Daniel Castro
Vice President, Information Technology and Innovation Foundation
Director, Center for Data Innovation

"The Internet of Things: Exploring the Next Technology Frontier"

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

March 24, 2015

Chairman Burgess, Ranking Member Schakowsky, and members of the committee, I appreciate the opportunity to appear before you to discuss the Internet of Things and the opportunities and challenges presented by this technology. My name is Daniel Castro. I am the vice president of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also the director of the Center for Data Innovation, an ITIF-affiliated non-profit research institute focusing on the intersection of data, technology, and public policy.

In my testimony today, I would like to describe the opportunity presented by the Internet of Things to address important economic and societal issues, its unique impact on manufacturing, and the opportunity Congress has to incentivize better privacy and security practices while not stifling innovation.

The Internet of Things Presents an Opportunity to Address Major Economic and Societal Issues

The Internet of Things encapsulates the idea that ordinary objects—from thermostats and shoes to cars and lamp posts—will be embedded with sensors and connected to the Internet.[1] These devices will then send and receive data that can be analyzed and acted upon. As the technology becomes cheaper and more robust, an increasing number of devices will join the Internet of Things. By 2020, industry analysts expect that the total worldwide count of connected devices to exceed 40 billion.[2]

Many of the changes to everyday devices may be subtle and go unnoticed by consumers since "smart" devices, like watches and bridges, look much the same as "dumb" ones. However, the long-term effect of the transition to the Internet of Things could ultimately have an enormously positive impact on individuals, businesses, and society. In particular, the Internet of Things offers solutions to many important real-world problems, including improving health care, public safety, and energy use.[3]

Health Care

The Internet of Things offers new solutions for preventing, screening, and diagnosing a variety of health conditions. Devices allow individuals to monitor every aspect of their health, including weight, body mass, sleep cycles, and daily activity levels. Preventable health conditions constitute 80 percent of overall disease burden and 90 percent of health care costs.[4] By collecting and tracking data about their health, patients are able to identify health problems sooner and get treatment faster. Not only does this cut down on health care costs, it also provides new opportunities for improved quality of life. For example, products like the activity sensors "Lively" can help monitor the health of older adults or people with disabilities, allowing

them to stay in their homes longer and retain their independence.[5] The demand for these types of health-related technologies is growing quickly. Already, 69 percent of American adults track at least one health indicator, and the U.S. market for wireless health monitoring devices is projected to reach $22 billion by 2015.[6] Data from connected devices, such as personal fitness monitors, can provide health officials with unprecedented insights into public health and medical researchers a better understanding of how to treat medical conditions. For example, tracking changes in biometric readings across a city could even help identify the spread of deadly outbreaks, helping public officials better contain diseases and start treating sick individuals earlier.

The Internet of Things is also providing new tools that allow individuals to monitor and manage their health conditions. These devices collect data about existing health conditions, thereby giving individuals and their health care providers more information on which to base health care decisions. For example, smart inhalers remind children to use their inhalers and automatically record each use. The data from these devices can be used to reinforce healthy habits in children, allow doctors to assess the effectiveness of treatments, and notify parents when a refill is needed.[7] Individuals will also be able to use technology to monitor and treat specific conditions. Continuous remote monitoring allows doctors to offer better care to patients when they need it and to make adjustments as necessary, rather than making patients wait until the next appointment. Individuals with diabetes, for example, can use continuous glucose monitoring to learn when their glucose levels get too low or high and to track insulin delivery. Finally, patients can use smart pill bottles like GlowCaps to receive automated alerts when it is time to take a dose. Using these types of notifications can increase rates of medication compliance and make a sizeable dent in the $290 billion annual cost of drug non-adherence in the United States.[8]

