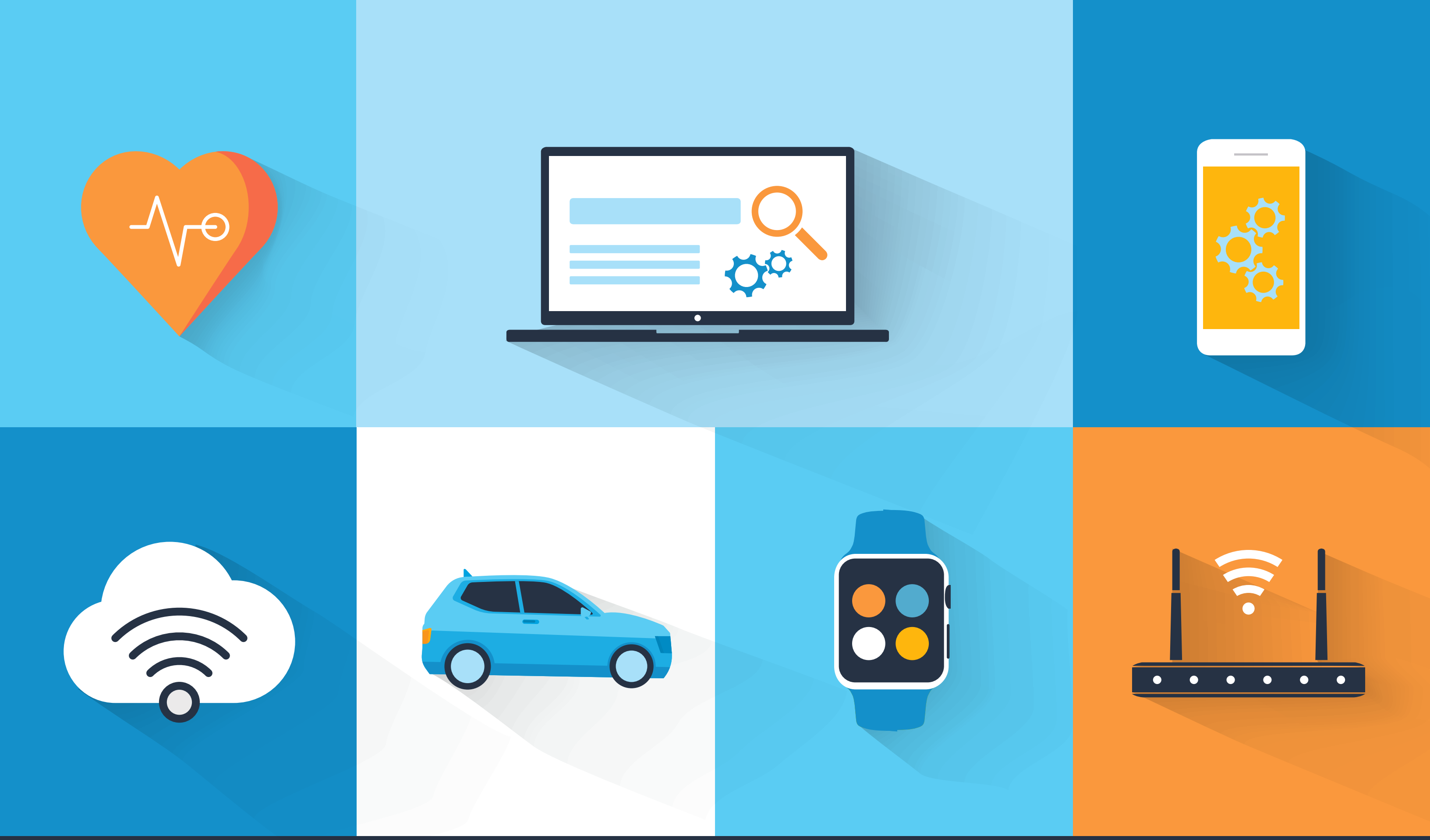


INTERNET OF THINGS:

A Framework for the Next Administration

November 2016

Consumer Technology Association™

Executive Summary

As an internet-based thread of connectivity among everyday objects, the Internet of Things (IoT) is changing how the world works. Soon, virtually everything will be connected, and devices from a tiny thermostat to large factory equipment will harness this power to create huge benefits for individuals, the economy and our society. Through products and services in the areas of audio/visual, smart home, wearables, transportation and others, the IoT will save consumers time and money, drive economic growth and enhance our nation's role as a global tech leader.

In this paper prepared by the Consumer Technology Association (CTA)™ – the trade association representing the $287 billion U.S. consumer technology industry – we consider the opportunities and challenges of IoT consumer applications and address the ways policymakers can encourage and support their growth. We also look at IoT success stories, such as how IoT technologies can help aging individuals and persons with disabilities to live independently.

The important efforts of the bipartisan, congressional Internet of Things Working Group and the Department of Commerce underscore that policymakers must approach the IoT with the twin goals of promoting consumer confidence and trust and preserving maximum flexibility to innovate. Government should accelerate its positive steps to promote the IoT by making more spectrum available, facilitating the ubiquitous deployment of broadband services, harmonizing federal agency interaction and providing clarity to citizens that the government will serve as an enforcement backstop if necessary to ensure public safety, privacy and other consumer protections.

Meanwhile, policymakers should refrain from broad, proscriptive regulatory action that could derail or delay new IoT applications. Instead, self-regulatory and other consensus-driven industry efforts will allow stakeholders to address discrete, specialized issues in a practical and flexible manner – what should be the default institutional mechanism for the IoT.

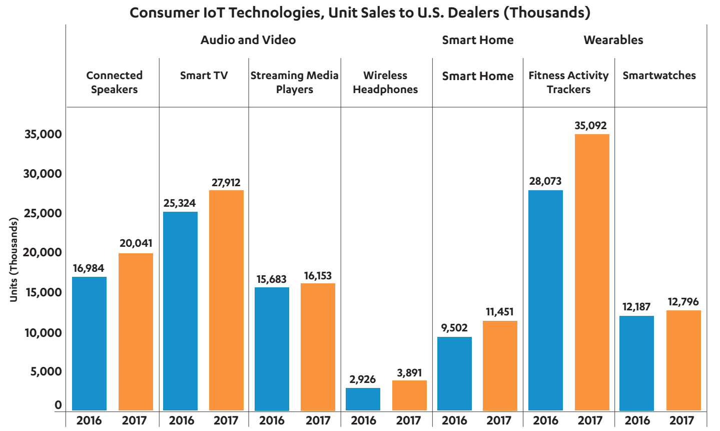
The Internet of Things is already changing our lives for the better, with an exponential array of benefits still to come. CTA welcomes the opportunity to work with policymakers and other stakeholders to ensure we leverage the IoT's maximum potential today and in the future.

I. Introduction

Whether you call it the "Internet of Things," the "Internet of Everything," the "Connected World," "IoT" or just plain amazing, the rapidly expanding thread of connectivity among everyday objects via the internet is changing how the world works. The IoT connects everyday objects to the internet, saving consumers time and money, driving economic growth and enhancing the United States' role as a global leader in technology.

The members of the Consumer Technology Association (CTA)™ include more than 2,200 companies in the consumer technology industry, many of whom are leading advancements in IoT applications and offering products and services that largely comprise IoT devices and infrastructure. CTA projections show that in 2016 alone, IoT applications will help drive 30 percent of the consumer technology industry's overall $287 billion in retail revenues.[1]

More specifically, the IoT is a critical catalyst for industry growth in several areas, as shown below:



Growth in Unit Sales 2016-2017, U.S.

Audio and Video	Connected Speakers	18%
	Smart TV	10%
	Streaming Media Players	3%
	Wireless Headphones	33%
Smart Home	Smart Home	21%
Wearables	Fitness Activity Trackers	25%
	Smart Watches	5%

Source: Consumer Technology Association (CTA)™, *U.S. Consumer Technology Sales and Forecasts, 2012-2017.*

Nowhere are the opportunities and promise of the IoT more clear than at the CES®, the world's gathering place for all who thrive on the business of consumer technologies. From around the globe, more than 3,800 companies display an awe-inspiring vision of our connected future.[2] CTA members and CES exhibitors are innovators who envision our tomorrow and provide solutions to problems we did not even know we had. These same tech companies manufacture the products and provide the services that comprise the IoT.

Each year, CES showcases the latest advancements in IoT technologies. Walking the CES show floor, attendees see a vision of the connected world that is jaw-dropping in its expanse and potential: multitudes of devices communicating with each other to improve quality of life across many metrics. The IoT's seamless connectivity, made possible by increased processing power and tiny sensors, will enable machines and devices to respond to conditions and situations pursuant to parameters dictated by a consumer – for example, increasing power to the freezer at a time of day when energy costs are low. Consumers and public officials can use the connected world to improve energy conservation, efficiency, productivity, public safety, health, education and more. Homes, cars, appliances and devices will evolve to have capabilities we cannot imagine today. The connected devices and applications that consumers choose to adopt will make their lives easier, safer, healthier, less expensive and more productive.

In 2016, a major development in the IoT was the expansion beyond individual devices to the rollout of IoT services – for example, Proctor & Gamble, Whirlpool, Nest and IBM's Watson all share information and/or partner services with Amazon. 2016 also saw a myriad of partnership announcements for collaborative IoT projects, such as Samsung and Microsoft working together on Windows 10. Just a few examples of the IoT technologies displayed and/or announced at CES include those that will:

Modernize our homes:

- Monitoring patterns in your home through various sensors, one system can notify you when something is awry, such as an escape of a family pet, a child not back from school on time, or a door left open.[3]
- Appliances with the built-in ability to order more detergent online and, interacting with other connected devices, switch to energy-saving or wrinkle-prevention modes when you're not home.[4]
- An app – designed with veterans in mind – to track the symptoms of users with post-traumatic stress disorder (PTSD) during sleep, using the technology of the smartwatch to gently wake PTSD sufferers out of their night terrors.[5]

Improve our health and life expectancy:

- Remote health monitoring devices, such as diabetes and heart monitors, that reduce the need for doctor visits.[6]
- Connected wheelchairs and other devices that expand accessibility.[7]
- Sunglasses with a built-in running and exercise coach and tracking capabilities.[8]
- A shirt that can measure heart rate[9] and another garment that can measure adrenaline levels and react accordingly.[10]
- A sock that captures a baby's heart rate and oxygen level[11] and a tag that tracks the number of words a baby is exposed to, regardless of who is talking.[12]
- A connected blood glucose meter that uploads readings in real time to the cloud and provides the patient an instant feedback message and tailored educational messages from the American Association of Diabetes Educators curriculum.[13]

Expand our travel and improve safety:

- An unmanned aircraft system that can carry a single human passenger, autonomously flying the passenger from one location to another.[14]
- A motorcycle helmet that projects traffic and vehicle information directly into the rider's field of view, increasing motorcycle safety.[15]
- A connected car that offers enhanced safety capabilities, such as vehicle-to-vehicle sensors and automated vehicle response features.[16]

Industry constantly is innovating. And consumers are driving innovation with their own ideas for certain outcomes that IoT and big data can facilitate – with consumers and companies working together, there is no telling what the future holds.

Exponential gains in IoT connectivity and the lightning-fast speed of innovation are driving strong growth across countless tech categories, especially as highly sophisticated technology becomes more affordable and accessible, improving our safety, productivity and entertainment. The next evolution of the IoT will build on connections already in place – as more products connect, consumers will manage their lives in ways that were impossible only a decade ago. This technological evolution and revolution will make consumers' lives exponentially safer, healthier and more convenient.[17]

The value of connected devices necessarily is tied to data analytics – big data and data management policies are what make them "smart."[18] When it comes to big data, policymakers must recognize that consumer data can provide broader public interest benefits, *e.g.*, using data from smart thermostats for grid management and traffic data from mobile phones for smart city development.

The IoT and big data also bring challenges. Some are artificial (and to some extent self-inflicted), such as a confusing and conflicting regulatory paradigm. Another is technological, such as interoperability. And yet others involve how consumers can use powerful IoT applications, while ensuring their information is treated appropriately and remains secure.

These challenges are not lost on IoT innovators and players – from startups designing first-of-their-type products through crowdfunding or technology giants investing in the development of new, incredible technologies. CTA urges policymakers to work *with* industry to ensure that any actions taken in the name of consumer protection do not inadvertently hamstring consumer-friendly IoT innovations.

