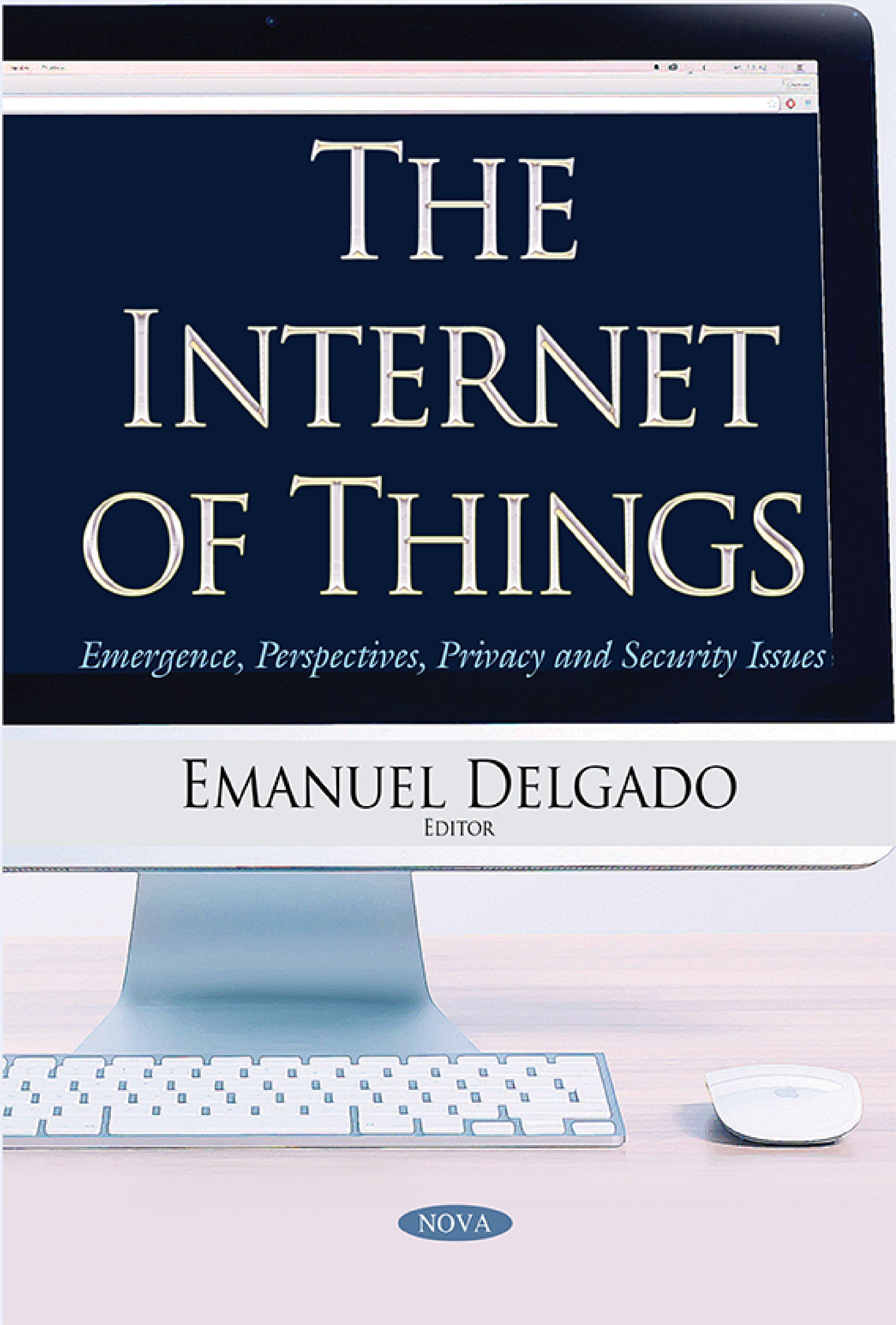
Internet Theory, Technology and Applications



The Internet of Things

Emergence, Perspectives, Privacy and Security Issues

Emanuel Delgado

Editor

NOVA

INTERNET THEORY, TECHNOLOGY AND APPLICATIONS

THE INTERNET OF THINGS

EMERGENCE, PERSPECTIVES, PRIVACY AND SECURITY ISSUES

Internet Theory, Technology and Applications

Additional books in this series can be found on Nova's website
under the Series tab.

Additional e-books in this series can be found on Nova's website
under the e-book tab.

INTERNET THEORY, TECHNOLOGY AND APPLICATIONS

THE INTERNET OF THINGS

EMERGENCE, PERSPECTIVES, PRIVACY AND SECURITY ISSUES

EMANUEL DELGADO
EDITOR

nova publishers
New York

NOTICE TO THE READER

The Publisher has taken reasonable care in the preparation of this book, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book. The Publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the readers' use of, or reliance upon, this material. Any parts of this book based on government reports are so indicated and copyright is claimed for those parts to the extent applicable to compilations of such works.

Independent verification should be sought for any data, advice or recommendations contained in this book. In addition, no responsibility is assumed by the publisher for any injury and/or damage to persons or property arising from any methods, products, instructions, ideas or otherwise contained in this publication.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the Publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Additional color graphics may be available in the e-book version of this book.

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-63482-443-9 (eBook)

Published by Nova Science Publishers, Inc. † New York

CONTENTS

PREFACE

This book discusses the emergence, perspectives, privacy and security issues of IoTs.

Chapter 1 – The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. Six years ago the number of "things" connected to the Internet surpassed the number of people.

Given these developments, the FTC hosted a workshop titled The Internet of Things: Privacy and Security in a Connected World. Workshop participants discussed benefits and potential security and privacy risks associated with the Internet of Things. This report summarizes the workshop and provides staff's recommendations in this area.

Chapter 2 – This is an edited, reformatted and augmented version of a concurring statement to the Federal Trade Commission's Internet of Things report issued by Commissioner Ohlhausen, January 27, 2015.

Chapter 3 – This is an edited, reformatted and augmented version of a dissenting statement to the Federal Trade Commission's Internet of Things report issued by Commissioner Wright, January 27, 2015.

Chapter 4 – It's called the Internet of Things – the burgeoning phenomenon of day-to-day consumer products and services that connect to the Internet. Maybe it's a simple convenience like a home automation system that turns lights on and off remotely. Other innovations have the potential to save lives – for example, a connected car that contacts first responders instantly in case of an accident or a mobile app that allows a patient to share vital signs with a doctor. What distinguishes the Internet of Things is the product's ability to use the Internet to communicate with us, with others, or with other devices.

The Internet of Things has the potential to offer enormous benefits to consumers. Innovative companies are already selling connected devices, apps, sensors, services, etc., unlike anything we've seen before. But businesses need to consider security, too. As with any online activity, it's important to protect consumers' sensitive data from thieves. The Internet of Things, however, adds new security dimensions to consider. For example, an insecure connection could give a hacker access not just to the confidential information transmitted by the device, but to everything else on a user's network. And in the Internet of Things, the risk isn't just to data. If that home automation system isn't secure, a criminal could override the settings to unlock the doors. And just think of the consequences if a hacker were able to remotely recalibrate a medical device – say, an insulin pump or a heart monitor.