Public Safety

The Internet of Things can provide information needed to improve public safety. The availability of real-time data is crucial in an emergency situation since a faster response time can mean the difference between life and death. For example, every minute of delay in responding to someone having sudden cardiac arrest decreases the expected survival rate by 5.5 percent.[9] In homes, connected sensors can improve home safety by detecting fires and other emergencies quickly and reliably and alert authorities sooner.[10] In vehicles, automatic crash response systems can use sensors to detect a crash and then automatically alert emergency responders. These systems can transmit a variety of critical information to responders, including the precise location of the vehicle, the direction the vehicle was traveling, the number and speed of impacts, and whether the vehicle has rolled over. Toyota has even taken this a step further and begun to predict the type and severity of injuries that occupants in a crash likely sustained.[11]

Automatically collecting and sending this information means that appropriate help can arrive sooner, potentially saving lives.[12]

Smart cities make their citizens safer. For example, government agencies can use the Internet of Things to improve the safety of public infrastructure through better monitoring. The Federal Highway Administration has deemed nearly a quarter of all bridges in the country structurally deficient or functionally obsolete, and preventing future disasters such as the collapse of the I-35 Mississippi River Bridge in Minneapolis remains a top public safety priority.[13] Wireless bridge sensors can reduce the risk of accidents by monitoring all aspects of a bridge's health, such as vibration, pressure, humidity, and temperature. Researchers at the University of Maryland, College Park have tested bridge sensors on the I-495 Bridge in Maryland and were able to use data analysis to detect structural changes that had developed after repairs. The system can also send automated alerts by email or text messaging to bridge engineers if an immediate threat is detected.[14]

Energy Use

As a result of growing populations and increasing demand, global energy consumption will rise by over 50 percent over the next thirty years.[15] The Internet of Things will help provide solutions to the global energy challenge by enabling clean energy technologies, creating better energy market dynamics, and optimizing the efficiency of existing products.

The Internet of Things has made some clean energy technologies commercially viable. For example, new wind turbines can use sensor and grid data to operate more efficiently, both bringing down the cost of clean energy production and increasing electricity production. By equipping turbines with sensors and algorithms to analyze the sensor data, companies are able to optimize energy production and keep their turbines running even in variable wind conditions. Wind energy has become increasingly important to the U.S. energy market, and sensor-equipped turbines have helped cut the cost of wind energy from 15 cents per kilowatt hour to 6.5 cents per hour, facilitating the expansion of renewable energy options.[16]

The Internet of Things can also be used to automate and encourage energy-efficient practices in the home and save consumers money. Major appliances, such as electric clothes dryers can use real-time electricity rates to automatically schedule energy-intensive tasks during off-peak hours when electricity is cheaper and more plentiful. Not only can users save twenty to forty dollars per year by time-shifting their energy use, they can also help reduce overall peak demand on the grid; this means fewer power plants have to be built.[17]

Smart devices in the home can also automatically regulate electricity usage based on whether anyone is home.[18] The Nest thermostat, for example, can help homeowners consume up to 20 percent less energy annually by learning the daily routine of its users and their temperature

preferences, and then combining this information with outdoor weather data to tailor the home's heating and cooling settings based on the time of day and whether anyone is home. In addition, products like smart blinds can automatically detect and filter out sunlight; smart heating and cooling systems can maintain different rooms at different temperatures; and smart lighting can automatically adapt to time of day and be controlled from a smartphone to make home life more comfortable.[19] As a result of these technologies, consumers can spend less money on their energy bills.

The Internet of Things Is the Foundation for Smart Manufacturing

Manufacturing is a major part of the U.S. economy, responsible for 12.5 percent of gross domestic product (GDP) and supporting 17.4 million U.S. jobs.[20] Maintaining a strong industrial sector is critical to ensuring future U.S. competitiveness, and the Internet of Things will be a key part of building a healthy manufacturing industry. "Smart manufacturing," as this approach is often called, could create $371 billion in net global value over the next four years.[21] Two important ways the Internet of Things will make U.S. manufacturers more competitive in the global economy are by improving factory operations and managing risk in the supply chain.

