02/the-real-privacy-implications-of-google-glass, *archived at* http://perma.cc/RR93-TWWA.

[450] *See, e.g.*, Singleton, *supra* note 405.

someone; removing it immediately when others seem uncomfortable; and never wearing it in bathrooms or other highly private settings.[451]

[156] More forceful opposition to Google Glass and other wearable computing or recording devices may develop in the future. Stop the Cyborgs is an advocacy group that offers various resources to push back against these technologies, including free downloadable "Google Glass ban signs" that can be displayed in places where such technologies may not be welcome.[452] The group also offers stickers and shirts that convey the same message.

[157] In the extreme, social sanction can sometimes even involve violence or the threat thereof. For example, in February 2014, a woman who wore Google Glass into a San Francisco bar was verbally and physically assaulted by a man who was upset about potentially having his privacy invaded.[453] It would be extremely unfortunate if tensions over wearable technologies resulted in violent altercations, but these early incidents may have the salubrious side effect of reminding users that not

[451] *See, e.g.*, Jedidiah Bracy, *Putting Google Glass on Ann Landers*, INT'L ASS'N OF PRIVACY PROF'L (Feb. 28, 2014), https://www.privacyassociation.org/privacy_perspectives/post/what_happens_when_ann_landers_puts_on_google_glass, *archived at* https://perma.cc/3KZB-FHDE; *see also* Rebecca Greenfield, *The First Rule of Google Glass Etiquette*, WIRE (May 6, 2013, 1:34 PM), http://www.theatlanticwire.com/technology/2013/05/google-glass-etiquette/64916, *archived at* http://perma.cc/2GNE-DQ88; Ryan Singel, *Devising a Personal Google Glass Privacy Policy*, MEDIUM (May 13, 2013), https://medium.com/future-participle/2334fecda87e, *archived at* https://perma.cc/K97R-AXDJ; Kevin Sintumuang, *Google Glass: An Etiquette Guide*, WALL ST. J., (May 3, 2013, 5:59 PM), http://online.wsj.com/article/SB10001424127887323982704578453031054200120.html, *archived at* http://perma.cc/H5DA-9VWW.

[452] *More . . . ,* STOP THE CYBORGS, http://stopthecyborgs.org/about, *archived at* http://perma.cc/AR8K-2LEN (last visited Dec. 7, 2014).

[453] *See* Jessica Guynn, *Clash over Google Glass Shows Hurdles Facing Wearable Tech*, L.A. TIMES, (Feb. 27, 2014), http://articles.latimes.com/2014/feb/27/business/la-fi-google-glass-attack-20140228, *archived at* http://perma.cc/T5YY-M6KL.

everyone shares their privacy values and that public uses of wearable technologies should be moderated accordingly.[454]

[158] Social norms and pressure can also be applied at the developer level to influence design choices. The behavior of developers of IoT and wearable technology will likely be influenced by the pressure applied by the broad and growing collection of privacy watchdog groups that exist, including the American Civil Liberties Union (ACLU), the Center for Democracy and Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, the Future of Privacy Forum, Privacy Rights Clearinghouse, and many others.[455] These advocacy groups have developed websites and materials to better inform consumers about how they can protect their privacy.[456] Such organizations agitate for more rigorous privacy protections incessantly, and privacy policies—both legal enactments and informal corporate standards—will continue to be significantly influenced by the pressure that these advocates exert on the process. Furthermore, there has been an explosion of academic interest in privacy-related matters in recent years, and this too influences developer behavior.

[159] Finally, media attention also plays an important role in curbing potentially problematic behavior—by individuals and developers alike. FTC Chairwoman Ramirez notes that

> [M]edia organizations . . . have a vital role to play as well. In recent years, premier news organizations have paid increasing attention to consumer privacy issues, publicizing excesses in some data gathering methods. Such public

[454] *See, e.g.*, Andrew Leonard, *Glasshole Nation: Tech's Culture War Takes Another Ugly Turn*, SALON (Feb. 28, 2014, 7:43 AM), http://www.salon.com/2014/02/28/glasshole_nation_techs_culture_war_takes_another_ugly_turn, *archived at* http://perma.cc/66TU-EZGY.

[455] *See Precautionary Principle*, *supra* note 282, at 483–84.

[456] *See Privacy, Security, and Human Dignity*, *supra* note 244, at 439.

> scrutiny gives firms a powerful incentive to act as responsible stewards of consumer information.[457]

There already exists intense media and blogger interest in the privacy and security-related implications of IoT and wearable technologies, and that coverage will likely grow as these devices and services multiply.

G. Law Enforcement Guidelines and Restrictions

[160] The use of wearable technologies by law enforcement officials—or law enforcement's ability to tap into private data flow from wearable devices—deserves special scrutiny and additional legal protections for the public. There are significant differences between public and private entities, and policymakers should continue to distinguish between them when considering data collection policies.[458] Private entities cannot fine, tax, or imprison people because they lack the coercive powers that governments possess. Moreover, although it is possible to ignore or refuse to be a part of various private services, the same is not true for governments, whose grasp cannot be evaded. Thus, special protections regarding wearables, IoT devices, and data flows are needed for law enforcement agencies and officials.

[161] The ACLU has developed a set of best practices for law enforcement use of "body cams" or "cop cams," which can be used to record an officer's interactions with the public.[459] The ACLU suggests,

---

[457] Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Protecting Consumer Privacy in a Big Data Age, Speech at the Media Institute, Washington, D.C. 12 (May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/308421/140508mediainstitute.pdf, *archived at* http://perma.cc/L282-DQPA.