In this paper, CTA expands on the clear opportunities and challenges of the IoT, focusing on consumer-facing applications (the "Consumer IoT") as distinct from industrial, commercial or enterprise applications. Consumer applications represent nearly one-third of the IoT's potential economic value, but attract a disproportionate amount of media attention.[19] And given their consumer focus, policymakers may be most tempted to address these applications. Because they offer the most potential economic and non-economic benefits for consumers, policymakers should ensure that Consumer IoT innovation is not discouraged by over-regulation.

Instead, policymakers can encourage and support IoT growth through federal and state efforts to spur research and development, immigration policies that allow U.S. IoT companies to attract the best and brightest and aggressively facilitating access to spectrum. In this vein, CTA applauds the recent creation of the bipartisan, congressional Internet of Things Working Group, which aims to educate members and bring them "up to speed on this technology and its impact on the modern economy and consumers"[20] as well as the various efforts that the Commerce Department is taking leading up to its IoT Green Paper.[21]

Policymakers also can promote consumer confidence and trust by ensuring protection of consumer privacy, sensitive data and network security under existing laws and rules. Finally, policymakers should support private sector, consensus-driven industry self-regulation, which has a proven history of minimizing consumer harms while maximizing flexibility to innovate, instead of government action that threatens to curb innovation.

II. Opportunities and Challenges

In the "innovate or die" world of technology, any new business model presents both opportunities and challenges. As the next phase in the development of the internet and World Wide Web, the IoT is no different. Until recently, people used the internet principally to obtain information, conduct transactions, communicate and connect with each other. Now, we connect physical objects to the internet and to each other through small, embedded sensors and wired and wireless technologies. This creates an ecosystem of ubiquitous computing, where "smart" devices securely collect and transmit data to other devices automatically and in real time.[22]

IoT Success Stories: Changing People's Lives. IoT applications have already had key impacts improving and, at times, saving consumers' lives. For example, wireless wearable fitness technologies have helped countless people lose weight and get healthier.[23] Connected smoke and carbon monoxide alarms have helped to save owners when their basements are full of carbon monoxide, as well as beloved pets when the pets' owners are out of town.[24] Connected security and video monitoring systems have aided consumers by, for example, allowing parents to leave an autistic child with a babysitter because of the system's remote monitoring capabilities, in addition to deterring would-be robbers.[25] And, IoT-powered efficiency gains can lead directly to lower utility bills.[26]

Moreover, IoT applications have the potential to provide critical services for Americans with particular needs. For example, CTA's research demonstrates that IoT applications can "prevent and preempt life inconveniences caused by...aging challenges."[27] As the aging population increases, institutional long-term care services cannot meet demand and, even if they could, many seniors want to age in their homes for as long as possible.[28] Emerging applications include safety monitoring that can prevent seniors from getting lost, improved living comfort through smart sensors and controls and health monitoring can help seniors stay in their homes longer by making homes a little friendlier and reducing the time caregivers and even medical professionals need to spend on-site.[29] And as elderly Americans stay in their homes longer, connected video and sensor technology allows their families to monitor them remotely to make sure they are safe, take their pills, or even close the front door.[30] CTA Foundation proudly supports the Older Adults Technology Services' (OATS) Senior Planet Exploration Center in New York, among many other initiatives, which offers classes and sits down with seniors to explain technologies, demystifying and unlocking technology.[31]

Similarly, individuals with disabilities – including many seniors – are harnessing the IoT to live safer, more independent lives:

> While many drivers dream about being able to sit back and relax during a long commute, driverless cars can literally open a new world to those who are physically unable to drive, providing access to daily routines such as grocery shopping or visiting friends and family, as well as bigger opportunities like facilitating steady employment and accessing health care.[32]

For those with physical limitations, controlling lights and thermostats can transform a dwelling into a comfortable home.[33] IoT applications convert signals delivered aurally—think a doorbell and telephone ring—into signals delivered into visually or physical—flashing lights and vibrating phones.[34] And, for individuals with cognitive disabilities, sensors can remind individuals to perform daily tasks or alert remote caregivers about a delayed routine task.[35] Importantly, many Consumer IoT applications are able to interface through smartphones, tablets and other mobile devices, which have built in accessibility features for app designers and consumers to use.

As more consumers adopt IoT technologies and innovators continue to improve these technologies and deploy new applications and services, we will see more and more "success stories" – until, finally, IoT achievements are simply an ordinary part of how we live.

Policymakers at the Crossroads. As the connected world expands, some "silver bullet" applications will help solve difficult problems and create new markets and efficiencies. Others will fail. Technology companies know these risks and enter the market mindfully, focused on bringing consumers the "must-have" technology they didn't even know they needed or wanted. What's key is that government must allow consumers and the market to decide IoT winners and losers, rather than dictating outcomes itself. In this way, regulation is itself a challenge spurred by rapid IoT developments.

Government can serve as either an enabler or an inhibitor to achieving the IoT's promise. And it can be an unintentional inhibitor, chilling innovation, when it sends mixed messages through various government agencies engaging in uncoordinated oversight activities. A significant challenge presented by the IoT is the fragmented approach of federal government agencies toward its development. As a 2015 *Politico* investigation revealed that "new networked-object technologies are covered by at least two dozen separate federal agencies – from the Food and Drug Administration (FDA) to the National Highway Traffic Safety Administration (NHTSA), from aviation to agriculture – and more than 30 different congressional committees."[36] Indeed, the FDA's rules and the Health Insurance Portability and Accountability Act (HIPAA), enforced by the Department of Health and Human Services, may apply to a wearable offered by your health provider, whereas the same device, purchased in a retail store, may be regulated in an entirely different agency, such as the Federal Trade Commission (FTC). Although connected and driverless cars seemingly fall within NHTSA's jurisdiction – certainly its wheelhouse – advocacy organizations petitioned the Federal Communications Commission (FCC) to take regulatory action, attempting to use the uncertainty of the regulatory landscape to impose new obligations on innovators.[37] A small startup developing a new wireless device may not be aware of FCC rules on equipment authorization and spectrum use. Meanwhile, the FTC, the federal agency most involved in exploring the IoT, increasingly shares jurisdiction with other agencies that lack expertise in consumer privacy issues.[38]

Any fragmentation or divergent and inconsistent regulatory approaches are potentially damaging to the development of IoT and confusing for consumers.[39] The specific laws, rules and regulatory regime(s) that apply to a particular IoT device or application may not always be obvious, and this complex web may be particularly difficult for smaller companies unable to afford counsel for each regime to navigate.

These challenges are exacerbated as innovation eviscerates historical distinctions between different types of services and applications. As the Commerce Department's Alan Davidson and Linda Kinney described in 2016:

> Regulators have long been focused on health and safety regulations that protect consumers; but in the past, enterprises in the transportation, healthcare and communications sectors have mostly functioned and been regulated independently. Now our physical and digital worlds are converging and lines between industries are increasingly blurred. Automobiles are becoming communication devices on wheels...[T]he Internet of Things is breaking down traditional silos...[40]

Moreover, laws and rules that focus on IoT-specific technologies (rather than on IoT as part of a larger, more comprehensive regime, or on an inappropriate use of a given IoT application) would be a mistake. They would threaten to put the government in the position of picking winners and losers to the detriment of competition, innovation, economic growth, and, ultimately, consumer and societal welfare. Government should avoid IoT design mandates, burdens on new marketplace entrants, or blessing (or banning) any specific technologies. Instead, policymakers should focus on desired outcomes and results and let the pace of innovation and market dynamics determine which IoT technologies prevail.

Given these concerns, CTA supports the U.S. Department of Commerce effort to develop a green paper based on public feedback aimed at supporting innovation and investment in the IoT and build a more cohesive federal government approach as the IoT continues to evolve.[41] The Department's green paper should recognize that policymakers must work *with* industry to ensure that any actions taken in the name of consumer protection do not inadvertently hamstring the myriad consumer-friendly IoT developments. Government must allow consumers and the market to decide IoT winners and losers, rather than dictating specific or rigid results. Policymakers thus should focus on private sector, consensus-driven industry self-regulation, which has a proven history of minimizing consumer harms while maximizing flexibility to innovate, instead of government action that threatens to curb innovation. In addition, policymakers should encourage and support growth and adoption of the IoT through efforts to spur research and development, lower effective tax rates, adopting immigration policies that allow U.S. companies to attract the best and brightest and aggressively facilitating access to spectrum. The government can best promote consumer confidence and trust in the IoT under applicable *existing* laws and rules; these existing legislative and regulatory vehicles will ensure protection of consumer privacy, sensitive data and network security. CTA looks forward to working with the Commerce Department and other stakeholders on implementing the recommendations of the green paper and supporting the development of a national strategy for IoT.

Privacy and Security Challenges of Increased Connectivity. Of course, the IoT faces challenges to its success beyond inconsistent and reactionary regulatory regimes. In January 2015, the FTC staff issued a report that discussed the benefits of IoT and identified potential security and privacy risks associated with increased connectivity between devices and the internet,[42] including: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks.[43] The identified privacy risks relate to the direct collection of sensitive personal information and the collection of personal information, habits, locations and physical conditions over time.[44]

At a fundamental level, the IoT relies greatly on collecting and sharing information among devices. Thus, it is premised on consumer trust and utility. Consumers must trust IoT applications and devices to adopt and use them. IoT manufacturers and service providers take seriously the need for consumer trust and, both as individual companies and as industries, have proactively addressed these issues. To ensure consumer trust, IoT companies must be transparent about their data collection and use practices and keep the promises about such practices they make to consumers. As discussed below, industry-wide, consensus-driven self-regulation works and works well to address these issues. Unlike government-imposed mandates, self-regulatory efforts are nimble, keep pace with technology and balance compliance requirements with the flexibility required to innovate.

For the IoT to flourish generally – and for new, never-thought-of-before Consumer IoT applications to positively impact and improve consumers' lives – government must partner with industry to eliminate barriers to innovation, exercise regulatory humility by considering any regulatory actions in light of greater economic impacts, and, when possible, embrace industry self-regulatory efforts that can address concerns as they arise without inhibiting innovation.

III. Advances in the IoT, Combined with General Innovation-Friendly Policies, Can Help the United States Maintain its Role as a Global Leader in Technology

The U.S. technology sector is the strongest and most innovative in the world. Appropriate federal and state government action will ensure that the nation maintains its leadership in the burgeoning IoT market.[45] However, this leadership is being challenged by other countries that are aggressively pursuing IoT transformation. For example, China has stated that "Made in China 2025", the Chinese government's blueprint for overhauling industry and rebranding China as a high-quality manufacturer, is based on smart manufacturing (a network of intelligent, connected factories), emphasizes innovation and quality, and includes U.S. $6.4 billion exclusively for China's emerging industries.[46] Germany pursues "Industrie 4.0," the German vision for the future of manufacturing, where smart factories use information and communications technologies to digitize their processes and reap huge benefits in the form of improved quality, lower costs and increased efficiency.[47] As CTA has observed:

> With some of the world's most "disruptive" companies - both global brands and innovative startups - the U.S. tech sector will help reduce the deficit, create jobs, improve sustainability and grow the economy. And tech's evolving sharing economy brings unique value, giving us more transportation and hospitality choices, creating good jobs with flexible hours and tapping capital resources such as a second car or a spare bedroom. But we must have the right policies in place to achieve tangible benefits.[48]

Federal, state and even local governments each can play a part in ensuring that the U.S. IoT sector maintains its global leadership role. Government should adopt targeted policies aimed at stimulating IoT demand and development and ensuring that the U.S. IoT industry has the tools that it needs to advance and expand. Just as important, however, governments must avoid rules that stymie innovation and repeal or clarify ambiguous rules that create regulatory uncertainty.

More and more states are adopting pro-innovation policies that create good jobs and fuel economic growth.[49] CTA applauds the 12 states and the District of Columbia that have excelled in CTA's 2016 "Innovation Scorecard": Arizona, Delaware, Indiana, Kansas, Massachusetts, Michigan, Nebraska, North Dakota, Texas, Utah, Virginia and Wisconsin.[50] Overall, these states have set the pace and tone for key practices (*e.g.*, strong right-to-work legislation, fast internet access, robust entrepreneurial climate, open posture to new business models and technologies, tax policy, tech workforce, investment attraction, STEM degrees, unmanned innovations and sustainability policies) that promote innovation and help avoid sending valuable talent and economic growth to a neighboring state – or even worse, overseas.

