MERCATUS CENTER
George Mason University

Statement for the Record

Adam Thierer
Senior Research Fellow, Technology Policy Program
Mercatus Center at George Mason University

March 3, 2016

House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade
Hearing: “Disrupter Series: Wearable Devices”

Mr. Chairman and members of the Committee, thank you for this opportunity to submit a statement for the record on wearable devices. 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.

My statement will address how wearable technologies will impact economic growth, how policymakers should approach wearable technologies, and how cybersecurity and privacy concerns should be addressed. Wearable technologies, or “wearables,” are a significant subset of my broader research on the “Internet of Things” or “IoT.” Appended to this statement are two documents. The first is a compendium of reports on the economic impact of the IoT and wearables that I coauthored with Andrea Castillo, and the second is a *Reason* article, “Uncle Sam Wants My FitBit,” further summarizing my perspective on the regulation and economic impact of wearables.

The projected number of Internet-connected devices, including wearables, is projected to grow by an amount anywhere from 19 billion devices to 40 billion devices by 2019. The global productivity gains from connected devices, including wearables, is expected to be between $2.3 trillion and $11.6 trillion over the next decade. In the healthcare sector alone, of which wearables perhaps most directly apply, the cost savings and productivity gains are calculated to be between $1.1 trillion and $2.5 trillion by 2025.

The topic of today’s hearing is important in broader policy discussions about the IoT because wearables, as we write in our appended paper, “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.”

If America hopes to be a global leader in wearable technologies, as it has been for the Internet more generally over the past two decades, then the country first has to get public policy right. America took a commanding lead in the digital economy because, in the mid-1990s, Congress and the Clinton administration crafted a nonpartisan vision for the Internet that protected "permissionless innovation"—the idea that experimentation with new technologies and business models should generally be permitted without prior approval.

The first order of business for policymakers is to send a green light to entrepreneurs communicating that our nation's default policy position remains "innovation allowed." Second, policymakers should avoid basing policy interventions on hypothetical worst-case scenarios—or else best-case scenarios will never come about. Our policy regime, therefore, should be responsive, not anticipatory.

Of course, there exist privacy- and security-related challenges that deserve attention. Data is going to be moving fluidly across so many platforms and devices that it will be difficult to apply traditional Fair Information Practice Principles in a rigid regulatory fashion for every conceivable use of these technologies.

Specifically, it will be challenging to achieve perfect "notice and choice" in a world where so many devices are capturing volumes of data in real time. Moreover, while "data minimization" remains a worthy goal, if it is mandated in a one-size-fits-all fashion, it could limit many life-enriching innovations.

Law will still play a role, but we're going to need new approaches.

- Policymakers can encourage privacy and security "by design" for wearable technology developers, but those best practices should not be mandated as top-down controls. Flexibility is essential.
- More privacy-enhancing tools—especially robust encryption technologies—will also help, and government officials would be wise to promote these tools instead of restricting them.
- Increased education is also essential, and governments can help get the word out about inappropriate uses of these technologies.
- Existing privacy torts and existing targeted rules (such as Peeping Tom laws) will also likely evolve to address serious harms as they develop.
- Finally, the Federal Trade Commission will continue to play an important backstop role, using its section 5 authority to police "unfair and deceptive" practices. The commission has already been remarkably active in encouraging companies to live up to the privacy and security promises they make to their consumers, and that will continue.

Thank you for the opportunity to submit this statement for the record. Policymakers should remain patient and continue to embrace permissionless innovation to ensure that wearable technologies thrive and American consumers and companies continue to be global leaders in the digital economy.