Chapter 5 – Testimony of Mike Abbott, General Partner, Kleiner Perkins Caufield & Byers.

Chapter 6 – Testimony of Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology.

Chapter 7 – Statement of Douglas Davis, Vice President and General Manager, Internet of Things Group, Intel.

Chapter 8 – Testimony of Lance Donny, Chief Executive Officer, OnFarm.

Chapter 9 – Testimony of Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 1

INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD[*]

Federal Trade Commission

EXECUTIVE SUMMARY

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff's recommendations in this area.[1] Consistent with the FTC's mission to protect consumers in the commercial sphere and the focus of the workshop, our

[*] This is an edited, reformatted and augmented version of a staff report, issued by the Federal Trade Commission, January 2015.

discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-tomachine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-indepth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such an approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer’s data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.[2]

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns. For example, a framework could set forth permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.[3]

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its

authority to take action against any actors it has reason to believe are in violation of these laws.

- **Consumer and business education:**
  The Commission staff will develop new consumer and business education materials in this area.
- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.
- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

BACKGROUND

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things (“IoT”), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn’t a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people.[1] Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[2] Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.[3] Three and one-half billion sensors already are in the marketplace,[4] and some experts expect that number to increase to trillions within the next decade.[5] All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.[6] By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video.[7]

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to consider.[8] In response to the request for comment, staff received twenty-nine public comments[9] from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.[10]

The workshop consisted of four panels,[11] each of which focused on a different aspect of the IoT.[12] The first panel, "The Smart Home,"[13] looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, "Connected Health and Fitness,"[14] examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, "Connected Cars,"[15] discussed the different technologies involved with connected cars, including Event Data Recorders ("EDRs")[16] and other vehicle "telematics," a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, "Privacy and Security in a Connected World,"[17] discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.[18] In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.[19]

This report summarizes the workshop and provides staff's recommendations in this area. Section II of this report discusses how we define the "Internet of Things." Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, "participants"), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

WHAT IS THE "INTERNET OF THINGS"?

Although the term "Internet of Things" first appeared in the literature in 2005,[20] there is still no widely accepted definition.[21] One participant described the IoT as the connection of "physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing."[22] Another participant described it as including "embedded intelligence" in individual items that can detect changes in their physical state.[23] Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, "[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data."[24]

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification ("RFID") tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the "things" in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other "things."

For purposes of this report, we use the term IoT to refer to "things" such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC's mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

BENEFITS AND RISKS

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.[25] One area in which these benefits appear highly promising is health care.[26] For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."[27] Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing medical research and allowing the medical community to better treat, and ultimately eradicate, diseases."[28]

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that "one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care."[29] Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration ("FDA") considers medications that reduce blood sugar by as little as one half point to be successful.[30]

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, "even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,"[31] thus empowering consumers to "make better decisions about how they use electricity."[32] Home automation systems can provide consumers with a "single platform that can connect all of the devices within the home, [with] a single app for controlling them."[33] Connected ovens allow consumers to "set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s]."[34] Sensors known as "water bugs" can notify consumers if their basements have flooded,[35] and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.[36]

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.[37] Connected cars also can "offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car."[38] In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should go first according to a standard protocol.[39] They would also allow people with visual impairments to use their own cars as a mode of transportation.[40]

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.[41]

Security Risks

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. [42] Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.[43] Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.[44]

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer’s network to which it is connected, or enable attacks on other systems.[45] For example, a compromised IoT device could be used to launch a denial of service attack.[46] Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.[47] Another possibility is that a connected device could be used to send malicious emails.[48]

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.[49] Another participant discussed a set of experiments where an attacker could gain “access to the car’s internal computer network without ever physically touching the car.”[50]

He described how he was able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things."[51] Although the risks currently may be small, they could be amplified as fully automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.[52] Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.[53] Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.[54] In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.[55] And if an update is available, many consumers may never hear about it.[56] Relatedly, many companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.[57]

Privacy Risks

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,[58] which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can "generate 150 million discrete data points a day"[59] or approximately one data point every six seconds for each household.[60]

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.[61] According to a participant, "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[62] This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals."[63] Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."[64]

Others noted that companies might use this data to make credit, insurance, and employment decisions.[65] For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such as in one case, the number of "hard brakes," the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.[66] Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit – but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).[67] According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.[68]

Participants noted that the Fair Credit Reporting Act ("FCRA")[69] imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.[70] The FCRA imposes an array of obligations on entities that qualify as consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.[71] However, the FCRA excludes most "first parties" that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA's provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could "eavesdrop" remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.[72] Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were able to determine what television show an individual was watching.[73] Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.[74]

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.[75] As one participant stated, "promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services."[76]

APPLICATION OF TRADITIONAL PRIVACY PRINCIPLES

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles ("FIPPs") of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,[77] others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.[78]

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.[79] Subsequently, in 1980, the Organization for Economic Cooperation and Development ("OECD") adopted a set of privacy guidelines, which embodied the FIPPs.[80] Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union Directive on the protection of personal data[81] and the Health Insurance Portability and Accountability Act ("HIPAA")[82] are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.[83] The Obama Administration's Consumer Privacy Bill of Rights also includes these principles,[84] as does the privacy framework set forth in the Commission's 2012 Privacy Report.[85]

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, "Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things."[86] Accordingly, as another participant noted, "[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT."[87]

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.[88] With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would "chok[e] off potential benefits and innovation."[89] A second participant cautioned that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.[90] Still another participant noted that "[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive."[91]

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the information collection that they make possible. As one participant observed, when "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things," it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.[92] Another participant talked about the risk that, if patients have “to consent to everything” for a health monitoring app, “patients will throw the bloody thing away.”[93] Yet another participant noted that any requirement to obtain consent could be “a barrier to socially beneficial uses of information.”[94]

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.[95] For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.[96] Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).[97]

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.[98] Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could “automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database.”[99]

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in “[p]lain language and multiple choices of levels.”[100] Another discussed a “consumer profile management portal[]” approach that would include privacy settings menus that consumers can configure and revisit,[101] possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into “packets.”[102] Finally, one participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.[103]

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.[104] With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data. One commenter characterized this approach as “shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability."[105]

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies "tag" data with its appropriate uses so that automated processes could identify and flag inappropriate uses.[106] Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law[107] or through voluntary self-regulatory efforts[108] or seal programs.[109] For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.[110]

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"[111] as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that ... provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."[112] And last November, Intel announced a "new platform ... designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics."[113]

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report ("White House Big Data Report"), and the President's Council of Advisors on Science and Technology released a companion report ("PCAST Report"). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that "the notice and consent framework threatens to be overcome" in certain instances, "such as the collection of ambient data by our household appliances."[114] The White House Big Data Report concluded that,