Demand Stimulation. Federal and state governments can generate demand for IoT technologies, which will help jumpstart the development of IoT ecosystems. For example, CTA's members are investing heavily in next generation cellular (5G) and next generation Wi-Fi technologies. Many companies look forward to partnering with the public sector as part of the Administration's Smart Cities Initiative, which will "invest over $160 million in federal research" to leverage IoT "to improve the life of…residents."[51] Similarly, innovative American companies are closely following DOT action in response to the recently enacted FAST Act.[52]

Government agencies can use IoT technology to increase efficiency in managing public infrastructure, and they can incent or require regulated utilities to use the IoT to conserve regulated resources such as energy and water. These actions will directly and immediately benefit the American public while stimulating the private IoT markets that supply the government and public utilities. Examples of this potential:

- IoT devices provide a serious opportunity to improve accessibility for such communities as the deaf and hard of hearing by replacing or supplementing otherwise audio cues with visual and tactile alerts.[53]
- Consumers increase their energy conservation efforts and see lower bills through government-incented smart meters and smart grids, both of which rely on IoT technology. As an added benefit, this would enhance the reliability of electricity distribution.[54]

- State and local governments can require IoT connectivity in building codes, and IoT technologies can be incorporated into the Leadership in Energy and Environmental Design (*i.e.*, LEED) standards.[55] IoT technologies such as photosensors, occupancy sensors, lighting controls, circuit-level control and adaptive lighting improve energy efficiency.[56]
- Government agencies can address traffic and parking congestion – an increasing problem in urban areas throughout the country – through the use of IoT sensors to better monitor and route existing traffic, ensuring maximum utilization of available parking resources while collecting data that can be used to improve transportation infrastructure planning.[57]

Moreover, by making the data collected by government-operated IoT systems available to the public and private industry (subject to privacy safeguards), governments can facilitate private companies' independent development of innovative new market niches.[58] In addition, through public-private partnerships, governments can empower private companies to develop new and better ways for governments to use IoT-generated data to provide more efficient and desirable public services.

Tax Code Clarification. Policymakers should explore the unintended consequences of tax policies on the IoT market. Tax laws should foster IoT innovation rather than providing disincentives to the continued rapid deployment of the IoT, which should be driven by competition and consumer demand. For example, IoT blurs the line between products, services, and telecommunications, each of which are taxed differently in most states. The IoT includes elements of each of these categories, which often makes it difficult for IoT companies to determine how they will be taxed.[59] In addition, harmonization of the application of state tax laws to the IoT should be a priority at the state level whenever feasible to avoid saddling IoT companies with the need to understand and comply with a hodge-podge of varying tax treatments of the IoT. By working with the IoT industry to provide clarity regarding the appropriate taxation of the IoT and harmonization of state-level tax laws in connection with the IoT, taxing authorities can free IoT companies to focus on their customers and spend less resources on tax planning and compliance.

Immigration Reform. Appropriate immigration policies also are key to unleashing the potential of the IoT sector. In light of the breathtaking growth expected in this sector over the next decade, it is unlikely that the U.S.'s science, technology, engineering and math (STEM) work force will be sufficient to support the sector's rapid expansion[60] unless Congress adopts meaningful reform to the U.S.'s overly restrictive immigration policies. There simply are not enough STEM-skilled U.S. workers today to fill the myriad of technical positions that will be created by the IoT sector at the hardware, operating system, connectivity, data management and user interface layers.

Although the United States' higher education system is one of its greatest resources, the portion of foreign students receiving advanced STEM degrees at U.S. institutions has been increasing for decades,[61] and many of these students are unable to remain in the United States after obtaining their degrees due to short-sighted immigration policies. Consequently, strategic immigration reforms are needed to encourage U.S.-educated immigrants to remain in the U.S. to build businesses and create domestic jobs. Further, rather than creating obstacles to the immigration of foreign entrepreneurs who want to take advantage of the U.S.' world-leading technology sector, U.S. immigration policy should proactively promote their participation. Bills such as Rep. Darrell Issa's Supplying Knowledge-Based Immigrants and Lifting Levels of STEM Visas Act (SKILLS Visa Act)[62] and Sen. Orrin Hatch's I-Squared Act of 2015[63] are aimed at addressing these issues.

Patent Reform. The U.S. Patent and Trademark Office (USPTO) can continue its efforts to improve "patent quality, especially in new technological domains, including IoT."[64] As more "things" become embedded with patentable technologies, the "attack surface" for patent assertion entities – better known as "patent trolls" – grows. Enabled by Congress and implemented by the USPTO, patent reform aimed at blunting patent trolls will remove a harmful tax on IoT development. More, the Federal Trade Commission's October 2016 report, "Patent Assertion Entity Activity, an FTC Study," shines the light brightly on the harm caused by patent trolls and it calls for critical reforms that will protect legitimate U.S. business from continued extortion.[65]

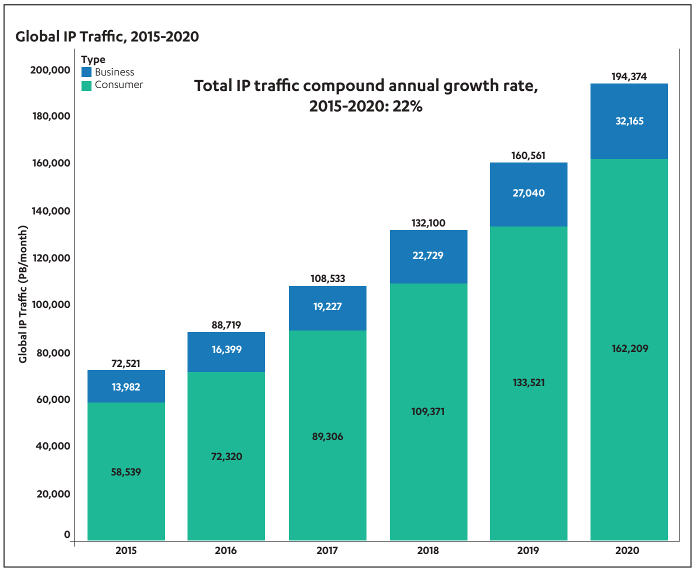
***

This by no means is a comprehensive evaluation of the ways in which federal and state governments can foster the IoT sector and benefit from its success. Many other opportunities and challenges will come to light as the IoT sector matures and IoT technology becomes a component of day-to-day life. Governments should work collaboratively with the IoT sector to pursue opportunities and overcome challenges. If government does not fulfill this role and fails to focus on the IoT sector, there is real risk that innovative IoT companies will move their operations and intellectual resources to other countries that have developed friendlier IoT regulatory and market environments.[66]

IV. Improved Access to Spectrum Is Critical To Fueling The IOT

The ability to untangle sensors and devices from wires and other cost-intensive infrastructure through wireless technology is a key reason that the IoT is nothing short of revolutionary. IoT applications utilize both unlicensed and licensed spectrum and both small, personal networks and wide area networks.[67] As the IoT hits its stride, it is readily apparent that demand for wireless spectrum, which already is extraordinary, will continue to grow. Federal agencies and Congress must continue to work with industry to increase access to valuable spectrum for both licensed and unlicensed operations.

The IoT Needs More Spectrum Than the Current Pipeline Will Provide. Tomorrow's Consumer IoT will expand beyond smart homes, smart cars and smart appliances into uses not imagined. According to one estimate, *per capita* devices and connections in North America will average of 12.18 in 2020, up from 7.14 in 2015.[68] To connect the billions of devices that will be in use by 2020, a network would require capacity that is "at least 1,000 times the capability that exists today."[69] Further, each new generation of networking technologies allows for better speeds, higher throughputs and lower power requirements, which, in turn, foster the adoption and usage of higher-bandwidth applications and ever-more connected devices.[70] This is true even for many IoT devices, which already can generate as much IP traffic as *seven* basic-feature phones.[71] For example, machine-to-machine connections (*i.e.*, those connecting vehicles, roads, the grid and even drones) are expected to experience IP traffic compound annual growth rates of 85 percent through 2020.[72]



Source: Cisco VNI

Unlicensed spectrum is a hotbed for innovation and integral in addressing the spectrum crunch. It provides a platform for innovative technologies implemented in numerous consumer products, such as Wi-Fi, Bluetooth, ZigBee, Z-Wave and wireless HDMI connections, which have opened new frontiers of communications, including high-speed internet, for consumers. For example, IoT devices like fitness trackers, locks and refrigerators connect online through simple, low-powered chips that often transmit information over unlicensed spectrum.[73] In addition to the 2.4 GHz and 5 GHz bands that feature Bluetooth, Wi-Fi and ZigBee, IoT devices are being designed for several other unlicensed bands such as: sub-125 kHz (video surveillance and access control systems); 13.56 MHz (near-field communications to support mobile payments); and 900 MHz (Electronic Product Code, one of the industrial standards for global Radio Frequency Identification).[74]

Already, unlicensed spectrum generates $62 billion per year just from the incremental retail sales value of devices using unlicensed spectrum to end-users[75] and over $200 billion when combined with "unlicensed spectrum's value in terms of cost savings."[76] These advances hold tremendous promise for increased quality of life and economic gain. Indeed, "the value of...indirect contributions in terms of savings, productivity and utility greatly exceed, and are additive to, unlicensed spectrum's direct input to the economy."[77]

IoT devices and services utilize both licensed and unlicensed spectrum simultaneously, such as mobile broadband. As Cisco explained, as mobile data traffic grew 74 percent in 2015, 51 percent of mobile data traffic was offloaded onto Wi-Fi or femtocell networks.[78] Importantly, "mobile offload *exceeded* cellular traffic for the first time in 2015."[79] Even with new AWS-3, Incentive Auction and other licensed spectrum for mobile broadband coming online, unlicensed spectrum will remain a vital complement to licensed spectrum in the long term. The federal government must continue to work with industry to ensure that both licensed and unlicensed spectrum is being efficiently and successfully used.

Congress and Federal Agencies Can Ensure the Right Spectrum is Available to Continue Building on IoT Successes. With the IoT showing promise in so many sectors of our economy, a broad range of agencies must partner among themselves and with industry to ensure sufficient spectrum to match the needs of the IoT. For this reason, CTA has encouraged and eagerly anticipated the FCC's first-ever Incentive Auction, which will introduce more licensed and unlicensed spectrum for mobile broadband services that will house IoT applications.[80] Likewise, recent FCC actions have started to enhance the spectrum pipeline, but more work is required (such as testing and agency guidance) to permit widespread and routine use by IoT devices and services.[81] The wide variety of IoT spectrum uses means that the FCC must continue to explore many different bands of spectrum. The FCC should build on the foundational data developed in the Technological Advisory Committee (TAC) for future FCC spectrum and equipment authorization actions.[82]

Given the promise of smart cities, the Department of Transportation (DOT) must also enable the IoT to flourish, both by supporting new IoT programs and working with the FCC to ensure that the spectrum needs of smart cities and cars are being met. The September 2016 DOT announcement of a driverless car framework helped move us forward.[83] Similarly, the joint letter signed by the leaders of the FCC, DOT and the Commerce Department committing to a testing plan for shared uses in the 5.9 GHz band, now allocated to Intelligent Transportation Systems, is an exemplar of interagency collaboration that could and should be replicated elsewhere.[84] However, until and unless the 5.9 GHz band issues are resolved, necessary research and development efforts by manufacturers will be impeded.

Similarly, the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) must continue important research into how spectrum can be shared and measured.[85] The joint FCC/NTIA "Test

City" effort to explore and test spectrum sharing technologies in a real world environment is another step towards the deployment of robust and ubiquitous broadband, a critical enabler of the IoT.[86] The recent Commerce Department request for comments and development of a green paper to determine the role it "could play to support innovation and investment in IoT" opens new doors for cross-industry and interagency partnership.[87]

Recognizing that the federal government is the largest single holder of spectrum in the country, Congress must continue to support and encourage federal agencies to share, and where possible, clear spectrum "to ensure the IoT industry has access to the spectrum it needs to continue to grow and change our lives for the better."[88] Public statements recognizing the importance of spectrum and the IoT are starting to build support for agency action.[89] Some of the bills before the 114th Congress contained the potential to greatly increase available spectrum for commercial uses, including the IoT.[90] These steps demonstrate that government can and should play an important role in providing sufficient spectrum to allow industry to build the networks that will provide the foundation for the IoT.