Sincerely,

Adam Thierer

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

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

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

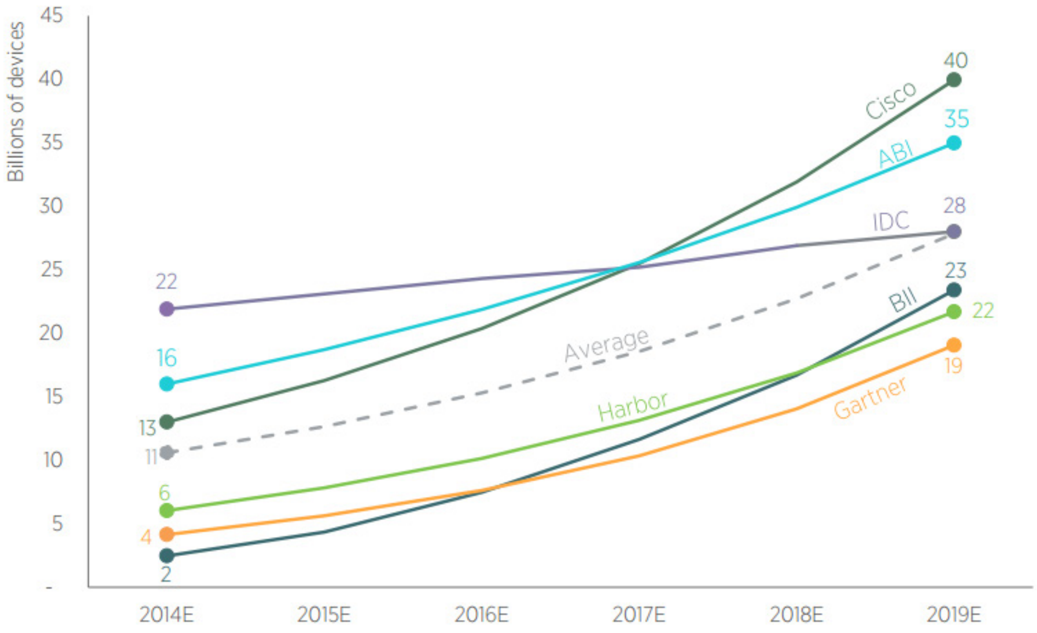
Adam Thierer and Ryan Hagemann of the Mercatus Center at George Mason University predict that networked vehicles and aircraft equipped with sensors, wireless communication, and dynamic programming will make unmanned transportation widely available and generate considerable benefits for consumers and 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.

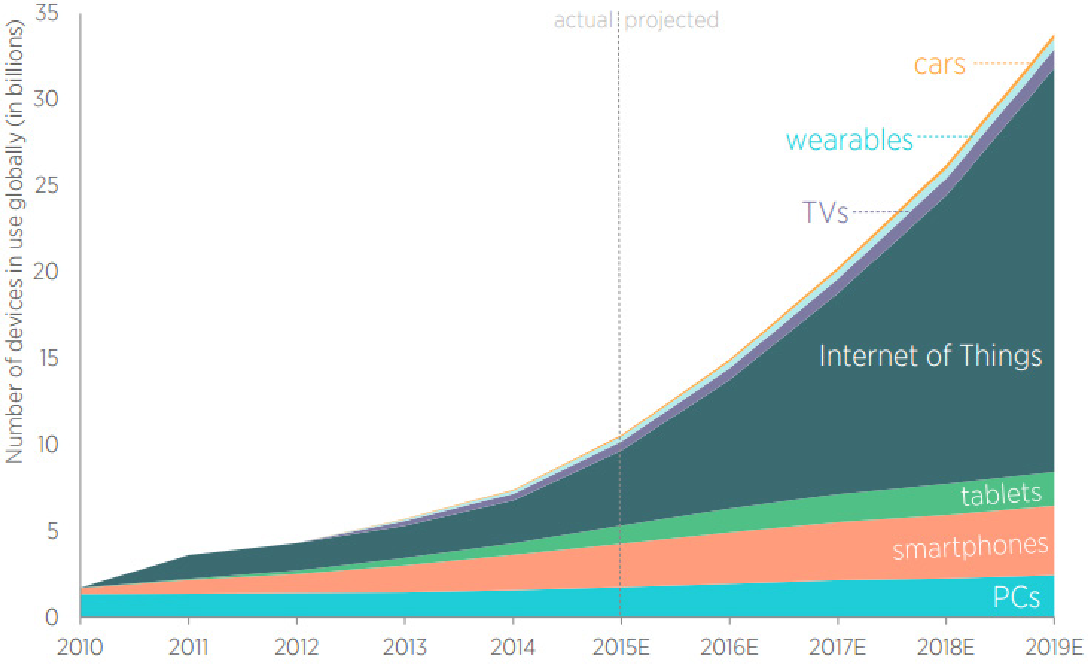
Harbor projects that 21.7 billion IoT devices will be connected and in use by 2019.

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

Uncle Sam Wants Your Fitbit

The fight for Internet freedom gets physical.

Adam Thierer | Apr. 9, 2015 9:00 am

We are at the dawn of the Internet of Things—a world full of smart devices equipped with sensors, all hooked up to a digital universe that will become as omnipresent as the air we breathe. Imagine every appliance in your home, every machine in your office, and every device in your car constantly communicating with a network and offering you a fully customizable, personalized experience. Besides neato gadgets and productivity gains, this hyper-connected future will also mean a new wave of policy wars, as politicians panic over privacy, security, intellectual property, occupational disruptions, technical standards, and more.