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[115]

Attention to the impact of the IoT spans the globe. In September 2014, Europe's Article 29 Working Group – composed of data protection authorities of EU member countries – issued an Opinion on Recent Developments on the Internet of Things.[116] In the opinion, the Working Group emphasized the importance of user choice, noting that "users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.[117]

Commission Staff's Views and Recommendations for Best Practices

This section sets forth the Commission staff's views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

Data Security

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device’s functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement “security by design” by building security into their devices at the outset, rather than as an afterthought.[118] One participant stated that security should be designed into every IoT product, at every stage of development, including “early on in the design cycle of a technology.”[119] In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.[120] As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.[121] Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their products – may simply forget to close “backdoors” in their products through which intruders could access personal information or gain control of the device.[122]

This last point was illustrated by the Commission’s recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.[123]

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that “if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security.”[124] Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code “doesn’t mean...understand[ing] anything whatsoever about the security of an embedded device.”[125]

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission's recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission's complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors' notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers' own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.[126] They noted that companies must take "additional steps to encrypt [the information] or otherwise secure it."[127] FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers' home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.[128] Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.[129] In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.[130] In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.[131] Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe ‘expiration dates’ for their commodity Internet-connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission’s first case involving an Internet-connected device. TRENDnet[132] marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were “secure.” In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users’ mobile devices, and failed to test consumers’ privacy settings to ensure that video feeds marked as “private” would in fact be private.[133] As a result of these alleged failures, hackers were able to access live feeds from consumers’ security cameras and conduct “unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities.”[134] This case demonstrates the importance of practicing security-by-design.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.[135] Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

Data Minimization

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.[136] While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.[137] Accordingly, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[138]

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation (“APEC”) Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.[139] Some observers have debated how data minimization would apply to new technologies.[140] In the IoT ecosystem, data minimization is challenging, but it remains important.[141] Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm from such an event.[142] Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.[143]

Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers’ reasonable expectations. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.[144] In this case, the risk associated with continued storage and use of the subscribers’ personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[145] Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.[146] The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.[147]

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.[148] The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations[149] require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information[150] or have an expert determine that the risk of re-identification is "very small."[151] As one participant discussed,[152] in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.[153] While deidentification can be challenging in several contexts,[154] appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.[155] This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.[156] This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.[157] As one participant noted, "[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design."[158]

Notice and Choice

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.[159]

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.[160] This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
  One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[161]

- **Tutorials:**
  Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.
- **Codes on the device:**
  Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.[162]
- **Choices during set-up:**
  Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.
- **Management portals or dashboards:[163]**
  In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).[164] Similarly, companies developing "command centers" for their connected home devices[165] could incorporate similar privacy dashboards. Properly implemented, such "dashboard" approaches can allow consumers clear ways to determine what information they agree to share.
- **Icons:**
  Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.
- **"Out of Band" communications requested by consumers:**
  When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.
- **General Privacy Menus:**
  In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into "packets." [166] This could involve having

more general settings like "low privacy," "medium," or "high," accompanied by a clear and conspicuous explanation of the settings.

- **A User Experience Approach:**
  One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.[167] For example, a manufacturer that offers two or more devices could use the consumer's preferences on one device (*e.g.*, "do not transmit any of my information to third parties") to set a default preference on another. As another example, a single device, such as a home appliance "hub" that stores data locally – say on the consumer's home network – could learn a consumer's preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.[168] In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop[169] and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.[170] Companies can use such de-identified data without having to offer consumers choices.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to "consumer report" information, including restrictions on the uses for which this information can be shared.[171] Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.[172] In addition, the FTC has used its "unfairness" authority to challenge a number of harmful uses of consumer data. For example, in the agency's recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers' Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.[173]

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.[174] If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook's launch of the Beacon service, as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.[175]

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.[176] Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.[177]

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

LEGISLATION

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.[178] One participant stated, "[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America."[179] Another participant noted that "we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing."[180] Still another worried that the workshop might "represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy" and advised policymakers to "exercise restraint and avoid the impulse to regulate before serious harms are demonstrated."[181] Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.[182]

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, "self-regulation and best business practices – that are technology neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things."[183] Another participant agreed, stating "[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security."[184]

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.[185] One participant who called for legislation noted that the "explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging," but went on to state:

> At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential

> public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.[186]

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs[187] designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.[188] These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.[189]

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.[190] Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.[191] Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.[192] These recommendations have been based on concerns about the lack of transparency regarding some companies' data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.[193] A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.[194] A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of consumers want to control the data that is collected through smart devices.[195] Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.[196] General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.[197] Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the Children's Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission's first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.
- **Consumer and business education:**
  Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA's multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy's multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.
- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

CONCLUSION

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.

End Notes for Executive Summary

[1] Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

[2] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

[3] Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

End Notes

[1] Dave Evans, Cisco Internet Bus. Solutions Grp., The Internet of Things: How the Next Evolution Of The Internet Is Changing Everything 3 (2011), *available at* http://www.cisco.com/web. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *Id.*

[3] Telefonica, Connected Car Industry Report 2013 9 (2013), *available at* http://websrvc.net/2013 /telefonica/Telefonica%20Digital Connected Car2013 Full Report English.pdf.

[4] *See* Stanford Univ., *TSensors SummitTM for Trillion Sensor Roadmap* 1 (Oct. 23-25, 2013), *available at* http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

[5] *Id.*

[6] Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018 3 (2014), *available at* http://www.cisco.com/c/en/us /solutions/collateral/

[7] University of Bristol, Exabyte Informatics, *available at* http://www.bris.ac.uk/research/themes /exabyteinformatics.html.

[8] Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04 /ftc-seeks-input-privacy-and-securityimplications-internet-things.

[9] Pre-workshop comments ("#484 cmt.") are available at http://www.ftc.gov/policy

[10] For a description of the workshop, *see* http://www.ftc.gov/news-events/events-calendar /2013/11/internet-thingsprivacy-security

[11] In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation ("Marzullo"), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen ("Nguyen") of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton "Vint" Cerf ("Cerf") of Google Inc., who gave the workshop's Keynote Address (Transcript of Workshop at 118-153).

[12] A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files /documents/public_events/internet-things-privacy-security-c. Videos of the workshop also are available at http://www.ftc.gov/news-events/audiovideo/ftc-events.

[13] Transcript of Workshop at 52-115.

[14] *Id.* at 164-234.

[15] *Id.* at 235-291.

[16] An EDR is "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event." 49 C.F.R. § 563.5.

[17] Transcript of Workshop at 292-364.

[18] Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-

[19] Post-workshop comments ("#510 cmt.") are available at http://www.ftc.gov/policy/

[20] *See* Remarks of Marzullo, Transcript of Workshop at 19.

[21] *See Comment of ARM/AMD*, #510 cmt. #00018 at 1.

[22] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 1.