V. Building A Strong Public Sector/Private Sector Partnership As The Foundation For Consumer Confidence And Trust In The IOT

Government also can advance the interests of consumers by working *with* industry to develop a system of trust between users and things. For example, together government and industry can work to educate consumers on issues such as how to limit risks associated with unsecured connected devices (*e.g.*, by changing default passwords, using password-protecting home Wi-Fi networks, and employing virtual private networks). Government also can convene interested parties, as the FTC has done in its groundbreaking 2015-2016 "Start with Security" series, in which the FTC has taken business guidance on the road to San Francisco, Seattle and Austin, to meet with startups, experts and agency officials to discuss effective data security strategies.[91]

In addition, the public/private partnership between government and industry that has coalesced around recent cybersecurity initiatives is particularly illustrative. Most notably, various critical infrastructure sectors came together under the auspices of NIST to develop the NIST Cybersecurity Framework, a voluntary, flexible, and non-regulatory approach that enables companies of all types and sizes to tailor their cybersecurity efforts to meet their business models, infrastructure and assets.[92] In response to requests for comment by NIST,[93] industry recently voiced continued support of the Cybersecurity Framework as companies work through the early phases of building it into their risk management processes. Similar business-led collaboration continues through other established mechanisms – for instance, the Sector Coordinating Councils formed for each of 16 critical infrastructure sectors, which facilitate information sharing and provide a forum in which to review pertinent industry and government actions.[94] Additional industry coordination is facilitated through the Communications Security, Reliability and Interoperability Council (CSRIC) – an advisory committee to the FCC that recommends best practices and potential actions to ensure optimal security, reliability and interoperability of commercial and public safety communications systems.[95] Concurrently, NTIA has used its multistakeholder processes to further catalyze industry discussion on the cybersecurity-related issues, with the stated goal of avoiding regulatory solutions.[96] Of course, all of these efforts parallel industry's own initiatives, such as the Building Security in Maturity Model (BSIMM) – a study of actual software security initiatives that likewise is not a one-size-fits-all prescription.[97] In short, cybersecurity issues are being addressed in a multi-layered fashion, with industry consistently taking a lead in shaping the discussion. A similar approach to consider challenges posed by the growth of the IoT would ensure protection of consumers' safety and quality of service, while affording industry the opportunity to directly participate and shape parameters that can evolve flexibly as new business and technological developments emerge.

VI. Continuing To Build Industry-Wide, Consensus-Driven Self-Regulation That Is Nimble And Accounts For Rapidly-Evolving Technologies

The internet's growth is largely attributable to the success of consensus-driven stakeholder processes to address policy issues.[98] The privacy and security concerns associated with the IoT closely mirror those in which industry already has a strong track record of developing and implementing best practices to protect consumers. And industry is carrying those efforts forward to the Consumer IoT context. CTA has been at the forefront of industry efforts, leading the charge on the development of IoT technical standards and addressing concerns related to the privacy of wellness data.[99] In addition, some CTA members also are members of industry groups that have developed cybersecurity resources for consumers and best practices for home security.[100] These efforts have expanded to address the privacy and security implications of new consumer technologies that fall under the Consumer IoT umbrella.

At a fundamental level, the IoT depends in great part on the collection and sharing of information among devices and machines, and thus is premised on consumer trust, data accuracy and utility. For example, IoT manufacturers and service providers take seriously the need for consumer trust and, both as individual companies and as industries, have proactively addressed these issues. History has shown that privacy concerns arise any time a new technology is introduced that involves the collection of consumer data, and that consumers generally come to recognize the need to make tradeoffs regarding the information they choose to share in order to obtain the benefits offered by new products and services. One person might decide it is worth it to share personal body measurements in order to obtain custom clothes; another – many others – might be willing to share medical information in order to access advanced monitoring, diagnosis and treatment applications. For example, a recent survey demonstrated that 90 percent of Americans are willing to share wearable data with healthcare providers.[101] Likewise, another survey reported that 60 percent of consumers are willing to have a video visit with a physician through a mobile device.[102] Just as consumers choose how, where, and for what purpose to use connected devices, they will choose how, where, and for what purpose they will share their personal information through such devices.[103] This is already happening as telemedicine is increasing year-over-year in patients (more than 15 million Americans last year expected to grow 30 percent this year), visits (1.2 million virtual doctor visits in 2016, a 20 percent increase over 2015), and providers (such as web companies Teladoc, Doctor on Demand and American Well).[104] Different individuals will choose to adopt different applications of these new forms of connectivity, some of which will rely on the transfer of information between and among devices.[105] The manufacturers and service providers that are poised to deliver this bright future to consumers understand and take seriously the need for consumer trust. The technology market is fiercely competitive, and consumers will not purchase products if they do not trust a manufacturer's or provider's handling of data.

Self-Regulation Works. Self-regulatory regimes have worked well to ensure consumer privacy and foster innovation. The use of consumer information for marketing and other purposes is not new, as marketers have engaged in responsible collection of data for more than 100 years.[106] Industry has a strong track record of developing and implementing best practices to protect information throughout this history, proactively addressing privacy and security issues. And, as noted below, industry already is proactively addressing these issues as they relate to the Consumer IoT.

Self-regulation, whether through the development of enforceable codes of conduct or industry best practices, works and works well. As detailed below, well-intentioned but unnecessary government action can skew or suppress innovation, create market uncertainty, and ultimately harm consumers. Legislation and regulation often fail to keep up with ever-evolving technology, and often rely – to the detriment of the marketplace and consumers – on government regulators' static assumptions and predictions of where the market is going and what consumers want.

Self-regulation can avoid these pitfalls. As the White House has observed, in contrast to regulation, multistakeholder processes "can provide the flexibility, speed and decentralization necessary to address Internet policy challenges."[107] Indeed, the "[f]lexibility in the deliberative process is critical to allowing stakeholders to explore the technical and policy dimensions –which are often intertwined – of Internet policy issues."[108] Self-regulation is nimble, and can be more easily updated to address changes in the marketplace and technology. Self-regulation also can be more efficient for businesses, allowing them to avoid costs that otherwise would be passed on to consumers.[109] And self-regulatory efforts push companies to "internalize ethical behavior and principles since the rules are based on social norms and conduct of peers rather than top-down prescriptive rules."[110]

In fact, self-regulatory codes may be the *best* way to effectuate consumer preferences for the IoT. As the Future of Privacy Forum observed:

> As the Internet of Things becomes more ubiquitous, parents will want to control what can be done with information collected from devices associated with their children. Others may want to indicate their preferences about how third-party connected devices will communicate with them. Self-regulatory codes of conduct will be the most effective means to honor these preferences and others in the rapidly evolving landscape of the Internet of Things.[111]

In contrast, a top-down regulatory approach would have serious downsides in the IoT space, where policy outcomes could percolate through several different industries and heterogeneous technologies. In this regard, a sector- or agency-specific IoT regulatory approach could artificially preserve traditional regulatory silos and ultimately pick the winners and losers of the IoT. Government can and should act when serious issues are identified, but should do so as narrowly as possible.

Accordingly, self-regulatory and other consensus-driven industry efforts should be the default institutional mechanism for the IoT. Self-regulation allows stakeholders to address discrete, specialized issues that arise in a practical and flexible manner and without the same risks to competition and innovation. Indeed, because "multistakeholder processes do not rely on a single, centralized authority to solve problems," multistakeholder institutions can "address specific kinds of Internet policy challenges."[112] According to the White House, "[t]his kind of specialization not only speeds up the development of solutions but also helps to avoid the duplication of stakeholders' efforts."[113]

Stakeholders Already Are Proactively Addressing IoT Concerns. Proactive industry efforts to address IoT concerns already are underway. CTA has been at the forefront of industry efforts, leading the charge on the development of IoT technical standards and addressing concerns related to the privacy of wellness data. In addition, CTA and its members participate in a number of other ongoing efforts to address IoT issues, including those convened by think tanks, other associations and the Administration.

*Standards Development***.** In the emerging IoT economy, voluntary global standards will accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path. To the extent that interoperability and reliability are related, enabling manufacturers and consumers to create a feedback loop will better calibrate end-user expectations and lead to more useful, cheaper IoT applications than any government mandate. Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges.

Government should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards. Specifically, government should encourage – but not mandate – the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. Moreover, the U.S. government should explicitly endorse private-sector leadership on technical standards (including those related to security) and ensure that its counterparts abroad do not interfere with these private sector processes. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

As the largest trade association representing more than 2,200 companies in the $287 billion U.S. consumer technology industry, CTA plays a key role in fostering the development of standards for the IoT, including security and interoperability standards. CTA's standards committees, which are accredited by the American National Standards Institute (ANSI), have produced many documents related to the IoT. Some of the most recent include *Host and Router Profiles for IPv6* (ANSI/CTA-2048), *Securing Connected Devices for Consumers in the Home* (CTA-TR-12), and *Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1* (CTA-TR-4). On Oct. 18 CTA released a tool that companies can use to self-assess how well they address security in their products. This online tool, developed by Cigital for CTA, is called the Building Security In Maturity Model and lets companies compare their security efforts against industry standards, and helps them address security throughout their workflow rather than test for bugs and flaws at the very end of the product development process.

Consumer trust is critical for the IoT to succeed, and companies thus have a built-in incentive to protect data collected and used by IoT devices. For example, in addition to its own standards work, CTA helps alliances of companies and professionals within the consumer technology industry like the Open Connectivity Foundation,[114] the Institute of Electrical and Electronics Engineers (IEEE),[115] and the Internet Engineering Task Force (IETF)[116] succeed in their efforts to develop and promote security and interoperability standards for the IoT. A substantial amount of work is happening in this area. A recent example is the merger of the Open Connectivity Foundation and the AllSeen Alliance, bringing interoperability and backward compatibility to devices using either the AllJoyn or IoTivity standards.[117] Several industry alliances attended CTA's Technology & Standards Forum in April 2016 and presented information about their work on IoT standards. These included Broadband Forum, HDMI LLC, HomeGrid Forum, HomePlugAlliance, Wireless Broadband Alliance and Z-Wave Alliance.[118] Several more industry alliances attended CTA's Technology & Standards Forum in October 2016 and presented information about their work on IoT security.[119] These included FIDO Alliance, Internet Society, and Trusted Computing Group. CTA tracks the efforts of these and many other industry alliances and keeps the industry informed about their activities through a quarterly email newsletter.

CTA's Guiding Principles on the Privacy and Security of Personal Wellness Data. In early 2015, CTA began a process to establish a first-of-its-kind set of voluntary guidelines for private sector organizations that handle personal wellness data, which often is generated by wearable technologies. The process culminated in CTA's October 2015 announcement of the *Guiding Principles on the Privacy and Security of Personal Wellness Data*, which establish a baseline, voluntary framework to promote consumer trust in technology companies. Among other things, the Guiding Principles address the following:

Security. Companies should provide robust security measures;

Transparency. Companies should provide clear, concise and transparent information on the use of data collection, storing and sharing, especially when transferring data to unaffiliated third parties;

Consumer confidence. Companies should ensure consumers have the ability to control and review their personal wellness data;

Opt-out. Companies should offer users the ability to opt out of advertising; and

Law Enforcement. Companies should clearly disclose their protocol for responding to law enforcement data requests.[120]

CTA intends to review the Guiding Principles with our members on a regular basis to ensure that the Principles accurately reflect current data privacy and security concerns. We also are working to assess other aspects of the IoT ecosystem to consider similar initiatives.

Other Multistakeholder Efforts. CTA is not the only group that is addressing privacy and security concerns implicated by the Consumer IoT. CTA or its members have been active participants in myriad other stakeholder efforts, such as:

- The Future of Privacy Forum's discussion document on privacy principles for facial recognition technology;[121]
- The President's National Security Telecommunications Advisory Committee (NSTAC), with the mission to provide the U.S. Government the best possible industry advice in areas of national security;[122]
- The Alliance of Automobile Manufacturers and the Association of Global Automakers' initiative to establish privacy principles;[123]
- The NTIA's multistakeholder process to develop privacy, transparency and accountability best practices for unmanned aircraft system use.[124]

***

Self-regulatory efforts can effectively address existing and emerging consumer concerns regarding the IoT without compromising the opportunities the IoT presents. CTA and others are addressing today's concerns through self-regulatory and multistakeholder initiatives, and will continue to do so as consumers' concerns evolve. Government should continue to embrace these efforts. If necessary, the FTC can utilize its Section 5 authority to protect against any privacy-related practices that are unfair or deceptive.