First, manufacturers can use data and analytics to improve operations on the factory floor. The rapid growth of low-cost sensor technologies has made nearly every manufacturing process and component a potential data source. As a result, factories can automatically turn off lights and air conditioning when workers leave, shut off valves if sensors detect leaks, and shut down dangerous equipment if sensors detect a malfunction.[22] Innovative manufacturers can use the resulting data sets to gain insights about the physical fabrication process, improving efficiency, increasing yields, and reducing product defects. Raytheon famously keeps track of how many times a screw has been turned in its factories, and other companies are working to collect as much detail about their own processes.[23] Harley Davidson tracks fan speed in its motorcycle painting areas and can algorithmically adjust the fans based on environmental fluctuations.[24] Merck improved one of its vaccines by conducting 15 billion calculations to determine what environmental and process factors influenced the quality of the final product.[25] And Intel uses predictive modeling on data to anticipate failures, prioritize inspections, and cut monitoring costs at its chip manufacturing plants.[26] With so many potential variables to track, no longer should "too little information" be an excuse for waste and loss in the factory environment.

Second, manufacturers can use the Internet of Things to manage their supply chains and more intelligently manage suppliers, distributors, and customers. The interconnected nature of global industrial supply chains creates risk and uncertainty without better data. Companies can use sensors to collect real-time data about their shipments including location, temperature, moisture, and other environmental factors to help ensure quality and optimize logistics. More information can mean the difference between a recall and a successful shipment. The National

Institute of Standards and Technology (NIST) is working on a project to develop standards, methods, and protocols for manufacturing data analytics, a key motivation for which is the increasing demand for more comprehensive supply-chain intelligence.[27]

The Internet of Things helps manufacturers at nearly every step, from their global supply chains to the turn of a screw in their factories. And because a healthier manufacturing sector is an important part of a healthier economy, the benefits of data-driven manufacturing will be felt throughout the country as well.

Congress Should Incentivize Good Privacy and Security Practices But Avoid Harming Innovation

Many new technologies are often met with fear, uncertainty, and doubt, especially by those who are unfamiliar with them or opposed to change. Policymakers cannot afford to succumb to these forces if they expect to enable society to take full advantage of the Internet of Things. In particular, policymakers should be extremely cautious about passing laws on the basis of purely speculative concerns that might not even come to pass, especially when doing so might curtail substantial economic and societal benefits, many of which are already being realized today.[28] As Google's CEO and co-founder Larry Page has noted, public squeamishness over mining of health data likely costs around 100,000 lives a year.[29] Most hypothetical concerns will never become reality because factors such as market forces, cultural norms, and new technologies are likely to intervene. In particular, Congress should act cautiously as it considers rules on privacy and security so as to not impede innovation.

Privacy

A significant amount of data collected by the Internet of Things will not involve information about individuals. Instead, the Internet of Things will collect data about the environment, factories, vehicles, machines, infrastructure, and other electronic devices. For example, a smart refrigerator does not need any personal information to know that it is running low on milk. In addition, when the Internet of Things does collect data about individuals, much of the data will be de-identified and aggregated. However, since some of the data collected by the Internet of Things will be about individuals, policymakers are right to consider how this will impact consumer privacy. In doing so, they should be aware that the Internet of Things has some important differences from past technologies and promote policies that protect consumers while still encouraging beneficial uses of data.

The current system of providing consumers written privacy notices will pose new challenges with the Internet of Things for the simple reason that many Internet-enabled devices will not have displays, will have small displays, or will not directly interact with individuals. While some consumer devices might come packaged with a privacy notice on paper, this may limit the

ability of manufacturers to easily send software updates to the device. Other non-consumer devices, such as parking sensors, roadway sensors, building sensors, or environment sensors, simply might not have an interface through which to share privacy policies with consumers easily. In addition, as more and more devices collect and use data, excessive privacy policy disclosures could end up inundating consumers with undesired notifications they would rather not receive. One solution is for Congress to avoid heavy-handed rules about data collection, and instead closely monitor and restrict uses of personal data that result in identifiable consumer harm. By restricting harmful uses of data, Congress can set clear rules for how consumers are protected while allowing innovators the freedom to create new devices and tackle important societal problems.