[23] Remarks of Marzullo, Transcript of Workshop at 19.

[24] *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

[25] *See Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 2.

[26] *See Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

[27] *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

[28] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 16.

[29] *See* Remarks of Stan Crosley, Indiana Univ. ("Crosley"), Transcript of Workshop at 199.

[30] *See* Remarks of Anand Iyer, WellDoc Communications, Inc. ("Iyer"), Transcript of Workshop at 188–189.

[31] *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

[32] Remarks of Eric Lightner, Department of Energy ("Lightner"), Transcript of Workshop at 54.

[33] Remarks of Jeff Hagins, SmartThings ("Hagins"), Transcript of Workshop at 64.

[34] Remarks of Michael Beyerle, GE Appliances ("Beyerle"), Transcript of Workshop at 60.

[35] *See* Remarks of Scott Peppet, Univ. of Colorado School of Law ("Peppet"), Transcript of Workshop at 167.

[36] *See* Remarks of Cerf, Transcript of Workshop at 132.

[37] *See* Remarks of Christopher Wolf, Future of Privacy Forum ("Wolf"), Transcript of Workshop at 247-48.

[38] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 13.

[39] *See* Remarks of Cerf, Transcript of Workshop at 127.

[40] *See id.* at 138.

[41] *See, e.g.*, Remarks of Craig Heffner, Tactical Network Solutions ("Heffner"), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation ("Tien"), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. ("Radcliffe"), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington ("Kohno"), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center ("Jacobs"), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. ("Rogers"), Transcript of Workshop at 344-45. *See also, e.g.*, HP, Internet of Things Research Study 5 (2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc= us&lc=en ("HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords

to cross-site scripting."); *id.* at 4 (noting that 80 percent of devices tested raised privacy concerns).

[42] *See, e.g.*, Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), *available at* http://money.cnn.com/2013/08/01/technology ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

[43] *See* Mario Ballano Barcena *et al.*, *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), *available at* www.symantec.com/content /en/us/enterprise/media/ (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled $24.7 billion, billions of dollars more than the losses for all other property crimes *combined*. Bureau Of Justice Statistics, U.S. Dep't Of Justice, Victims Of Identity Theft, 2012 (Dec. 2013)), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. *See* Javelin, 2013 Identity Fraud Report, *available at* https://www.javelinstrategy.com/brochure/276.

[44] *See, e.g.*, Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

[45] *See* Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . . There should never be a device on your network that you shouldn't care about the security of.").

[46] *See, e.g.*, Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World,* SYMANTEC (Jan. 21, 2014), *available at* www.symantec.com/connect/blogs (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

[47] *Id.*

[48] *See* Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), *available at* http://www.symantec.com/connect/blogs (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, "While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don't be surprised if, in the near future, your refrigerator actually does start sending spam.").

[49] *See* Remarks of Radcliffe, Transcript of Workshop at 182. *See also* Remarks of Tien, Transcript of Workshop at 82-83 ("And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.").

[50] Remarks of Kohno, Transcript of Workshop at 245.

[51] *See id.* at 245-47, 266.

[52] *See* discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. *See* Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), *available at* www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. *See also* Kashmir Hill, *'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, FORBES (Aug. 27, 2013), *available at* www.forbes.com/sites/kashmirhill/2013/08/27 /baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

[53] Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

[54] *See Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

[55] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), *available at* http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

[56] *Id. See also* Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

[57] *See, e.g., Bruce Schneier, The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), *available at* http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-ahuge-problem ("The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it's shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority.").

[58] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

[59] Remarks of Hagins, Transcript of Workshop at 89.

[60] *Cf. infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

[61] *See* Article 29 Working Group Opinion, *supra* note 55, at 8 ("Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.").

[62] Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) ("*Regulating the Internet of Things*"), *available at* http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

[63] *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

[64] Remarks of Tien, Transcript of Workshop at 67.

[65] *See* Remarks of Peppet, Transcript of Workshop at 169.

[66] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. *See also, e.g.*, Progressive, Snapshot Common Questions, *available at* http://www.progressive.com/auto

/snapshot-common-questions/; StateFarm, Drive Safe & Save with In-Drive, *available at* https://www.statefarm.com/insurance/auto/discounts/drive-safesave/indrive.

[67] *See* Remarks of Peppet, Transcript of Workshop at 167-169.

[68] *See id.* at 93, 123-24.

[69] 15 U.S.C. § 1681 *et seq.*

[70] *See, e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things, supra* note 62, at 126-127.

[71] *See* 15 U.S.C. §§1681e, 1681j.

[72] *See, e.g.*, Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, Bloomberg (May 12, 2014), *available at* http://origin-www.bloomberg.com /apps/news?pid =conewsstory&tkr=WPP:LN&sid=aPY7EUU9oD6g (reporting that the "world's biggest advertising agency" and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, "Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it."). *See also Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 ("to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.").

[73] *See* Dario Carluccio & Stephan Brinkhaus, Presentation: "Smart Hacking for Privacy," 28th Chaos Communication Congress, Berlin, December 2011, *available at* https://www. youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be. Moreover, "the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away." *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

[74] *See, e.g.*, Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that "enabled hackers to remotely turn on the TVs' built-in cameras without leaving any trace of it on the screen").

[75] *See, e.g., Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass'n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

[76] *Comment of GS1 US*, #484 cmt. #00030 at 4.

[77] *See, e.g.*, Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada ("Chibba"), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

[78] *See, e.g., Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

[79] *See* FTC, Privacy Online: A Report To Congress 48 n.27 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress

[80] *See* OECD, OECD Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data (1980), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is

available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf). *See also* FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 3-4, 43 n.25 (2000).

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice /policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[82] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[83] *See, e.g.*, Network Adver. Initiative, NAI Code Of Conduct 2013, *available at* http://www.networkadvertising.org/2013_Principles.pdf; Internet Adver. Bureau, Interactive Advertising Privacy Principles (Feb. 24, 2008), *available at* http://www.iab.net /guidelines

[84] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), *available at* http://www.whitehouse.gov /sites/default/files/privacy-final.pdf.

[85] FTC, Protecting Consumer Privacy in an ERA of Rapid Change: Recommendations for Businesses and Policymakers vii-viii (2012) ("Privacy Report"), *available at* http://www. ftc.gov/sites/default/files/documents/reports /federal-trade-. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

[86] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

[87] *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 ("There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they've done well. And they've gone on to push out products where there have been no issues.").

[88] *See, e.g.*, *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

[89] Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP ("Caprio"), Transcript of Workshop at 339.

[90] *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

[91] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 6–7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT "risks unduly limiting the development of new services and the discoveries that may follow from valuable research").

[92] Remarks of Peppet, Transcript of Workshop at 215–16.

[93] Remarks of Iyer, Transcript of Workshop at 230.

[94] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 8.