VII. Avoiding Government Action That Directly Or Indirectly Curbs Innovation

While government has a critical role to play in ensuring that its policies enable industry to meet consumer demand of IoT offerings, it must be sure to limit other types of regulatory intervention – and to forego entirely any actions that could stifle innovation in the nascent IoT ecosystem. Many of the IoT applications being planned or even sent to market today were impossible to envision just a decade ago; there is no reason to doubt that the coming years will generate a wealth of additional as-yet-unimagined opportunities for American consumers. Prescriptive regulation, however well intentioned, could inadvertently deter the development and deployment of such offerings. Thus, policymakers at all levels of government should exercise regulatory humility: They should focus on promoting innovation, favor market-based outcomes over regulation where possible, and, in cases where the marketplace will not produce optimal results, rely on self-regulatory models over command-and-control regulation. Consistent with these principles, policymakers should reject mandates that would distort the IoT's trajectory and undercut the growth of offerings that would expand consumers' welfare. In particular, they should repudiate requirements that favor one platform or technology over another or create or expand uncertainty, and should foreswear excessively punitive enforcement penalties, which serve no valid purpose and ultimately harm consumers.

Core Principles. Policymakers should, in the first instance, premise any action relating to the IoT on a handful of core principles that should at this point be beyond dispute. Prescriptive regulation, however well intentioned, could inadvertently deter the development and deployment of the IoT. Likewise, fragmented and, its flip-side, overlapping rules are artificial hurdles that government should avoid. Specifically, policymakers at all levels of government should exercise regulatory humility, taking only actions consistent with the following core framework:

First, to promote innovation, policymakers should favor market-based solutions over prescriptive rules. Our economic success is built on a foundation of freedom, including freedom to contract and freedom to innovate. Government should apply regulation only if there is a compelling public interest in doing so.[125] When providers are competing in a marketplace, they face very strong incentives to adapt and respond to customer preferences, and to do so extremely quickly. Market rivalry requires providers not only to reduce prices, but also (for example) build safe equipment, be transparent about their offerings and the terms and conditions on which they are made available, and provide consumers the privacy protections they demand. When it works well, regulation is intended to approximate a well-functioning marketplace and thereby improve consumer well-being. But regulation can also impose significant costs, especially in areas of lightning-fast innovation. Among other things, it can "lock in" today's presumptions and understandings, stymying providers' efforts to respond to changing consumer needs and deterring the deployment of new offerings altogether.[126] Thus, policymakers should eschew top-down mandates where the marketplace is likely to work and where there is no evidence that the marketplace is not functioning properly.

To this end, policymakers should not reflexively second-guess how consumers decide to incorporate technology into their lives. Indeed, piling on requirements to educate consumers, or otherwise force them to confront the "peril" associated with information flows, may lead to notice fatigue, as consumers merely seek to get the service that they want. Any government action here must be targeted to address a specific, well-defined problem.

To take one example relevant to the IoT, consumers are sophisticated and understand that data powers the smart technology they use.[127] They recognize that the sweeping benefits of the connected world are not possible without the collection of information and the sharing of information among devices.[128] Policymakers cannot simply assume that consumers do not understand, and thus require "protections" from, such sharing. There may be elements of peril associated with the abundant information flows fostered by the IoT, as some suggest, but there is also the enormous promise of real benefits for American consumers both individually and collectively. The rise of wearable health monitors, connected cars, and smart energy meters has profoundly improved our ability to make choices – both individually and collectively – that improve welfare and pose minimal threat to user privacy.[129] It is for customers, not regulators, to choose whether to avail themselves of such benefits. Moreover, just as users have become familiar with and learned to manage the privacy-related risks of computers and smartphones, they will quickly learn to understand the benefits and costs associated with other aspects of IoT offerings. As economists have understood for centuries, consumer value is maximized when the *consumer* makes the decision whether to exchange one good or service for another, not when a third party makes the decision for her. According to CTA data from March 2016, 63 percent of U.S. adults are open to the use of biometric technologies for altruistic purposes, such as medical research.[130]

Likewise, in determining whether regulation is truly superior to a market-based outcome, policymakers should apply empirical analyses to determine whether the *benefits* of a proposed mandate will exceed its *costs*. Such cost-benefit analyses can help balance the need for consumer protection with the need to allow flexibility to innovate. They also will complement industry efforts to better understand risks and benefits, particularly those that are intangible. For example, the Future of Privacy Forum (FPF) has published guidance for organizations to weigh the benefits of new or expanded data processing against attendant privacy risks.[131] FPF found that current Privacy Impact Assessment practice helps quantify privacy risks but does not provide sufficient information regarding benefits. Thus, FPF recommends that decision-makers engage in a Data Benefit Analysis that balances big data benefits against privacy risks.

For decades, executive branch agencies in the United States have been required to "(1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) tailor [their] regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations; (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public."[132] President Obama enhanced these principles, directing agencies to, among other things, "identify and consider regulatory approaches that reduce burdens and maintain flexibility and freedom of choice for the public" where permitted by law.[133] Agencies establishing the regulatory framework for the IoT – whether within the Executive Branch or not – should take these mandates to heart and subject proposed requirements to searching evaluation before incurring the costs that always accompany regulatory "solutions."

Second, the primary goal of any IoT policy regime should be to promote innovation. Innovation "has been America's strength for many reasons: our 'can-do' attitude; a free-market system that rewards savvy risk-takers; an educational system that encourages questions rather than rote learnings; our First Amendment, which promotes different views without government censorship; our heterogeneous society; and our willingness to treat failure as a learning experience, rather than a badge of dishonor."[134] If the American people are free to choose their own ideas and pursue their opportunities, we can bring our economy back to life from the ground up," and "one of the great miracles of innovation is that it breeds more innovation."[135] As President Barack Obama observed in his 2011 State of the Union address: "The first step in winning the future is encouraging American innovation…[W]hat America does better than anyone else…is spark the creativity and imagination of our people…In America, innovation doesn't just change our lives. It is how we make our living." Further, "our free enterprise system is what drives innovation."

Policymakers have expressly recognized that innovations in the use of big data can offer solutions to major societal concerns.[136] And of course, innovation's central importance is recognized across the political spectrum: Economists from Joseph Schumpeter to Milton Friedman have championed the role of innovation in creating value and improving lives. Innovation lies at the heart of our nation's productivity and competitiveness, and fuels the economic engine that has raised Americans' standard of living throughout the country's history. By all accounts, policies that foster innovation may be more important than ever. As a recent policy paper from the Progressive Policy Institute put it, "encouraging innovation is more essential than ever before" because productivity growth has been slowing, with nonfarm business labor productivity down from three percent to 1.3 percent between 2005 and 2015, due largely to declining innovation.[137] And the libertarian Cato Institute has called the freedom to innovate "the secret sauce that powered the information revolution."[138]

Third, if policymakers decide that some form of oversight is appropriate in a given case, they should proceed with caution, favoring self-regulation over command-and-control on determining how the outcomes are achieved. CTA and similar groups have long been committed to solutions that marry industry expertise, stakeholder involvement, and the flexibility required by a fast-changing marketplace. Standards ensure that technical issues are addressed in cooperative forums, principally by technologists rather than attorneys, and often eliminating any need for regulatory mandates. A wide variety of groups develop and enforce tailored industry codes of conduct that hold bad actors to account without undermining innovation, and these groups follow due process safeguards.[139]

Consistent with these principles, policymakers should reject mandates that would distort the IoT's trajectory and undercut the growth of offerings that would expand consumers' welfare. In particular, they should reject actions that favor one platform or technology over another or create or expand uncertainty, and should foreswear excessively punitive enforcement penalties.[140] In the case of the IoT, incorrect, unnecessary, or premature mandates have the potential to distort the marketplace in a way that may disadvantage the U.S. on a globally competitive basis. They could delay, dis-incentivize or prevent the development of new and superior technologies that would do better to improve our health outcomes, energy conservation efforts, or highway safety (to take just three examples). While protection of consumers should always remain at the forefront of regulators' minds, government must refrain from over-reaching enforcement actions that harm consumers by mandating a specific technology, increasing the cost of providing service, or entering a sector without providing commensurate consumer benefit. Self-regulatory approaches often solve the problems occasioned by market failure while skirting the corresponding problems posed by inflexible governmental mandates. Thus, if policymakers believe the market alone will not produce optimal results, they should turn to these modern-day approaches rather than the top-down dictates far more appropriate for a bygone era.

Traps for the Unwary. Just as important as what policymakers should do in considering IoT regulation is what they should *not* do.

First, policymakers must avoid the temptation to select winners and losers in the marketplace, opting instead for technologically neutral rules over platform-specific mandates. For the marketplace to work – and for industry to develop in accordance with the needs of consumers rather than the demands of regulators – any regulation must apply equally to similarly situated providers, irrespective of the technologies they use to provide service. Rules that target specific technologies distort the market by privileging one offering over another based on factors other than the benefits and costs associated with each. This problem was well illustrated by recent state bills that create separate "crimes" for offensive operations using unmanned aircraft systems when such actions are crimes under existing law.[141] Instead, policymakers should promote flexibility in the design and operation of new offerings, thereby letting sound engineering and business planning govern.

Second, policymakers should forswear open-ended rules that create or expand uncertainty in the marketplace. Governmental actors may prefer broad mandates on the grounds that malleable rules preserve the flexibility to invalidate a broad range of behaviors as the industry develops, but this is precisely the reason why they must swear off such rules. Just like vague encumbrances on free expression, imprecise or overbroad mandates relating to technology tend to chill behavior that is both lawful and socially beneficial.[142] In the case of the IoT, open-ended mandates could delay or prevent the development of new technologies that would improve our health outcomes, energy conservation efforts, or highway safety (to take just three examples), all because a decision-maker could later interpret an overly ambitious legal proscription in a way that limits, conditions, or bars its use. Policymakers must not actively discourage or burden new offerings that Americans demand through use of such mandates.[143] Indeed, policymakers should embrace incremental change, which takes into account changes in industry practice and consumer perception, and may also wish to address, on a case-by-case basis, specific regulatory sunsets to ensure that any requirements remain narrowly tailored to address actual harms.

Third, while protection of consumers should always remain at the forefront of regulators' minds, government must refrain from over-reaching and punitive enforcement actions that harm consumers by increasing the cost of providing service and raise barriers to entry without providing any commensurate consumer benefit. To be sure, entities that violate easily understood requirements or prohibitions should be called to account: These bad actors distort competition and their behavior harms those who play by the rules[144]. But when the rules are unclear – or, worse, when those in power adopt a novel interpretation that the governed could not have anticipated – punishment serves no purpose: It cannot act as a deterrent, because one cannot be deterred from doing that which one does not know is forbidden. And it can serve no rational punitive interest, because there is no fair basis for punishing an action that the perpetrator could not have known to be unlawful. Further, even when it was (or should have been) clear that a party was acting unlawfully; the punishment should be calibrated to the harm, if any, inflicted. Wildly disproportionate penalties serve only to drive up costs and, in turn, the prices consumers pay for associated products and services. They therefore are inimical to sound public policy, and should be avoided.

Fourth, Policymakers and regulators should avoid creating regulatory "silos" that confuse industry and consumers. Instead, regulatory responsibilities should be clarified in order to avoid duplication among agencies. CTA supports implementation of a consistent approach on privacy and security, building on the expertise of cross-cutting agencies such as the FTC, NIST and NTIA and other agencies, as appropriate.

***

In the words of the non-profit, non-partisan Center for Data Innovation:

> The Internet of Things presents an enormous opportunity for achieving economic and social benefits; however, maximizing those benefits will require smart policy decisions. In particular, there is a need for policymakers to break away from old ways of thinking about data as something to be tightly controlled, and instead view it as a valuable resource to harness for social good...Given the many opportunities available for the Internet of Things to make a significant impact on existing societal challenges, policymakers should be some of the most prominent champions of this technology.

The principles set out above, and throughout this White Paper, are designed to aid policymakers in assuming that mantle, facilitating the IoT's rise, and ushering in a new era of American productivity and innovation.