Whereas in the past, most innovation occurred before any data was ever collected, in the future data collection will be just the beginning of the innovation process. Many of the potential benefits from the Internet of Things will arise from the ability to analyze, utilize, share, and combine data after it is collected. For example, imagine a wireless device that collects data on a home's plumbing system. One service might use data from pressure sensors installed in a home's plumbing system to detect leaks. Another service might use that same data to monitor the health of an older adult living alone by checking for anomalous behavior, perhaps combined with information from other devices. Consumers will benefit the most if data can be reused for multiple purposes.

Congress should recognize that privacy principles designed for a "small data" world do not work in a "big data" world. In particular, the Fair Information Practice Principles (FIPPs), developed in the 1970s, are not an appropriate foundation for policymaking today. Principles such as data minimization—the idea that an entity collecting data should limit the collection of information to what is directly needed to accomplish a specific purpose—are based on the mistaken belief that it is always possible for an organization to predetermine what information is useful and collect only that minimum amount of information. Data-driven innovation often involves exploration and discovery, sometimes from unexpected data sources.[30] Data-driven innovation is not a routine linear process, but rather it is a creative cycle with multiple feedback loops. Many of the benefits from data come from exploratory analysis that finds new correlations, trends, relationships, and insights that were not obvious at the outset. Restricting data collection with rules that limit data collection could severely curtail the many potential benefits of the Internet of Things.

Security

As consumers and businesses connect more devices to the Internet, it will be more important than ever that these devices incorporate strong security features. It is worth noting that companies already have strong incentives to build secure products. Customers will not continue

to do business with a company known to make insecure products and services. In addition, regulatory agencies such as the Federal Trade Commission have made clear that they will go after companies that are negligent with their cybersecurity practices.[31] Still, Congress has policy levers at its disposal to further incentivize stronger security practices by adopting policies that decrease the cost of strong security and increase the cost of weak security.[32]

Over the past decade, there have been over 5,000 data breaches publicly reported in the United States affecting over 800 million records.[33] Requiring companies to notify consumers in the event of a data breach incentivizes companies to better protect consumer data to avoid expensive and embarrassing revelations about security mishaps. For example, some state data breach laws exempt companies from notifying their customers if consumer data is securely encrypted when hackers access their systems. While most states have data breach legislation, laws vary by state. Congress should pass data breach notification legislation to help standardize this practice. By creating a national standard that preempts state law, Congress can reduce the legal compliance cost companies face from complying with multiple rules and allow them to focus more resources on improving the security of their products.

Congress should also pass cybersecurity information-sharing legislation. By encouraging the public and private sector to share information on cybersecurity threats quickly and efficiently, organizations can proactively respond to threats based on real-time intelligence. Better reporting of cybersecurity threats combined with industry adoption of a voluntary cybersecurity framework may also provide some of the actuarial data needed to spur the development of a more robust cyber risk insurance market. A well-functioning cyber risk insurance market would reward companies for implementing best practices in cybersecurity and penalize those who deviate from them with higher premiums.

Finally, Congress should encourage universities to integrate cybersecurity training into technical degrees so that the next generation of coders and engineers build strong security into products from the outset. In addition, Congress could provide funding for a university to develop a series of massive online open courses on cybersecurity. These courses could cover specialized topics, such as security considerations for wearables or smart homes. By providing current workers access to high-quality cybersecurity training at no cost, Congress can help raise the bar for security across the entire U.S. tech sector.