Behind these battles will be a grander clash of visions over the future course of technology. The initial boom of digital entrepreneurship was powered by largely unfettered experiments with new technologies and business models. Will we preserve and extend this ethos going forward? Or will technological reactionaries pre-emptively eliminate every hypothetical risk posed by the next generation of Internet-enabled things, perhaps regulating them out of existence before they even come to be?

Web Wars

The first generation of Internet policy punditry was dominated by voices declaring that the world of bits was, or at least should be, a unique space with a different set of rules than the world of atoms. Digital visionary John Perry Barlow set the tone with his famous 1996 essay, "A Declaration of the Independence of Cyberspace," which argued not just that governments should leave the Internet unregulated but that Internet regulation was not really feasible in the first place.

Barlow's vision thus embodied both *Internet exceptionalism* and *technological determinism*. Internet exceptionalism is the notion that the Net is a special medium that shouldn't be treated like earlier media and communications platforms, such as broadcasting or telephony. Technological determinism is the belief that technology drives history, and (in the extreme version) that it almost has an unstoppable will of its own.

First-generation exceptionalists and determinists included Nicholas Negroponte, the former director of the MIT Media Lab, and George Gilder, a technology journalist and historian. "Like a force of nature, the digital age cannot be denied or stopped," Negroponte insisted in his 1995 polemic, *Being Digital*. But Barlow's declaration represented the high-water mark of the early exceptionalist era. "Governments of the Industrial World," he declared, "are not welcome among us [and] have no sovereignty where we gather." The "global social space we are building," he added, is "naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."

It turned out we had reasons to fear after all. If the first era of Internet policy signified *A New Hope*, the second generation—beginning about the time the dot-com bubble burst in 2000—could be called *The Empire Strikes Back*. From taxes to surveillance to network regulation, governments gradually learned that by applying enough pressure in just the right places, citizens and organizations will submit.

A second generation of Internet scholars cheered on these developments. The scholar-activists at Harvard's Berkman Center for Internet and Society, such as Lawrence Lessig, Jonathan Zittrain, and Tim Wu, joined with a growing assortment of policy activists with tangential pet peeves they wanted governments to address. Together they revolted against the earlier ethos and called for stronger powers for governments to direct social and commercial activities online.

Mark Rightmire / The Orange County Register / ZUMAPRESS.com

In the new narrative, the real threat to our freedom was not public law but private code. "Left to itself," Lessig famously predicted, "cyberspace will become a perfect tool of control." Thus, government controls were called for. Later, Wu would advocate a forcible disintegration of the information economy via a "separations principle" that would segregate information providers into three buckets—creators, distributors, and hardware makers—and force them to stay put. All in the name of keeping us safe from "information monopolies."

Spurred on by this crowd, governments across the globe are clamoring for even greater control over people in cyberspace. But the second generation's narrative has proved overly simplistic in two ways.

First, the exceptionalists and techno-determinists were partially right—the Internet, while not being unregulatable per se, really has proven more resistant to government control than analog-era communications systems. The combination of highly decentralized networks, a global scale, empowered end-users, and the unprecedented volume of information created in the process has created formidable enforcement challenges for would-be censors and economic regulators.

With each passing year, the gap between "Internet time" and "government time" is widening. As the technology analyst Larry Downes argued in his 2009 book *The Laws of Disruption*, information-age "technology changes exponentially, but social, economic, and legal systems change incrementally." His examples ranged from copyright law, where bottling up published works is growing harder, to online privacy, where personal information is flowing faster than the ability of the law to control it.

This leads to the second way in which the *Empire Strikes Back* narrative falls short. As the Internet changes the way people connect with one another, governments have had to change the way they try to impose their wills on the rest of us. The old command-and-control models just don't work on highly distributed and decentralized networks.

Consider regulation of speech. Outright censorship has proven extremely difficult to enforce, and not just in the United States, where we have a First Amendment keeping the police at bay. Although some atavistic regimes still try to clamp down on content and communications, most attempt to shape behavior by encouraging firms and organizations to adopt recommended codes of conduct for online speech, often in the name of protecting children.

A similar phenomenon is at play for data privacy and cybersecurity policy. While some comprehensive regulatory frameworks have been floated, the conversations are shifting toward alternative methods of encouraging compliance. Many governments are choosing the softer road of encouraging codes of conduct and "best practices."

Economic regulations have evolved, too. Price and entry controls are almost never suggested as a first-order solution to concerns over market concentration. Instead of hard-nosed, top-down diktats, governments are increasingly using "nudges," convening "multistakeholder" meetings and workshops, and deploying what Tim Wu calls "agency threats." The Obama administration's Commerce Department and Federal Trade Commission (FTC) have already used this approach in their attempts to influence "big data" collection, biometrics, online advertising, mobile app development, and other emerging sectors and technologies.