Conclusion

Technology is changing our lives for the better – helping us live healthier lives, improving our efficiency at work and home, connecting us to loved ones around the globe and keeping us safer wherever we go. The U.S. has a chance to harness the specific opportunities the IoT offers to bring significant consumer, business and societal benefits to the nation and solidify our global leadership in technology innovation and deployment.

Policymakers should carefully consider – and aggressively accelerate – the positive steps government can take to promote IoT innovation, growth and deployment such as making more spectrum available and harmonizing federal agency interaction. Meanwhile, policymakers should refrain from broad regulatory action that would derail or delay new IoT applications. Self-regulatory and other consensus-driven industry efforts allow stakeholders to address discrete, specialized issues that may arise in a practical and flexible manner and without the same risks to competition and innovation – these should be the default institutional mechanism for the IoT.

For the IoT to flourish generally – and for new, never-before-imagined IoT applications to positively impact and improve our lives – government must partner with industry to eliminate barriers to innovation, exercise regulatory humility by considering any regulatory actions in light of greater economic impacts and embrace industry self-regulatory efforts that can address concerns as they arise without inhibiting innovation.

The Internet of Things will connect virtually everything, and CTA welcomes the opportunity to work with policymakers and other stakeholders to ensure we leverage the IoT's maximum potential today and in the future.

[1] Consumer Technology Association (CTA), *U.S. Consumer Technology Sales and Forecasts* (July 2016), https://www.cta.tech/Research-Standards/Reports-Studies/Studies/2016/U-S-Consumer-Technology-Sales-and-Forecasts-(July.aspx; Grand View Research, *IoT Market Analysis By Component (Devices, Connectivity, IT Services, Platforms), By Application (Consumer Electronics, Retail, Manufacturing, Transportation, Healthcare) And Segment Forecasts To 2022* (Apr. 2016), http://www.grandviewresearch.com/industry-analysis/iot-market ("Grand View Research").

[2] Press Release, CTA, *CES 2016 Opens with Technology Changing the World* (Jan. 7, 2016), http://www.ces.tech/News/Press-Releases/CES-Press-Release.aspx?NodeID=2d11a459-e026-409e-a828-3d0e9212cb68.

[3] Cees Links, *Family@Home Transforms Smart Houses into Smart Homes*, GreanPeak, 1-4 (2015), http://www.greenpeak.com/press/PressKit/2015GreenPeakWhitepaperFamilyatHome.pdf.

[4] Rich McCormick, *Whirlpool's New Smart Appliances Have Amazon Dash Built In*, The Verge (Jan. 4, 2016, 2:09 AM), http://www.theverge.com/2016/1/4/10706978/whirlpool-smart-washer-dryer-amazon-dash-ces-2016.

[5] Nicholas Fearn & Sophie Charara, *Tech for good: The wearable tech projects and devices trying to save the world*, WAREABLE (Sept. 16, 2016), https://www.wareable.com/saves-the-day/the-best-wearables-for-good-1969.

[6] *See, e.g.*, *IoT Healthcare Solutions*, KAA, http://www.kaaproject.org/healthcare (in part detailing telehealth and remote patient monitoring capabilities); *see also* James Manyika *et al.*, *Unlocking the Potential of the Internet of Things*, McKinsey & Company (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world ("in 2025 remote monitoring could create as much as $1.1 trillion a year in value by improving the health of chronic-disease patients").

[7] *See, e.g.*, *AT&T and Permobile Unveil the Connected Wheelchair Proof of Concept at CTIA*, AT&T Newsroom (Sept. 8, 2015), http://about.att.com/story/att_permobil_unveils_connected_wheelchair.html; *Furtwangen University develops "IoT Walker" and "IoT Wheelchair" using PTC's ThingWorx*, ThingWorx, https://www.thingworx.com/wp-content/uploads/2016/04/Furtwangen_Case_Study_Final.pdf.

[8] Dan Seifert, *Intel and Oakley made Sunglasses that talk to you*, The Verge (Jan. 5, 2016, 10:22 PM), http://www.theverge.com/2016/1/5/10721146/intel-oakley-radar-coaching-sunglasses-ces-2016.

[9] *Hexoskin's biometric-tracking shirt can do more than your Fitbit (hands-on)*, CNET (Jan. 6, 2016, 1:57 PM), http://www.cnet.com/products/hexoskin-smart-shirt.

[10] Mat Smith, *Intel's conceptual Adrenaline Dress gets upset when you do*, Engadget (Jan. 6, 2016), https://www.engadget.com/2016/01/06/intels-conceptual-adrenaline-dress-gets-upset-when-you-do.

[11] Roger Cheng, *Oh, poop. Baby tech rattles a dad-to-be*, CNET (Jan. 10, 2016, 5:00 AM), http://www.cnet.com/news/oh-poop-baby-tech-rattles-a-dad-to-be.

[12] Christina Bonnington, *People Either Love or Hate This Controversial New Baby Gadget*, Refinery29 (Oct. 20, 2015, 11:00 AM), http://www.refinery29.com/2015/10/95982/versame-wearable-tracks-words.

[13] Anastasia Albanaese-O'Neill, *New diabetes devices improve connectivity, but patient, provider education needed*, Healio Endocrine Today (Feb. 2016), http://www.healio.com/endocrinology/diabetes/news/print/endocrine-today/%7B8e107cf3-aa06-4f92-88c5-452d83099333%7D/new-diabetes-devices-improve-connectivity-but-patient-provider-education-needed.

[14] Ben Coxworth, *Ehang 184 drone could carry you away one day*, New Atlas (Jan. 6, 2016), http://newatlas.com/ehang-184-aav-passenger-drone/41213.

[15] Press Release, BMW Group, *BMW Motorrad Presents Concepts for Motorcycle Laser Light and Helmet with Head-up Display* (Apr. 1, 2016), https://www.press.bmwgroup.com/global/article/detail/T0247812EN/bmw-motorrad-presents-concepts-for-motorcycle-laser-light-and-helmet-with-head-up-display-innovative.

[16] *See, e.g.*, Harriet Green, *Getting Onboard the Future of Transportation Today*, IBM THINK (June 16, 2016), http://asmarterplanet.com/blogs/think/2016/06/16/ibm-olli (detailing Local Motors' autonomous "Olli" vehicle, which "leverages IBM Watson Internet of Things (IoT) to analyze the massive volume of transportation and rider awareness data from more than 30 sensors embedded throughout the vehicle and provide the interface and platform for interaction between the passengers and Olli"); *see also Local Motors Debuts the First Self-Driving*

Vehicle to Tap the Power of IBM Watson, IBM, http://www.ibm.com/internet-of-things/iot-solutions/iot-automotive.

[17] Given that consumer attitudes sometimes can lag behind technological capabilities, there may be products and services on the market today – or poised for launch – that will take months or even years to emerge as game-changers.

[18] *See, e.g.*, Alex Reynolds, *Wellness Data Guiding Principles*, CTA i^3 42 (Nov./Dec. 2015), http://mydigimag.rrd.com/publication/?i=280050 (It follows that if government regulates data, it effectively will regulate devices).

[19] Grand View Research.

[20] Rep. Bob Latta (R-OH) and Rep. Peter Welch (D-VT), *The Internet of Things has the potential to be the engine that powers our economy for decades to come,* The Hill Congress Blog (May 31, 2016, 9:01 AM), http://thehill.com/blogs/congress-blog/technology/281495-the-internet-of-things-has-the-potential-to-be-the-engine-that.

[21] Afua Bruce, Dan Correa, and Suhas Subramanyam, *Internet of Things: Examining Opportunities and Challenges*, White House Blog (Aug. 30, 2016, 7:15 PM), https://www.whitehouse.gov/blog/2016/08/30/internet-things-examining-opportunities-and-challenges.

[22] Cisco, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, 3 (Apr. 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (By some estimates, there will be as many as 50 billion connected devices worldwide by 2020); *see also* Organization for Economic Cooperation and Development, *Machine-to-Machine Communications Connecting Billions of Devices*, OECD Digital Economy Papers, 7-8 (Jan. 2012), http://www.oecd-ilibrary.org/science-and-technology/machine-to-machine-communications_5k9gsh2gp043-en (over the next decade, as the cost of inexpensive, small sensors continues to decline and more Internet Protocol ("IP") addresses become available to connect devices to the Internet, the number of connected devices will explode. These sensors and actuators will continue to connect "things" that are fixed and mobile, large and small, animate and inanimate, including home appliances, industrial and agricultural equipment, livestock, automobiles, parking meters, bike rental stations, roads, highway signs, traffic lights, retail merchandise, heart monitors, and ingestible health monitoring devices).

[23] *See* Fitbit, *Success Stories*, https://blog.fitbit.com/category/be-inspired/success-stories.

[24] *See* Nest, *Nest Protect customer stories*, https://nest.com/blog/2016/01/22/nest-protect-customer-stories.

[25] *See* Vivint.SmartHome, *Our Customers*, http://www.vivint.com/company/customer-stories.

[26] *See* Bryan Urban, Kurt Roth, and Chimere (David) Harbor, *Energy Savings from Five Home Automation Technologies: A Scoping Study of Technical Potential*, Fraunhofer USA (April 2016), https://www.cta.tech/CTA/media/policyImages/Energy-Savings-from-Five-Home-Automation-Technologies.pdf ("*Home Automation Technologies*").

[27] CTA, *Active Aging Study*, CTA Report 1, 6 (Mar. 2016), https://www.cta.tech/Research-Standards/Reports-Studies/Studies/2016/Active-Aging-Study.aspx ("*Active Aging Study*").

[28] *Id.* at 66-68; Steve Ewell, *Smart Homes for Long Lives*, CTA i^3 46 (Sept./Oct. 2015), http://mydigimag.rrd.com/publication/?i=272619&p=48 (also noting that programs, such as the CTA Foundation-supported Selfhelp Virtual Senior Center, is "using technology to reconnect homebound seniors").

[29] *Active Aging Study* at 6.

[30] See Jim Miller, *How to Keep Tabs On an Elderly Parent with Video Monitoring,* The Huffington Post (Jan. 11, 2016, 8:36 AM), http://www.huffingtonpost.com/jim-t-miller/how-to-keep-tabs-on-an-el_b_8954044.html.

[31] *See, e.g.*, CTA Foundation, Our Work, https://www.cta.tech/CTA-Foundation/Our-Work.aspx ("CTA Foundation"); *see also* CTA Foundation (quoting a Senior Planet member, "This week I was awarded my 100th Elance job! I have retained my five-star average, and now have six repeat clients, and my latest ranking as of last week is No. 76 out of the 239,000 writers registered with the site worldwide. Prior to my OATS training, I had never even heard of Elance, but through your classes I gained the skills and confidence to give it a try.").

[32] CTA, *2015 Sustainability Report: Innovating a Better World*, CTA Report 1, 44 (2015), http://content.ce.org/SReport2016/CTA_SR_2016/report-builder/_pdf/CTA_2015_SR.pdf ("*Innovating a Better World*").

[33] *See*, *e.g.*, Shalene Gupta, *For the disabled, smart homes are home sweet home*, Fortune (Feb. 1, 2015, 6:00 AM), http://fortune.com/2015/02/01/disabled-smart-homes ("For years, [Steve O'Hear, who uses an electrical wheelchair,] had to rely on someone else to turn the lights on–that is until he installed Internet-connected lights that he could turn on with his smartphone.").

[34] In particular, the CTA Foundation is partnering with the Gallaudet University Technology Access Program to use IoT to enable alerts for people are deaf or hard of hearing.

[35] *Innovating a Better World* at 44.

[36] *See* Darren Samuelsohn, *What Washington really knows about the Internet of Things*, Politico (June 29, 2015, 5:25 AM), http://www.politico.com/agenda/story/2015/06/internet-of-things-caucus-legislation-regulation-000086.

[37] Public Knowledge and the Open Technology Institute at New America, *Petition for Rulemaking and Request for the Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.9925 GHz Band (5.9 GHz Band)*, Docket No. RM-11771 (filed June 28, 2016).

[38] The FTC approaches the IoT by convening workshops and issuing business guidance; it can also bring enforcement actions under its general authority to prohibit unfair and deceptive acts and practices. Notably, the FTC believes that IoT-specific rules are unnecessary at this time. *See* FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World*, FTC, 48-49 (Jan. 2015) ("FTC IoT Report") (agreeing that there is "great potential for innovation" in the IoT and that "legislation aimed specifically at the IoT at this stage would be premature").