[458] *See* Adam Thierer, *Do We Need a Constitutional Amendment Restricting Private-Sector Data Collection?*, INT'L ASS'N OF PRIVACY PROF'L (Jan. 23, 2014), https://privacyassociation.org/news/a/do-we-need-a-constitutional-amendment-restricting-private-sector-data-colle/, *archived at* https://perma.cc/8H66-6Z5S.

among other things, that citizens be notified that they are being recorded, that data "be retained no longer than necessary for the purpose for which it was collected," and "that this technology not become a backdoor for any kind of systematic surveillance or tracking of the public."[460]

[162] When government seeks access to privately held data collected from wearables or other IoT technologies, strong constitutional and statutory protections should apply. Privacy advocates fear that "the government will inevitably demand access" to any private data that is collected for commercial purposes,[461] but to the extent that this is a growing problem, those advocates should redouble their efforts to constrain government surveillance powers and the ability to indiscriminately suck up privately held data. Congress should reform the Electronic Communications Privacy Act of 1986 (the primary federal statute that governs when law enforcement agencies may compel private entities to divulge information held on behalf of third-party subscribers) to require the government to obtain a warrant issued upon a showing of probable cause before accessing the privately held data and communications.[462] Also, courts should revisit the "third-party doctrine,"[463] which holds that individuals sacrifice their Fourth

[459] Adi Robertson, *The ACLU Wants Police Officers to Wear Cameras, But Only With Privacy Protections*, THE VERGE (Oct. 9, 2013, 2:09 PM), http://www.theverge.com/2013/10/9/4820600/aclu-issues-guidelines-for-police-officer-cameras, *archived at* http://perma.cc/9JPG-EQCM.

[460] JAY STANLEY, POLICE BODY-MOUNTED CAMERAS: WITH RIGHT POLICIES IN PLACE, A WIN FOR ALL 4–5 (2013), *available at* https://www.aclu.org/files/assets/police_body-mounted_cameras.pdf, *archived at* https://perma.cc/KZ78-PFQL.

[461] Jeffrey Rosen, Op-Ed., *Madison's Privacy Blind Spot*, N.Y. TIMES, Jan. 19, 2014, at SR5, *available at* http://www.nytimes.com/2014/01/19/opinion/sunday/madisons-privacy-blind-spot.html?_r=0, *archived at* http://perma.cc/SBJ5-M4WB.

[462] *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 129–30, 154 (2011).

[463] Babak Siavoshy, *Need an Alternative to the Third Party Doctrine? Look Backwards, Not Forward (Part I)*, CONCURRING OPINIONS (July 7, 2014),

Amendment interest in their personal information when they divulge it to a third party, even if that party has promised to safeguard that data.[464] Other bolstered Fourth Amendment constraints on national security and law enforcement powers are also essential.[465] Again, because governments have unique powers and responsibilities, they qualify for a different level of legal scrutiny.

VII. CONCLUSION

[163] The privacy and security-related challenges associated with IoT and wearable technologies will be considerable, but it is essential that experimentation and innovation in this space not be derailed on the basis of speculation about hypothetical worst-case scenarios. Profound benefits will be associated with these new technologies, but those benefits may not come about if preemptive, precautionary policy interventions limit new innovation opportunities.

[164] Nevertheless, the public should not turn a blind eye to the challenges raised by these new developments, because "the Internet of things is not only a technological revolution, but also social revolution."[466]

---

http://www.concurringopinions.com/archives/2014/07/need-an-alternative-to-the-third-party-doctrine-look-backward-not-forward.html, *archived at* http://perma.cc/TD9Z-PEPD.

[464] *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV., 1381, 1401–02 (2008), *available at* http://www.wcl.american.edu/journal/lawrev/57/harper.pdf, *archived at* http://perma.cc/BUU7-NWQT (citing *United States v. Miller*, 425 U.S. 435, 440 (1976)).

[465] *See* James X. Dempsey, Vice President, Ctr. for Democracy & Tech., The Path to ECPA Reform and the Implications of United States v. Jones, Keynote Address at the University of San Frisco Law Review Symposium (Feb. 24, 2012), *in* 47 U.S.F.L. REV. 225, 226 n.5, 241–44 (2012).

[466] *The Philosophy of IoT: Will It Help or Hurt?*, *PC-100* (May 26, 2014), http://www.pc-100.com/the-philosophy-of-iot-will-it-help-or-hurt/, *archived at* http://perma.cc/UR2B-MSBP (quoting Justin McKeown, head of the program for Fine Art and Computer Science at York St. John).

As these technologies become (sometimes literally) woven into the fabric of consumers' lives, they will spawn social disruptions that deserve careful consideration and constructive solutions.[467] This paper has offered a framework for accomplishing that goal without derailing innovative efforts that could yield countless life-enriching applications and opportunities.

[165] To the extent that some public policy responses are needed to guide technological developments, simple legal principles are greatly preferable to technology-specific, micromanaged regulatory regimes. *Ex ante* (preemptive and precautionary) regulation is often highly inefficient, even to the extent of being dangerous. Prospective regulation based on speculation about future harms that may never materialize is likely to come at the expense of innovation and growth opportunities. When corrective actions are needed to address more serious harms, ex post measures—especially via common-law actions and FTC enforcement activities—will generally be more sensible.

[166] Using such a balanced, layered approach to privacy and security concerns will ensure that those important values can be protected without derailing the many beneficial forms of economic and social innovation that could flow from IoT and wearable technologies.

[467] *See* Langley, *supra* note 180 (quoting Simon Randall of wearable camera maker Autographer) ("I think in 10 years' time it'll be pretty easy to put a wafer level camera in a lapel—if you wanted to.").