Conclusion

The success of the Internet of Things will depend in part on the actions of Congress. Not only should policymakers avoid heavy-handed rules that would imposes costs, limit innovation, and slow adoption, they should actively support accelerating the development and deployment of the Internet of Things, such as by creating pilot projects for smart cities, encouraging smart

infrastructure projects, and designing an efficient regulatory review process for wearable health technologies. Just as the success of the Internet today can be credited in part to policymakers actively taking a role to ensure its growth, a similar approach should to be applied to building the Internet of Things.

Congress should help pave the road for innovation by asking the Department of Commerce to develop a national strategy to guide the deployment and adoption of the Internet of Things. In addition, federal agencies involved in specific sectors should develop targeted action plans for particular industries. By doing so, policymakers can ensure that opportunities to use the Internet of Things to address important societal issues, such as health care and public safety, are a top priority. For example, the Department of Housing and Urban Development should develop an action plan to promote smart homes, and the Department of Energy should develop a plan to improve energy efficiency with connected devices. The Internet of Things has the potential to positively impact virtually every industry from agriculture to health care, and the federal government should be an active partner in its development.

Thank you for the opportunity to share with you my thoughts on the Internet of Things. I look forward to answering your questions.

References

1. Daniel Castro and Josh New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 2014, http://www2.datainnovation.org/2014-iot-policy-principles.pdf.
2. Ibid.
3. Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data Innovation, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.
4. "Health Care Statistics," PreventDisease.com, n.d., http://www.preventdisease.com/worksite_wellness/health_stats.shtml (accessed November 13, 2013).
5. "Lively Introduces Activity-Sharing Products that Connect Older Adults and their Families," IoT News Network, April 16, 2013, http://www.iotnewsnetwork.com/body-health/lively-introduces-activity-sharing-products-that-connect-older-adults-and-their-families/.
6. "Making Sense of Sensors: How New Technologies Can Change Patient Care," California HealthCare Foundation, February 2013, http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/M/PDF%20MakingSenseSensors.pdf.
7. "GeckoCap: Simple Asthma Management," GeckoCap, n.d., http://www.geckocap.com/ (access November 13, 2013).
8. "Product," GlowCap, http://www.glowcaps.com/product/ (accessed on November 13, 2013).
9. Mary Larsen et al., "Predicting survival from out-of-hospital cardiac arrest: a graphic model." *Annals of emergency medicine* 22, no. 11 (1993): 1652-1658.
10. Juhwan Oh, Zhongwei Jiang, and Henry Panganiban, "Development of a Smart Residential Fire Protection System, Advances in Mechanical Engineering, Volume 2013, 2013, http://www.hindawi.com/journals/ame/2013/825872/.
11. "Advanced Automatic Crash Notification," Toyota Collaborative Safety Research Center, September 21, 2011, http://www.toyota.com/csrc/advanced-automatic-crash-notification.html.
12. "Emergency," OnStar, accessed November 13, 2013, https://www.onstar.com/web/portal/emergencyexplore?tab=1&g=1.
13. Mike Collins, "Just How Bad Are America's Infrastructure Problems?," Manufacturing.net, April 1, 2014 http://www.manufacturing.net/blogs/2014/04/just-how-bad-are-america%E2%80%99s-infrastructure-problems.
14. Annika McGinnis, "Experts develop sensors to prevent bridge disasters," *Times Dispatch*, September 10, 2012, http://www.timesdispatch.com/news/experts-develop-sensors-to-prevent-bridge-disasters/article_5e5bd991-490a-5fea-b465-07ce07e4dc7e.html.
15. "International Energy Outlook 2013," U.S. Energy Information Administration, 2013, http://www.eia.gov/forecasts/ieo/pdf/0484(2013).pdf.
16. Kevin Bullis, "Novel Designs Are Taking Wind Power to the Next Level," *MIT Technology Review*, February 6, 2013, http://www.technologyreview.com/news/510481/novel-designs-are-taking-wind-power-to-the-next-level/.
17. Michael Graham Richard, "These Smart Clothes Dryers Could Reduce Electricity Demand by the Equivalent of 6 Coal Power Plants," Treehugger, September 29, 2009, http://www.treehugger.com/sustainable-product-design/these-smart-clothes-dryers-could-reduce-electricity-demand-by-the-equivalent-of-6-coal-power-plants.html.
18. Austin Harney, "Smart Metering Technology Promotes Energy Efficiency for a Greener World" Analog Dialogue, Volume 43-01, January 2009, http://www.analog.com/library/analogdialogue/archives/43-01/smart_metering.pdf; Ilana Greene, "Smart Houses Help Reduce Energy Use and Save Money," *Huffington Post*, December 19, 2013, http://www.huffingtonpost.com/ilana-greene/smart-houses-help-reduce-_b_4472919.html.
19. Jason Chen, "Home Automation! What You Need to Know to Not Be Dumb," Gizmodo, September 27, 2010, http://gizmodo.com/5647352/home-automation-what-you-need-to-know-to-not-be-dumb.
20. "What Manufacturing Really Looks Like Today," U.S. Department of Commerce, September 23, 2014, http://www.commerce.gov/blog/2014/09/23/what-manufacturing-really-looks-today.