[39] For example, sector-specific privacy rules adopted by sector-specific agencies such as NHTSA or the FCC could create a patchwork of inconsistent privacy requirements across the IoT space. In contrast, allowing the FTC to continue its role as the primary privacy enforcer in the United States will ensure that all companies are treated in a consistent manner. *See id*.

[40] Alan Davidson & Linda Kinney, *Fostering Investment and Innovation in Smart Cities and the Internet of Things (IoT)*, Nat'l Telecomm. & Info. (Feb. 25, 2016, 3:52 PM) ("Davidson & Kinney"), https://www.commerce.gov/news/blog/2016/02/fostering-investment-and-innovation-smart-cities-and-internet-things-iot (this "growing global patch of regulation threatens to increase costs and delay the launch of new products and services", which "in turn, could dampen investment").

[41] *See The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Request for Public Comment, Docket No. 1603311306-6306-01, RIN 0660-XC024, 81 Fed. Reg. 19,956 (Apr. 6, 2016) ("NTIA RFC"); Comments of CTA, Docket No. 1603311306-6306-01 at 8, http://1.usa.gov/1Y7tVEU.

[42] FTC IoT Report at 10-18.

[43] *Id*. at 10.

[44] *Id*. at 14.

[45] *See* Intel, *Policy Framework for the Internet of Things (IoT)* (2014), http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/poli-cy-iot-framework.pdf (describing the value to the U.S. economy of the U.S. tech sector taking a leading role in the global IoT market).

[46] Ringier Metalworking, *Smart Manufacturing in China*, industrysourcing (Sept. 5, 2015, 11:09 AM), http://www.industrysourcing.com/article/smart-manufacturing-china.

[47] Sara Zaske, *Germany's vision Industrie 4.0: The revolution will be digitized*, ZDNet (Feb. 23, 2015, 8:33 AM), http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised.

[48] Press Release, CTA, *Tech Innovation Key to President's SOTU Vision, Says Consumer Technology Association* (Jan. 12, 2016), https://www.cta.tech/News/Press-Releases/2016/January/Tech-Innovation-Key-to-President-s-SOTU-Vision,-sa.aspx.

[49] CTA, *Innovation Scorecard* (2016), https://www.cta.tech/News/InnovationScorecard.aspx.

[50] Press Release, CTA, *Innovation on the Rise: More States Adopting Pro-Innovation Policies, According to Consumer Technology Association's 2016 Innovation Scorecard* (Feb. 2, 2016), https://www.cta.tech/News/Press-Releases/2016/February/Innovation-on-the-Rise-More-States-Adopting-Pro-In.aspx.

[51] Press Release, The White House, *FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services* (Sept. 14, 2015), http://1.usa.gov/1MttsZD (The new capabilities and services made possible by the IoT require advancement and investment in our current infrastructures in order to securely deliver, grow, and scale adoption. Our current networks do not have the capacity to transmit, secure, or store the explosion of data that is being generated by the fifty billion estimated devices connecting by 2020.).

[52] Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 STAT. 1312, (Dec. 4, 2015).

[53] Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, Prepared Remarks at the TDI Conference (Aug. 20, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-334979A1.pdf ("I met a deaf student at the Rochester Institute of Technology, who is exploring ways to use the platform to leverage the Internet of Things to give her notifications for sounds around the house – such as when a microwave or washer/dryer is done or the water is left running.").

[54] Alan Rose *et al.*, *How the Internet of Things Will Enable Vast New Levels of Efficiency*, ACEEE (2014), http://aceee.org/files/proceedings/2014/data/papers/9-832.pdf.

[55] U.S. Green Building Council, *About*, http://www.usgbc.org/about; U.S. Green Building Council, *LEED*, http://leed.usgbc.org.

[56] *See Home Automation Technologies* (evaluating just five approaches to home automation that can be implemented in the vast majority of homes and finding significant potential energy savings); Press Release, CTA, *Home Automation, IoT Could Cut Energy Consumption 10 Percent CTA Study* (May 19, 2016), https://www.cta.tech/News/Press-Releases/2016/May/Home-Automation,-IoT-Could-Cut-Energy-Con-sumpt-%281%29.aspx.

[57] *See* Intel, *The Internet of Things (IoT) and Automotive & Transportation Policy Principles* (2014), http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-automotive-transportation.pdf.

[58] Tim Berners-Lee: The year open data went worldwide (Mar. 2010), https://youtu.be/3YcZ3Zqk0a8 (explaining the benefits of open data, and government-released data in particular).

[59] *Tax Implications of the Internet of Things*, The Wall Street Journal: Deloitte Insights (Jan. 6, 2016, 12:01 AM), http://deloitte.wsj.com/cfo/2016/01/06/tax-implications-of-the-internet-of-things.

[60] Adams B. Nager & Robert D. Atkinson, *Debunking the Top Ten Arguments Against High-Skilled Immigration*, Information Technology & Innovation Foundation (Apr. 2015), http://www2.itif.org/2015-debunking-myths-high-skilled.pdf?_ga=1.42898860.847894678.1456315207.

[61] Ruth E. Wasem, *Immigration of Foreign Nationals with Science, Technology, Engineering, and Mathematics (STEM) Degrees*, Congressional Research Service, 3-4 (Nov. 26, 2012), https://www.fas.org/sgp/crs/misc/R42530.pdf ("*STEM Degrees*"); *see also* Drew DeSilver, *Growth from Asia Drives Surge in U.S. Foreign Students*, Pew Research Center (June 18, 2015), http://www.pewresearch.org/fact-tank/2015/06/18/growth-from-asia-drives-surge-in-u-s-foreign-students.

[62] *See STEM Degrees*. Supplying Knowledge-Based Immigrants and Lifting Levels of STEM Visas Act, H.R. 2131, 113th Cong. (2014). Among other things, the SKILLS Visa Act would make up to 55,000 visas available to employers in FY2016 and subsequent fiscal years to hire qualified immigrants who hold a doctorate degree in a STEM field from a U.S. institution if there are an insufficient number of appropriately qualified U.S. citizens to fill these positions. Any visas that are not used for doctorate-level STEM graduates would be available to masters-level STEM graduates.

[63] *Id*. Immigration Innovation or I-Squared Act of 2015, S. 153, 114th Cong. (2015). Among other things, the I-Squared Act more than doubles the number of H-1B visas available each year and streamlines the visa acquisition and renewal process by reforming various currently applicable bureaucratic requirements.

[64] NTIA RFC at 19,958.

[65] Fed. Trade Comm'n, *Patent Assertion Entity Activity,* FTC Study (October 2016).

[66] Scott Amyx, *Internet of Things Needs Government Support*, InformationWeek (Oct. 9, 2014, 9:06 AM), http://www.informationweek.com/government/leadership/internet-of-things-needs-government-support/a/d-id/1316455 (discussing IoT policies of China, Europe, and South Korea).

[67] *See, e.g.*, Technological Advisory Committee, *Summary of Meeting*, Fed. Commc'ns Comm'n, 120 (Sept. 23, 2014), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92314/TACMeetingSummary9-23-14.pdf (reviewing IoT connectivity technologies).

[68] Cisco, *Cisco Visual Networking Index: The Zettabyte Era: Trends and Analysis*, Table 2 (July 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf.

[69] Murray Slovick, *5G: The Mobile Tech of 2020*, CTA i^3 20 (Nov./Dec. 2014), http://mydigimag.rrd.com/publication/?i=232265.

[70] *See* Gary Arlen, *Game of Gigs*, CTA i^3 17 (Nov./Dec. 2015), http://mydigimag.rrd.com/publication/?i=280050 (noting that consumers will not be "satisfied to leave their high-speed wired homes and go back to 3 Mpbs wireless access," but "wired and wireless will both get faster").

[71] Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update: 2015-2020*, 27 (Feb. 3, 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html ("VNI 2016").

[72] Cisco, *VNI Mobile Forecast Highlights, 2015-2020, United States – Potential M2M Connections, M2M Traffic*, http://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/index.html.

[73] *See, e.g.*, Grace Dobush, *Internet of Things: 13 Innovations for a Smarter Kitchen*, CTA Blog (Apr. 29, 2015), https://www.cta.tech/News/Blog/Articles/2015/April/Internet-of-Things-13-Innovations-for-a-Smarter-Ki.aspx, (highlighting smart kitchen applications that use Bluetooth technology).

[74] Paul Barbagallo, *As "Internet of Things" Evolves, FCC's Spectrum Strategy Will Be Put to the Test*, Bloomberg BNA (Nov. 19, 2014), http://www.bna.com/internet-things-evolves-n17179912070.

[75] CTA, *Unlicensed Spectrum and the American Economy: Quantifying the Market Size and Diversity of Unlicensed Devices*, 2 (2014) ("Unlicensed Spectrum Report"), https://ecfsapi.fcc.gov/file/7521751148.pdf#page=2.

[76] CTA, *Unlicensed Spectrum: The Fuel of Innovation*, CTA i^3 (July 10, 2014).

[77] Unlicensed Spectrum Report at 2.

[78] VNI 2016 at 1.

[79] *Id.*

[80] *Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, Report and Order, 29 FCC Rcd 6567 (2014); *see also* Press Release, CTA, *CEA Praises FCC's Next Steps on TV Incentive Auctions* (Dec. 11, 2014), https://www.cta.tech/News/Press-Releases/2014/December/CEA-Praises-FCC%E2%80%99s-Next-Steps-on-TV-Incentive-Aucti.aspx ("spectrum auction presents a tremendous opportunity to free up this much-needed resource for all the innovators, entrepreneurs and consumers who demand and deserve more spectrum").

[81] *See, e.g.*, *Amendment of Parts 1, 2, 15, 90 and 95 of the Commission's Rules to Permit Radar Services in the 76-81 GHz Band*, Notice of Proposed Rulemaking and Reconsideration Order, 30 FCC Rcd 1625 (2015) (proposing the expansion of vehicular radar in the 76-81 GHz band); *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band, Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959 (2015); *Office of Engineering and Technology Announces the Approval of Google, Inc.'s TV Bands Database System for Operation*, Public Notice, 299 FCC Rcd 11687 (2014) (announcing that Google may operate its "TV bands database system" with new procedures for registration of certain facilities).

[82] For example, the 2014 TAC included an IoT Working Group that developed a common taxonomy and explored IoT spectrum needs. *Technological Advisory Council – 2014*, Fed. Commc'ns Comm'n, https://www.fcc.gov/oet/tac/2014#block-menu-block-4.

[83] Dep't of Transp., Nat'l Highway Traffic Safety Admin., *Federal Automated Vehicles Policy: Accelerating the Next Revolution In Roadway Safety* (Sept. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

[84] Letter from Penny Pritzker, Sec'y, Dep't of Commerce, Anthony Foxx, Sec'y, Dep't of Transp., and Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, to John Thune, Chairman, Senate Committee on Commerce, Sci., and Transp. (Jan. 2016), http://src.bna.com/bZt.

[85] In particular, NTIA has been responsive to the recommendations of the Commerce Spectrum Management Advisory Committee ("CSMAC") with respect to industry-government collaboration and spectrum sharing. Paige R. Atkins, Assoc. Adm'r, Nat'l Telecomm. & Info. Admin., *CSMAC Recommendations: NTIA Preliminary Response* (Dec. 2, 2015) (observing that many of CSMAC's recommended actions are already initiated or are a part of on-going NTIA activities), http://www.ntia.doc.gov/files/ntia/publications/preliminary_ntia_actions_151201.pdf.

[86] *See, e.g.*, Nat'l Telecomm. & Info. Admin., *Bringing Spectrum Sharing to a "Model City"*, NTIA Blog (Apr. 17, 2015), http://www.ntia.doc.gov/blog/2015/bringing-spectrum-sharing-model-city.

[87] See Davidson & Kinney.

[88] Press Release, CTA, *Future IoT Success Depends on Access to Spectrum, CTA Says* (Mar. 3, 2016) (quoting CTA President and CEO Gary Shapiro in support of the Developing Innovation and Growing the Internet of Things Act, https://www.cta.tech/News/Press-Releases/2016/March/Future-IoT-Success-Depends-on-Access-to-Spectrum,.aspx.