[95] *See, e.g.*, *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

[96] *See* FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency 10–11 (2013) ("Mobile Disclosures Report"), *available at* Http://Www.Ftc.Gov/Sites/Default

/Files/Documents/Reports/Mobile-Privacy-Disclosures-Building-Trust-Through-Transparency

[97] In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – *e.g.*, a sensor network to monitor electricity use in hotels. *See, e.g., Comment of GS1 US*, #484 cmt. #00030 at 5 (noting that "[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?"); *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

[98] Remarks of Chibba, Transcript of Workshop at 300-01.

[99] Comment of EPIC, #484 cmt. #00011 at 17-18.

[100] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[101] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[102] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

[103] Remarks of Nguyen, Transcript of Workshop at 48.

[104] *See* Remarks of Peppet, Transcript of Workshop at 210-211 (advocating "drawing some lines around acceptable use" through legislation or regulation in addition to notice and choice); *see also* Remarks of Crosley at 213 (supporting "the appropriate use of the context"); Remarks of Hall at 214 (expressing support for "[u]se restrictions, as long as they have teeth. That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body").

[105] Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

[106] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing Hal Abelson, *Information Accountability as the Foundation of 21st Century Privacy Protection* (2013), *available at* http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf). We note that such an approach would require coordination and potential associated costs.

[107] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

[108] *See, e.g., Comment of Consumer Elec. Ass'n,* #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n,* #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[109] *See, e.g.¸Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

[110] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

[111] Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), *available at* http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/.

[112] Microsoft Health, http://www.microsoft.com/Microsoft-Health/en-us (last visited Jan. 9, 2015).

[113] Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), *available at* http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-

[114] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values (May 2014) ("White House Big Data Report") at 56, *available at* http://www.whitehouse.gov /sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. *See also* President's Council of Advisors on Science and Technology, Report to the President: Big Data and Privacy: A Technological Perspective 38 (May 2014), *available at* http://www. whitehouse.gov/administration /eop/ostp/pcast.

[115] *White House Big Data Report* at 56.

[116] Article 29 Working Group Opinion, *supra* note 55.

[117] *See* oneM2M, *Technical Specification, oneM2M Security Solutions* at 15-16, *available at* http://www.onem2m.org/images Solutions-V-2014-08.pdf.

[118] *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

[119] Remarks of Kohno, Transcript of Workshop at 281.

[120] Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

[121] *See generally* Remarks of Rogers, Transcript of Workshop at 344 ("Default passwords are something that should never pass through into production space. It's an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren't often doing this kind of assessment − so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer's desk which, at the end of the day, the consumers aren't capable of setting that level of security, nor should they have to.").

[122] *See generally* Remarks of Heffner, Transcript of Workshop at 73-74.

[123] Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov /enforcement/cases-proceedings/132-3089 /fandango-llc. *See also* HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter

[124] Remarks of Hagins, Transcript of Workshop at 110.

[125] *Id.* at 92.

[126] *Id.* at 102.

[127] Remarks of Heffner, Transcript of Workshop at 102-03.

[128] Remarks of Hall, Transcript of Workshop at 178-79.

[129] *See, e.g.*, Brett C. Tjaden, Fundamentals of Secure Computer Systems 5 (2004). *See also* HP, Internet of Things Research Study, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

[130] There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

[131] oneM2M Candidate Release August 2014, *available at* http://www.onem2m.org/technical /candidate-releaseaugust-2014 (last visited Dec. 19, 2014).

[132] Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/pressreleases/2013/09/marketer-internet-connected-home-security

[133] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[134] *Id*. at 5.

[135] *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131 gmr statement.pdf: The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no onesize-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

[136] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

[137] *See, e.g.*, *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

[138] Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) ("Data Broker Report"), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-

[139] *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecdprivacy-guidelines (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov /xlibrary/assets (stating a Data Minimization principle: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites /default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).").

[140] *See* White House Big Data Report, *supra* note 114, at 54 (Because "the logic of collecting as much data as possible is strong ... focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); PCAST Report at x-xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

[141] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

[142] Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

[143] *See CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/ *DSW, Inc*., No. C-4157, 2006

WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order)*, available at* http://www.ftc.gov/enforcement/casesproceedings/042-3160/bjs-wholesale. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

[144] Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), *available at* http://www.ftc.gov/enforcement/

[145] *Comment of Transatl. Computing Continuum Policy Alliance,* #484 cmt. #00021 at 4.

[146] *Id. See also* Remarks of Chibba, Transcript of Workshop at 330.

[147] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

[148] *See* Flu Near You, *available at* https://fluneаryou.org/.

[149] 45 C.F.R. §§ 164.514(a)-(c).

[150] 45 C.F.R. § 165.514(b)(2).

[151] 45 C.F.R. § 165.514(b)(1).

[152] *Comment of Future of Privacy Forum,* #510 cmt. #00013, Appendix A at 8.

[153] *Id.*

[154] Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.,* Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), *available at* http://randomwalker.info/publications/no-silver

[155] *See, e.g.*, Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/06/pbd-deidentifcation_essential.pdf; *Comment of Ctr. for Democracy & Tech,* #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

[156] *See* Privacy Report, *supra* note 85, at 21; *see also Comment of Future of Privacy Forum,* #510 cmt. #00013, Appendix A at 7.

[157] *See, e.g., Comment of Future of Privacy Forum,* #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

[158] *Comment of Transatl. Computing Continuum Policy Alliance,* #484 cmt. #00021 at 3. *See also* Remarks of Chibba, Transcript of Workshop at 330.

[159] *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 ("In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices."); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 ("[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.").

[160] Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

[161] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[162] *See* Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a "device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections").

[163] *Comment of Future of Privacy Forum,* #484 cmt. #00013 at 6.

[164] *See* Mobile Disclosures Report, *supra* note 96, at 16-17.

[165] Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), *available at* http://www.wsj.com/articles/the-race

[166] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

[167] Remarks of Nguyen, Transcript of Workshop at 48.

[168] This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

[169] *See, e.g.*, *Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

[170] *See, e.g.*, Comment of CTIA – The Wireless Ass'n, #484 cmt. #00009 at 10-11; Comment of Future of Privacy Forum, #510 cmt. #00013 at 5.

[171] FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

[172] FCRA, 15 U.S.C. § 1681–1681v.

[173] Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/12/ftccharges-data-broker-facilitating-theft

[174] Ann Cavoukian Et Al., Info. & Privacy Comm'r, Ont., Can., The Unintended Consequences of Privacy Paternalism (2014), *available at* http://www.privacybydesign.ca/content/uploads /2014/03/pbdprivacy paternalism.pdf.

[175] *See, e.g.*, Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[176] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

[177] Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. *See, e.g.*, Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. *See, e.g.*, Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), *available at* http://www.ftc.gov/enforcement

[178] *See, e.g.*, *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010.

[179] *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

[180] Remarks of Rogers, Transcript of Workshop at 359.

[181] *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

[182] Remarks of Cerf, Transcript of Workshop at 149-50 ("Well, I have to tell you that regulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.").

[183] *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[184] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 18.