Think of it as a "soft power" approach to tech policy: Policy makers dangle a regulatory Sword of Damocles over the heads of Internet innovators and subtly threaten them with vague penalties—or at least a lot of bad press—if they don't fall into line. The sword doesn't always have to fall to be effective; the fact that it's hanging there is enough to intimidate many firms into doing what regulators want. It's similar to the approach that the Food and Drug Administration has employed for decades with many food or medical device manufacturers: constantly harping on them about how to better develop their products, often without ever implementing formal regulations clarifying exactly how to do so.

That's how policy makers are already approaching the Internet of Things, too.

Why Matter Matters

It may feel like the Internet is already a ubiquitous backdrop of our existence, but "getting online" still requires a conscious effort to sit in front of a computer or grab a smartphone and then take steps to connect with specific sites and services. The Net does not have a completely seamless, visceral presence in our everyday lives. Yet.

The Internet of Things can change that, ushering in an era of ambient computing, always-on connectivity, and fully customizable, personalized services. Wearable health and fitness devices like Fitbit and Jawbone are already popular, foreshadowing a future in which these devices become "lifestyle remotes" that help consumers control or automate many other systems around them-in their homes, offices, cars, and so on.

Nest, recently acquired by Google, is already giving homeowners the ability to better manage their homes' energy use and to do so remotely. It signals the arrival of easy-to-program home automation technologies that will, in short order, allow us to personalize nearly every appliance in our home.

Meanwhile, our cars are quickly becoming rolling computers, loaded with chips and sensors that automate more tasks and make us safer in the process. Soon, automobiles will be communicating not only with us but with everything else around them. While fully driverless cars may still be a few decades away, semi-autonomous technologies that are already here are gradually making it easier for our cars to drive us instead of us driving them.

Think of this new world as the equivalent of Iron Man Tony Stark's invisible butler JARVIS; we'll be able to interface with our devices and the entire world around us in an almost effortless fashion. Apple's Siri and similar digital personal assistants are already on the market but are quite crude. The near future will bring us Siri's far more advanced descendants, ambient technologies that are invisible yet omnipresent in our lives, waiting for us to bark out orders and then taking immediate, complex actions based on our demands.

After that we may quickly enter the realm of cyberpunk. There are already plans for "digital skin" and "electronic tattoos" that affix ultrathin wearables directly to the body. Many firms have already debuted "epidermal electronics" that, beyond the obvious health monitoring benefits, will allow users to interface with other devices—money scanners might be one obvious application—to allow frictionless transactions. Monitoring and communication technologies could also be swallowed or implanted within the body, allowing users to develop a more robust and less invasive record of their health at all times.

These innovations are poised to fuel an amazing transformation in the industrial world too, leading to a world of machine-to-machine communications that can sense, optimize, and repair instantaneously, producing greater efficiency. Consulting firms such as McKinsey and IDC have predicted that this transformation will yield trillions of dollars' worth of benefits by expanding economic opportunities and opening up new commercial sectors.

When the Net is being baked into everything we contact, policy anxieties will multiply rapidly as well. Security and privacy concerns already dominate policy discussions about the Internet of Things. Critics fear a future in which marketers or the government scrape up the data our connected devices will collect about us. But even more profound existential questions are being raised by legal theorists, ethical philosophers, and technology critics, who often conjure up dystopian scenarios of intelligent machines taking over our lives and economy.

Which Vision Shall Govern?

This is where the question of permissionless innovation comes into play. Will Internet of Things–era innovators be at liberty to experiment and to offer new inventions without prior approval? Or will a more precautionary approach prevail, one where creators will have to get the blessing of bureaucrats before launching new products and services?

The FTC has already issued reports proposing codes of conduct to manage the growing deluge of data. The goal is to encourage coders to bake in "privacy by design" and "security by design" at every step of product development. In particular, FTC officials want developers to provide users with adequate notice regarding data collection practices, while also minimizing data collection in the aggregate.

Many of those practices are quite sensible as general guidelines, especially those related to promoting the use of encryption and anonymization to better secure stored data. But the FTC wants developers *always* to adopt such privacy and data security practices, and it wants to be able to hit them with fines and other penalties (using the agency's "unfair and deceptive practices" authority) if they fail to live up to those promises. If the intimidation game gets too aggressive and developers reorient their focus to pleasing Washington instead of their customers, it could have a chilling effect on many new forms of data-driven, Internet-enabled innovation.