[89] *See, e.g.*, Cory Booker, Kelly Ayotte, Brian Schatz, & Deb Fischer, *Policymakers Must Look Ahead to Realize the Potential of the Internet of Things*, CTA i^3 (Mar. 10, 2016), http://mydigimag.rrd.com/publication/?i=295432; Rep. Bob Latta & Mike O'Rielly, *Improving the 5.9 GHz Band to Enhance Unlicensed and Wi-Fi Networks*, The Hill Congress Blog (Mar. 2, 2016, 9:00 AM), http://thehill.com/blogs/congress-blog/technology/271408-improving-the-59-ghz-band-to-enhance-unlicensed-and-wi-fi.

[90] *See, e.g.*, Developing Innovation and Growing the Internet of Things Act, S. 2607, 114th Cong. (2016); MOBILE NOW Act, S. 2555, 114th Cong. (2016); Wi-Fi Innovation Act, H.R. 821 and S. 424, 114th Cong. (2016).

[91] Press Release, Fed. Trade Comm'n, *FTC Kicks Off "Start With Security" Business Education Initiative* (June 30, 2015), https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative. Events were held in San Francisco, Austin, Seattle, and Chicago. *See* Fed. Trade Comm'n, Start with Security – San Francisco (Sept. 9, 2015), https://www.ftc.gov/news-events/events-calendar/2015/09/start-security-san-francisco; Fed. Trade Comm'n, Start with Security – Austin (Nov. 5, 2016), https://www.ftc.gov/news-events/events-calendar/2015/11/start-security-austin; Fed. Trade Comm'n, Start with Security – Seattle (Feb. 9, 2016), https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle; Fed. Trade Comm'n, Start with Security – Chicago (June 15, 2016), https://www.ftc.gov/news-events/events-calendar/2016/06/start-security-chicago. No future events have been announced.

[92] NIST, *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, 1 (Feb. 12, 2014) (explaining that the "[f]ramework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses"), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[93] *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, 80 Fed. Reg. 76,934 (Dec. 11, 2015).

[94] *See, e.g.*, *About CSCC*, U.S. Commc'ns Sector Coordinating Council, http://www.commscc.org/about (describing means of coordination used by the Communications Sector Coordinating Council).

[95] See Fed. Commc'ns Comm'n, *The Communications Security, Reliability and Interoperability Council*, http://transition.fcc.gov/pshs/advisory/csric. CSRIC's working groups have proposed implementation guidance to help communications companies implement the NIST Cybersecurity Framework and continue to recommend and refine best practices in this space. CSRIC IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[96] *See, e.g.*, Multistakeholder Process on Internet of Things Security Upgradability and Patching, 81 Fed. Reg. 64139 (Sept. 19, 2016) (announcing that NTIA will "convene meetings of a multistakeholder process concerning Internet of Things Security Upgradability and Patching," with an immediate goal "to develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers"); Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14,360, 14,363 (Mar. 19, 2015) (recognizing that traditional regulation in this context is "difficult and inefficient" in light of the "pace of innovation in the highly dynamic digital ecosystem"); *Id.* at 14,365 (stating that "[i]n the digital ecosystem, the rapid pace of innovation often outstrips the ability of regulators to effectively administer key policy questions," and that "[o]pen, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive"); Angela Simpson, Deputy Assistant Sec'y of Commerce for Commc'ns and Info., Nat'l Telecomm. & Info. Admin., Remarks at the Vulnerability Research Disclosure Multistakeholder Process (Sept. 29, 2015) ("it is not our job to tell you what to do. NTIA will not impose its

views on you. We will not tip the scales. We are not regulators. We are not developing rules. We do not bring enforcement actions. Instead, we are in a unique position to encourage you to come together, to cooperate, and to reach agreement on important issues"), https://www.ntia.doc.gov/speechtestimony/2015/remarks-deputy-assistant-secretary-angela-simpson-vulnerability-research-disclo.

[97] Building Security in Maturity Model (BSIMM), *About BSIMM*, https://www.bsimm.com/about.

[98] *See, e.g.*, Executive Office of the President of the United States, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 (2012) ("Consumer Data Privacy Framework"), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("the Administration believes that multistakeholder processes underlie many of the institutions responsible for the Internet's success").

[99] Press Release, CTA, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx.

[100] For example, the National Cyber Security Alliance and the WiFi Alliance, both of which share some members with CTA, have developed the following resources: http://www.StaySafeOnline.org and http://www.wi-fi.org/discover-and-learn/security.

[101] *See, e.g.*, Accenture Consulting, *Accenture 2016 Consumer Survey on Patient Engagement*, U.S. Report at 21 (2016) ("Patient Engagement Survey"), https://www.accenture.com/t20160629T045303__w__/us-en/_acnmedia/PDF-6/Accenture-Patients-Want-A-Heavy-Dose-of-Digital-Research.pdf.

[102] PwC, *Top Health Industry Issues Of 2016* at 1 (Dec. 2015) ("*Top Health Industry Issues Of 2016*"), https://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/2016-us-hri-top-issues.pdf.

[103] Patient Engagement Survey at 14 (describing the types of people and institutions that should and should not have access to one's electronic health records).

[104] Melinda Beck, *How Telemedicine Is Transforming Health Care*, Wall Street Journal (June 26, 2016 10:10 PM), http://www.wsj.com/articles/how-telemedicine-is-transforming-health-care-1466993402.

[105] In some cases, consumers have conflicting desires. Often, consumers prefer technologies that are multifunctional (e.g., smart watches versus fitness trackers), but those multiple functions may require data portability and interoperability and thereby give rise to consumer privacy concerns. Companies recognize the challenges in striking a balance that promotes and preserves consumer trust, often working to achieve this through incremental changes based on direct customer feedback.

[106] Susan Taplinger, *The Plain Facts: Why Self-Regulation Works Better than Government Regulation*, The DMA (May 9, 2014), http://thedma.org/blog/advocacy/the-plain-facts-why-self-regulation-works-better-than-government-regulation.

[107] Consumer Data Privacy Framework at 23.

[108] *Id.*

[109] *See, e.g.,* Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising*, The Information Technology & Innovation Foundation, 5-6 (Dec. 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

[110] *Id.* at 6.

[111] Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things"*, The Future of Privacy Forum, 11 (Nov.19, 2013), https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[112] Consumer Data Privacy Framework at 23.

[113] *Id.*

[114] Open Connectivity Foundation, About Open Connectivity Foundation, https://openconnectivity.org/about (last visited Nov. 1, 2016) ("The Open Connectivity Foundation (OCF) is creating a specification and sponsoring an open source project to make this possible.... OCF will help ensure secure interoperability for consumers, business, and industry.").

[115] *See* Institute of Electrical and Electronics Engineers, About IEEE, http://www.ieee.org/about/index.html (last visited Nov. 1, 2016) ("IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE and its members inspire a global community to innovate for a better tomorrow through its highly-cited publications, conferences, technology standards, and professional and educational activities.").

[116] *See* Internet Engineering Task Force, Mission Statement, http://ww.ietf.org/about/mission.html (last visited Nov. 1, 2016) ("The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.... We make standards based on the combined engineering judgement of our participants and our real-world experience in implementing and deploying our specifications.").

[117] Barb Darrow, *This Mega Tech Consortium Wants to Connect All Our Devices*, Fortune (Oct. 10. 2016 1:57 PM), http://fortune.com/2016/10/10/open-connectivity-foundation-wants-to-connect-all-devices.

[118] Press Release, CTA, CTA Technology & Standards Forum to Focus on Security, Data and Efficiency (April 5, 2016), https://www.cta.tech/News/Press-Releases/2016/April/CTA-Technology-Standards-Forum-to-Focus-on-Securit.aspx.

[119] Press Release, CTA, IoT Security Front and Center at Next CTA Technology & Standards Forum (August 2, 2016), https://www.cta.tech/News/Press-Releases/2016/August/IoT-Security-Front-and-Center-at-Next-CTA-Technolo.aspx.

[120] *See* CTA, *Guiding Principles on the Privacy and Security of Personal Wellness Data*, (Oct. 15, 2015), https://fpf.org/wp-content/up-loads/2015/10/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf; Press Release, CTA, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx.

[121] The Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology* (Dec. 2015), https://fpf.org/wp-content/up-loads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

[122] *See* Dep't of Homeland Security, About NSTAC, https://www.dhs.gov/about-nstac.

[123] The Alliance of Automobile Manufacturers, *Automotive Privacy: Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers*, (last visited Nov. 1, 2016), http://www.autoalliance.org/auto-issues/automotive-privacy.

[124] Nat'l Telecomm. & Info., Multistakeholder Process: Unmanned Aircraft Systems (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

[125] *See* Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, Tech Dirt (Aug. 25, 2015), https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

[126] *See* Michael Mandel & Diana Carew, *Innovation in a Rules-Bound World: How Regulatory Improvement Can Spur Growth*, Progressive Policy Institute 1, 2 (Dec. 2015) ("Mandel & Carew"), http://www.progressivepolicy.org/issues/economy/innovation-in-a-rules-bound-world-how-regulatory-improvement-can-spur-growth ("it is tempting and even easy for regulators to adopt stricter rules to protect against potential dangers, even at the cost of slowing or even suppressing innovation and growth.... However, when the regulators adopt stricter rules to preemptively avert any potential dangers, the costs of these regulations can tend towards outweighing the benefits. Innovation-driven productivity losses come at a great economic cost that must be taken into consideration as well").

[127] Patient Engagement Survey at 21 (reporting consumer preferences for sharing wearable data across several institutions).

[128] *Top Health Industry Issues Of 2016* (noting that 88 percent of consumers are willing to share personal data with their doctor to find new treatments).

[129] *See, e.g.,* Gary Shapiro, *Balancing Consumer Privacy and the Potential of Consumer Technology*, The Hill Congress Blog (Oct. 28, 2015, 7:30 AM), http://thehill.com/blogs/congress-blog/technology/258250-balancing-consumer-privacy-and-the-potential-of-consumer.

[130] *See* Press Release, CTA, *Biometric Technology Enjoys Strong Support from Consumers, Says CTA* (Mar. 30, 2016), https://www.cta.tech/News/Press-Releases/2016/March/Biometric-Technology-Enjoys-Strong-Support-from-Co.aspx. CTA's report on *Biometric Technologies: Understanding Consumer Sentiments* is available upon request.

[131] *See* Benefit-Risk Analysis for Big Data Projects, Future of Privacy Forum (2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnaly-sis_FINAL.pdf.

[132] *See* Exec. Order No. 13, 563, 76 Fed. Reg. 3,821 (Jan. 18, 2001) (summarizing Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993)).

[133] *Id*.

[134] Gary Shapiro, *Ninja Innovation: The Ten Killer Strategies of the World's Most Successful Businesses* 31 (2013).

[135] *Id.*, 169-70, 180.

[136] Kate Dvorak, *Karen DeSalvo: We must 'roll up data into big data' for population health management,* Fierce Healthcare, (Mar. 12, 2015) http://www.fiercehealthit.com/story/karen-desalvo-we-must-roll-data-big-data-population-health-management/2015-03-12.

[137] *See* Mandel & Carew.

[138] *See* Adam Thierer, *Embracing a Culture of Permissionless Innovation*, Cato Institute (Nov. 2014), https://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.

[139] *See infra* Section II.J, responding to Questions 16-17.

[140] *See* Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, Tech Dirt (Aug. 25, 2015) ("*The Heavy Hand of Government*"), https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

[141] For example, the California State Legislature considered a bill that would criminalize operating a drone "in a manner that violates an individual's fundamental right to privacy." State Remotely Piloted Aircraft Act, S.B. No. 868, 2015-2016 Sess. (CA 2016). Invasion of privacy is unlawful under California law. *See* Cal. Penal Code § 630-638.53 (2014). *See also* http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

[142] *See* Gary Shapiro, *Why Washington Comes to CES*, Fox News (Dec. 31, 2015), http://www.foxnews.com/opinion/2015/12/31/why-washing-ton-comes-to-ces.html.

[143] *See The Heavy Hand of Government*.

[144] CTA, Bad Actors Shouldn't Cause Us to Overlook IoT Opportunity, Innovation, Says CTA (October 25, 2016), https://www.cta.tech/News/Press-Releases/2016/October/Bad-Actors-Shouldn-t-Cause-Us-to-Overlook-IoT-Oppo.aspx