[185] Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement "in the meantime").

[186] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

[187] Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

[188] *See* discussion *supra* pp. 10-14 and accompanying notes.

[189] One commenter argued that breach notification laws should be even broader in the IoT context. *See* Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal information protected under existing laws). The Commission has not taken a position on such an approach at this time.

[190] Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), http://www.washingtonpost.com/blogs/

[191] Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

[192] *See, e.g.*, Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-

[193] Remarks of Chibba, Transcript of Workshop at 312-13; *see also* Remarks of Wolf, Transcript of Workshop at 260 (noting that "the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies"); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 ("If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.").

[194] Jan Lauren Boyles et al., Pew Internet Project, Privacy and Data Management on Mobile Devices (2012), *available at* http://www.pewinternet.org /files/old-media//Files/Reports /2012/PIPMobilePrivacy Management.pdf.

[195] The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, *available at* http://www.truste.com/usinternet-of-things-index-2014/.

[196] *See, e.g.*, Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), *available at* http://www. evidon.com/blog/researchconsumers-feel-better-about-brands-that-give-them-transparency Scott Meyer, *Data Transparency Builds Trust*, Brandrepublic (Oct. 31, 2012), *available at* http://www.brandrepublic.com /news/1157134/; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

[197] Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 2

INTERNET OF THINGS WORKSHOP REPORT: SEPARATE STATEMENT OF COMMISSIONER MAUREEN K. OHLHAUSEN[*]

I concur in the issuance of the staff report on the Internet of Things (IoT) workshop.

As the report acknowledges, we are in the early days of this rapidly developing technology. I have often advocated approaching complex technologies and rapidly changing business models with an attitude of regulatory humility.[1] This means we must work to understand the likely benefits and risks of IoT technology, focus on actual rather than speculative harms, and evaluate the ability of our existing tools to deal with such harms before calling for new laws or regulations. This report makes some progress consistent with these goals, and therefore I generally support it, with a few caveats.

The staff report does five things well:

- The report opposes IoT-specific legislation, stating that such legislation "would be premature" because the industry "is in its relatively early stages," and has "great potential for innovation."
- The report focuses on devices sold to or used by consumers, particularly devices that collect sensitive consumer information, such as real-time location or health information. Although consumers will

[*] This is an edited, reformatted and augmented version of a concurring statement to the Federal Trade Commission's Internet of Things report issued by Commissioner Ohlhausen, January 27, 2015.

likely benefit greatly from industrial and other business uses of IoT technology, such non-consumer facing technologies present very different data security and privacy issues than do consumer-oriented devices.

- The report prioritizes security of IoT technology and the personal data collected as a primary concern. Some IoT devices have already experienced data security failures that have harmed consumers.[2] The report thus reiterates the Commission's recent unanimous and bi-partisan call for data security legislation.[3]
- The report acknowledges the challenges that the IoT raises for the Fair Information Practice Principles (FIPPs), particularly the principles of notice and choice and data minimization. The report reasonably concludes that for many available consumer IoT applications, there are myriad ways to provide notice and choice for collecting consumers' personal information. It also notes the findings of the White House and PCAST Big Data reports that there are types of data collection and use that notice and choice simply cannot address.[4] By acknowledging FIPPs' potential limits the report takes an important step forward.
- The report acknowledges that limiting certain data uses is a promising approach to protecting consumer privacy in IoT applications. Indeed, the report acknowledges the use-based approach in the Fair Credit Reporting Act (FCRA) and notes that the use-based approach informs parts of the Commission's current privacy framework, including its unfairness authority to challenge harmful uses of consumer data. In short, the report's discussion of use-based approaches joins the ongoing dialog on how to supplement FIPPs to promote innovation and protect consumers more effectively.

However, I do not support two of the staff report's recommendations.[5]

First, I do not support the recommendation for baseline privacy legislation because I do not see the current need for such legislation. The FTC's Section 5 deception and unfairness authority already requires notice and opt-in consent for collecting consumers' sensitive, personally identifiable information. It also protects against uses of personal information that cause substantial, unavoidable consumer harm not outweighed by benefits to consumers or competition. Furthermore, sector-specific laws, such as FCRA, provide additional protections for consumers. Thus, I question what current harms baseline privacy legislation would reach that the FTC's existing authority cannot.

Second, I am concerned that the report's support for data minimization embodies what scholar Adam Thierer has called the "precautionary principle,"[6] and I cannot embrace such an approach. The report, without examining costs or benefits, encourages companies to delete valuable data – primarily to avoid hypothetical future harms. Even though the report recognizes the need for flexibility for companies weighing whether and what data to retain, the recommendation remains overly prescriptive.

One final, more general caveat: The report misses the opportunity to explore fully the emerging tension between information technology (including IoT) and the FIPPs approach to protecting consumer privacy. The White House and PCAST reports raised these issues (as noted above), as have others, including some workshop participants.[7] The staff report acknowledges the conflict, but fails to grapple with it in a substantial way. We will need to address these issues in the relatively near future, and I look forward to playing a role in that effort.

Overall, the report advances the Commission's efforts to understand the benefits and risks of IoT technology and government's proper role in maximizing these benefits and mitigating these risks. For these reasons, I concur in the issuance of this staff report on the Internet of Things Workshop.

End Notes

[1] See, e.g., Comments of Commissioner Maureen K. Ohlhausen, Federal Trade Commission, to NTIA on Big Data, Consumer Privacy, and the Consumer Bill of Rights at 12 (Aug. 5, 2014), available at http://www.ftc.gov/system/files/documents/public_ statements/573921/ 140806bigdata.pdf.

[2] By contrast, the privacy harms discussed in the report are thus far largely hypothetical.

[3] See Prepared Statement of the Federal Trade Commission, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches," Before the Senate Committee on Commerce, Science, And Transportation, 114th Cong., Mar. 26, 2014, available at http://www.ftc.gov/system/files/documents/public statements/293861/ 140326datasecurity. pdf.

[4] See Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values at 54 (May 2014) (because "the logic of collecting as much data as possible is strong ... focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); President's Council of Advisors on Science and Technology, Report To The President: Big Data and Privacy: A Technological Perspective at x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth.").

[5] I share Commissioner Wright's concerns with the report's lack of a rigorous cost-benefit analysis regarding its recommendations for privacy legislation and data minimization. However, given the report's limited scope, I find its reiteration of the Commission's previous unanimous data security legislative recommendation and its generally modest recommendations – other than the disputes noted here – to be appropriate.

[6] Adam Thierer, The Internet of Things and Wearable Technology at 31 (Nov. 2014), available at http://mercatus.org/sites/default/files/Thierer-Wearable-Tech.pdf.