The FTC has already gone after dozens of digital operators in this way, including such Internet giants as Google. In consent decrees, the commission extracted a wide variety of changes to those companies' privacy and data collection practices while also demanding that they undergo privacy audits for a remarkable two decades. That'll provide regulators with a hook for nudging corporate data decisions for many years to come.

While the FTC looks to incorporate the Internet of Things within this expanded process, some precautionary-minded academics are pushing for even more aggressive interventions. Many critics of private-sector data collection would like to formalize the FTC's privacy and security auditing process. Decrying a supposed lack of transparency regarding the algorithms that power various digital devices and services, they propose that companies create internal review boards or hire "data ethicists" (like themselves) to judge the wisdom of each new data-driven innovation before product launch.

More far-reaching would be the "algorithmic auditing" proposed by tech critic Evgeny Morozov and others. Advocates seek a legal mechanism to ensure that the algorithms that power search engines or other large-scale digital databases are "fair" or "accountable," without really explaining how to set that standard. There's also a movement afoot for some sort of "right of reply" to protect our online reputations by forcing digital platforms to give us the chance to respond to websites or comments we don't like. The European Union is already going down this path with the so-called Right to be Forgotten law, which mandates that search results for individuals' names be scrubbed upon request.

Fortunately, we are protected from such mandates in the U.S. by the First Amendment. The right to code is the right to speak. Technocrats will have to be cleverer to impose their controls stateside. Realizing that those roadblocks lie ahead, some activists are already trying to shift the discussion by claiming it's about "civil rights" and the supposed disparate impact that will occur if algorithmic decisions are left to the marketplace. Danielle Keats Citron, a law professor at the University of Maryland, calls for "technological due process" that would subject private companies to the sort of legal scrutiny usually reserved for government actors.

Meanwhile, new bureaucracies are being floated to enforce it all. Apparently the alphabet soup of technocratic agencies already trying to expand their jurisdictions to cover emerging technologies —FCC, FTC, FDA, FAA, NHTSA, etc.—aren't doing enough for the critics. For example, Frank Pasquale, also of Maryland's law school, favors not only a right of reply but also a Federal Search Commission to oversee "search neutrality" (think of it as net neutrality for search engines and social networking sites), as well as "fair automation practices" that would regulate what he regards as the "black box" of large private databases. And Ryan Calo of the University of Washington School of Law fears "digital market manipulation" that might "exploit the cognitive limitations of consumers." He also proposes a Federal Robotics Commission "to deal with the novel experiences and harms robotics enables."

Better Safe Than Sorry?

Anticipatory regulatory threats such as these will proliferate in tandem with the expanding penetration of ambient, networked technologies. The logic that animates such thinking has always been seductive among the wet-blanket set: Isn't it better to be safe than sorry? Why not head off hypothetical problems in privacy and security?

There is no doubt that slowing Internet of Things development could prevent future data spills or privacy losses, just as there is no doubt that regulatorily strangling Henry Ford's vision in the crib would have prevented numerous car crashes (while also preventing all the advantages cars have brought to our lives as well). If we spend all our time worrying over worst-case scenarios, that means the *best-case* scenarios will never come about either. Nothing ventured, nothing gained.

The trans-Atlantic contrast between the U.S. and Europe on digital innovation over the past 15 years offers real-world evidence of why this conflict of visions matters. America's tech sector came to be the envy of the world, and many U.S.-based firms are household names across Europe. (Indeed, European regulators are constantly trying to take the likes of Google, Amazon, and Facebook down a peg.) Meanwhile, it is difficult to name more than a few major Internet innovators from Europe. America's more flexible, light-touch regulatory regime left more room for competition and innovation compared to Europe's top-down regime of data directives and bureaucratic restrictions.

Instead of precaution, a little patience is the better prescription. Long before the Internet of Things came along, many predecessor technologies—telephones, broadcast networks, cameras, and the Net itself—were initially viewed with suspicion and anxiety. Yet we quickly adapted to them and made them part of our daily routines.

Human beings are not completely subservient to their tools or helpless in the face of technological change. Citizens have found creative ways to adjust to technological transformations by employing a variety of coping mechanisms, new norms, or other creative fixes. Historically, the births of new, highly disruptive networking technologies—think of social networking sites just a decade ago—have been met by momentary techno-panics, only to see citizens quickly adapting to them and then clamoring for more and more of the stuff. The same will be true as we adjust to the Internet of Things.

If we hope to usher in what Michael Mandel, chief economic strategist at the Progressive Policy Institute, calls "the next stage of the Internet Revolution," we'll need to guarantee that innovators will remain free to experiment with new and better ways of doing things. That's the Internet freedom we should be fighting for.