21. "'Data smart' strategies for customers are yielding 'early but impressive returns,'" Microsoft, May 22, 2014, http://blogs.microsoft.com/firehose/2014/05/22/data-smart-strategies-for-customers-are-yielding-early-but-impressive-returns/.
22. Tony Kontzer, "IoT's supply chain benefits becoming clearer," TechTarget, July 2014, http://searchmanufacturingerp.techtarget.com/feature/IoTs-supply-chain-benefits-becoming-clearer.
23. James Hagerty, "How Many Turns in a Screw? Big Data Knows," *Wall Street Journal*, May 15, 2013, http://www.wsj.com/news/articles/SB10001424127887324059704578472671425572966.
24. "Building Smarter Manufacturing with the Internet of Things," Lopez Research, January 2014, http://www.cisco.com/web/solutions/trends/iot/iot_in_manufacturing_january.pdf.
25. Doug Henschen, "Merck Optimizes Manufacturing With Big Data Analytics," *InformationWeek*, April 2, 2014, http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/merck-optimizes-manufacturing-with-big-data-analytics/d/d-id/1127901.
26. Daniel Castro and Travis Korte, "Data Innovation 101," Center for Data Innovation, November 3, 2013, http://www.datainnovation.org/2013/11/data-innovation-101/.
27. "Real-Time Data Analytics for Smart Manufacturing Systems Project," National Institute of Standards and Technology, October 1, 2013, http://www.nist.gov/el/msid/lifecycle/rtdasms.cfm.
28. Daniel Castro and Travis Korte, "A Catalog of Every 'Harm' in the White House Big Data Report," Center for Data Innovation, July 15, 2014, http://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-the-white-house-big-data-report/.
29. Alex Hern, "Google: 100,000 lives a year lost through fear of data-mining," *The Guardian*, June 26, 2014, http://www.theguardian.com/technology/2014/jun/26/google-healthcare-data-mining-larry-page.
30. For example, a Pinterest data scientist remarked, "As we've grown, we're increasingly able to use historical data that we might not have looked at before to understand large-scale trends on the service and come up with new ideas for the product." See "5 Q's for Andrea Burbank, Search and Data Mining Engineer at Pinterest," Center for Data Innovation, February 23, 2015, http://www.datainnovation.org/2015/02/4077/.
31. "TRENDnet, Inc." Federal Trade Commission, February 7, 2014, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
32. Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene," Information Technology and Innovation Foundation, February 2015, http://www2.itif.org/2015-how-when-regulators-intervene.pdf.
33. "Data Breaches," Identity Theft Resource Center, n.d. http://www.idtheftcenter.org/id-theft/data-breaches.html (accessed March 19, 2015).