[7] See Remarks of Peppet, Transcript of Fed. Trade Comm'n Workshop, Internet of Things at 210-211 (Nov. 19, 2013) (advocating "drawing some lines around acceptable use" in addition to notice and choice), available at http://www.ftc.gov/sites/default/files/ documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf; Scott R. Peppet, Regulating the Internet of Things, 93 Texas L. Rev. 85, 147, 149 (calling notice and choice "an ill-fitting solution" and proposing constraining "certain uses of Internet of Things data"); THIERER, supra n.6 at 48 ("[I]t is almost impossible to envision how a rigid application of traditional notice and choice procedures to IoT would work in practice.").

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 3

INTERNET OF THINGS WORKSHOP REPORT: DISSENTING STATEMENT OF COMMISSIONER JOSHUA D. WRIGHT[*]

I dissent from the Commission’s decision to authorize the publication of staff’s report on its Internet of Things workshop (“Workshop Report”) because the Workshop Report includes a lengthy discussion of industry best practices and recommendations for broad-based privacy legislation without analytical support to establish the likelihood that those practices and recommendations, if adopted, would improve consumer welfare.[1] This approach differs from the normal approach to a workshop report, which is to synthesize the record developed during the proceedings, and not to make broad policy recommendations. An economically sound and evidence-based approach to consumer protection, privacy, and regulation of the Internet of Things would require the Commission to possess and present evidence that its policy recommendations are more likely to foster competition and innovation than to stifle it.

The Commission has a long and well-regarded history of producing public reports that examine novel, emerging or otherwise important issues. These reports are integral to the Commission’s role in protecting consumers and competition in the marketplace. The genesis of such reports varies. Congress may ask the Commission to investigate certain subject matter and then to submit a report to them on the findings.[2] In preparing such Congressional

[*] This is an edited, reformatted and augmented version of a dissenting statement to the Federal Trade Commission's Internet of Things report issued by Commissioner Wright, January 27, 2015.

reports, the Commission sometimes will seek information using our authority under Section 6(b) of the Federal Trade Commission Act to compel private parties to submit information for review.[3] Commission staff reports often are the result of extensive research, rigorous investigation into certain industry sectors, practices or products, and economic analysis.[4] Reports taking advantage of the Commission's unique ability to collect and analyze data and to conduct economic analyses to form the basis of its recommendations predictably have had significant impact on public policy debates.[5] Another category of reports prepared by staff include those that document public workshops conducted by the Commission, as well as the public comment process that usually accompanies such workshops. While these documentary reports rarely reflect independent research or investigation, they can potentially serve a somewhat useful role in synthesizing the discussion at the workshop, the comments placed on the public record, and the Commission's enforcement actions and policy positions relating to the workshop topic.

The Workshop Report falls into neither of these categories and thus raises several concerns.

First, while documentary reports may serve a useful purpose in preserving a record of the workshop proceedings and the accompanying public comment process, one must recognize that merely holding a workshop – without more – should rarely be the sole or even the primary basis for setting forth specific best practices or legislative recommendations. If the purpose of the workshop is to examine dry cleaning methods[6] or to evaluate appliance labeling,[7] the limited purpose of the workshop and the ability to get all relevant viewpoints on the public record may indeed allow the Commission a relatively reasonable basis for making narrowly tailored recommendations for a well-defined question or issue. But the Commission must exercise far greater restraint when examining an issue as far ranging as the "Internet of Things" – a nascent concept about which the only apparent consensus is that predicting its technological evolution and ultimate impact upon consumers is difficult. A record that consists of a one-day workshop, its accompanying public comments, and the staff's impressions of those proceedings, however well-intended, is neither likely to result in a representative sample of viewpoints nor to generate information sufficient to support legislative or policy recommendations.

Second, the Commission and our staff must actually engage in a rigorous cost-benefit analysis prior to disseminating best practices or legislative recommendations, given the real world consequences for the consumers we are obligated to protect. Acknowledging in passing, as the Workshop Report does, that various courses of actions related to the Internet of Things may well have some potential costs and benefits does not come close to passing muster as cost-benefit analysis. The Workshop Report does not perform any actual *analysis* whatsoever to ensure that, or even to give a rough sense of the likelihood that the benefits of the staff's various proposals exceed their attendant costs.[8] Instead, the Workshop Report merely relies upon its own assertions[9] and various surveys that are not necessarily representative and, in any event, do not shed much light on actual consumer preferences as revealed by conduct in the marketplace. This is simply not good enough; there is too much at stake for consumers as the Digital Revolution begins to transform their homes, vehicles, and other aspects of daily life. Paying lip service to the obvious fact that the various best practices and proposals discussed in the Workshop Report might have both costs and benefits, without in fact performing such an analysis, does nothing to inform the recommendations made in the Workshop Report.

The abbreviated analysis underlying staff's data minimization recommendation illustrates the concerns I have with the Workshop Report's failure to analyze costs and benefits in general. In the Report, without limiting the scope of "data,"[10] staff identifies the benefits of data minimization in terms of eliminating two scenarios: (1) the possibility that larger data stores present a more attractive target for thieves; and (2) retention of large stores of data increase the risk that data will be used in a way that deviates from consumers' reasonable expectations. In considering the costs of data minimization, staff merely acknowledges it would potentially curtail innovative uses of data. Without providing any sense of the magnitude of the costs to consumers of foregoing this innovation or of the benefits to consumers of data minimization, and without providing any evidence demonstrating that the benefits of data minimization will outweigh its costs to consumers, staff nevertheless recommends that businesses "develop policies and practices that impose reasonable limits on the collection and retention of consumer data."[11]

Third, I remain unconvinced that the proposed framework described in the Workshop Report – a combination of Fair Information Practice Principles as well as other concepts such as "security by design" – is the proper framework to apply to the still-nascent Internet of Things. In contrast, I support the well-established Commission view that companies must maintain reasonable and appropriate security measures; that inquiry necessitates a cost-benefit analysis. The most significant drawback of the concepts of "security by design" and other privacy-related catchphrases is that they do not appear to contain any meaningful analytical content. Relying upon the application of these concepts and the Fair Information Practice Principles to the Internet of Things can instead substitute for the sort of rigorous economic analysis required to understand the tradeoffs facing firms and consumers. An economic and evidence-based approach sensitive to those tradeoffs is much more likely to result in consumer-welfare enhancing consumer protection regulation. To the extent concepts such as security by design or data minimization are endorsed at *any* cost – or without regard to whether the marginal cost of a particular decision exceeds its marginal benefits – then application of these principles will result in greater compliance costs without countervailing benefit. Such costs will be passed on to consumers in the form of higher prices or less useful products, as well as potentially deter competition and innovation among firms participating in the Internet of Things.

Before setting forth industry best practices and recommendations for broad-based privacy legislation relating to the Internet of Things – proposals that could have a profound impact upon consumers – the Commission and its staff should, at a minimum, undertake the necessary work not only to identify the potential costs and benefits of implementing such best practices and recommendations, but also to perform analysis sufficient to establish with reasonable confidence that such benefits are not outweighed by their costs at the margin of policy intervention. At this juncture, I believe the Workshop Report either should set forth that evidence or, in the alternative, request additional empirical evidence upon which to make future recommendations. In the absence of such evidence, the Commission should decline to publish the Workshop Report's recommendations.

End Notes

[1] Although an agency's recommendations regarding industry best practices do not carry the force of law, there is a very real danger that companies may reasonably perceive failure to achieve those practices or to adopt such recommendations as actionable. Where an agency's recommendations regarding best practices are not supported by cost-benefit analysis, firms may respond by adopting practices or engaging in expenditures that make consumers worse off.

[2] See, e.g., Fed. Trade Comm'n, Marketing Violent Entertainment to Children: A Review of Self-Regulation and Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries (2000).

[3] See, e.g., Fed. Trade Comm'n, Cigarette Report for 2011(2013); Fed. Trade Comm'n, Smokeless Tobacco Report for 2011 (2013); Fed. Trade Comm'n, Marketing Food to Children and Adolescents (2008); Fed. Trade Comm'n, Credit-Based Insurance Scores: Impact on Consumers of Automobile Insurance (2007); Press Release, Fed. Trade Comm'n, FTC Orders Nine Insurers to Submit Information for Study of the Effect of Credit-Based Insurance Scores on Consumers of Homeowners Insurance (Dec. 23, 2008), http://www.ftc.gov/newsevents/press-releases/2008/12/ftc-orders-nine-insurers-submit-information-study-effect-credit.

[4] See, e.g., Fed. Trade Comm'n, Bureau Of Econ., Improving Consumer Mortgage Disclosures: An Empirical Assessment of Current and Prototype Disclosure Forms (2007); Fed. Trade Comm'n, Broadband Connectivity Competition Policy (2007); Fed. Trade Comm'n, Emerging Health Care Issues: Follow-On Biologic Drug Competition (2009); Fed. Trade Comm'n, Possible Antitrust Competitive Barriers to E-Commerce: Wine (2003).

[5] See, e.g., Fed. Trade Comm'n, the Evolving Ip Marketplace: Aligning Patent Notice and Remedies with Competition (2011) (cited in Nautilus, Inc. v. Biosig Instruments, Inc., 134 S.Ct. 2120, 2129 (2014)); Fed. Trade Comm'n, Generic Drug Entry Prior to Patent Expiration (2002) (cited in Caraco Pharmaceutical Laboratories, Ltd. v. Novo Nordisk A/S, 132 S.Ct. 1670, 1678 (2012)); Fed. Trade Comm'n, to Promote Innovation: The Proper Balance of Competition and Patent Law and Policy (2003) (cited in Microsoft Corp. v. i4i Ltd. Partnership, 131 S.Ct. 2238, 2252 (2011)); Fed. Trade Comm'n, Possible Anticompetitive Barriers to E-Commerce: Wine (2003) (cited in Granholm v. Heald, 544 U.S. 460, 466 (2005)).

[6] Press Release, Fed. Trade Comm'n, FTC to Host Roundtable on Proposed Changes to its Care Labeling Rule for Clothing (Feb. 11, 2014), http://www.ftc.gov/news-events/press-releases/2014/02/ftc-host-roundtable-proposedchanges-its-care-labeling-rule.

[7] Press Release, Fed. Trade Comm'n, Commission Announces Workshop on Effectiveness of the Appliance Labeling Rule (Mar. 31, 2006), http://www.ftc.gov/news-events/press-releases /2006/03/commission-announcesworkshop-effectiveness-appliance-labeling.

[8] See generally, Fed. Trade Comm'n, The Internet of Things: Privacy and Security in a Connected World (hereinafter "Workshop Report") at 31-37 (2015) (recommending the adoption of data minimization without quantifying or analyzing the costs or benefits of this proposal); see also id. at 37-44 (recommending the adoption of the notice and choice model without providing any actual estimates of its costs or benefits).

[9] See, e.g., Workshop Report at 31-32 ("While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers. Accordingly, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.") (footnotes omitted); see also id. at 26 ("Of course, what constitutes reasonable security for a given device will depend upon a number of factors . . . . Nonetheless, the specific security best practices companies should consider include the following . . .").

[10] The Report identifies two types of data collection – the direct collection of sensitive information and the "collection of personal information, habits, locations, and physical conditions over time." Workshop Report at 13. The danger, as set forth in the Report, of this latter category of collection is that it "may allow an entity that has not directly collected sensitive data to infer it." Id. While the Commission is familiar with the risks associated with the collection and misuse of sensitive data, other than through hypothetical scenarios, the Workshop Report provides no information to quantify the actual extent or true risks attendant to this latter category of data collection. As I noted previously in my responses to the Data Broker Report, I am wary of extending FCRA-like coverage to other uses and categories of information without first performing a more robust balancing of the benefits and costs associated with imposing these requirements. Fed. Trade Comm'n, Data Brokers: a Call for Transparency and Accountability 52, n. 88 (2014).

[11] Workshop Report, Executive Summary at 4.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 4

CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS[*]

Federal Trade Commission

It's called the Internet of Things – the burgeoning phenomenon of day-to-day consumer products and services that connect to the Internet. Maybe it's a simple convenience like a home automation system that turns lights on and off remotely. Other innovations have the potential to save lives – for example, a connected car that contacts first responders instantly in case of an accident or a mobile app that allows a patient to share vital signs with a doctor. What distinguishes the Internet of Things is the product's ability to use the Internet to communicate with us, with others, or with other devices.

The Internet of Things has the potential to offer enormous benefits to consumers. Innovative companies are already selling connected devices, apps, sensors, services, etc., unlike anything we've seen before. But businesses need to consider security, too. As with any online activity, it's important to protect consumers' sensitive data from thieves. The Internet of Things, however, adds new security dimensions to consider. For example, an insecure connection could give a hacker access not just to the confidential information transmitted by the device, but to everything else on a user's network. And in the Internet of Things, the risk isn't just to data. If that home automation system isn't secure, a criminal could override the

[*] This is an edited, reformatted and augmented version of a document issued by the Federal Trade Commission, January 2015.

settings to unlock the doors. And just think of the consequences if a hacker were able to remotely recalibrate a medical device – say, an insulin pump or a heart monitor.

Businesses and law enforcers have a shared interest in ensuring that consumers' expectations about the security of these new products are met. Like any other industry in its infancy, the Internet of Things must prove itself worthy of consumer confidence. Is your company taking reasonable steps to protect consumers' devices from hackers, snoops, and thieves?

There's no one-size-fits-all checklist to guarantee the security of connected devices. What's reasonable will depend on a number of variables, including the kind and amount of information that's collected, the type of functionality involved, and the potential security risks. But based on input from industry, consumers, academics, and others, the FTC has a series of steps for your company to consider if you're designing and marketing products that will be connected to the Internet of Things.

START WITH THE FUNDAMENTALS

When it comes to security, the technology is ever-changing, but certain time-tested tenets have emerged.

- Encourage a *culture of security* at your company. Designate a senior executive who will be responsible for product security. Train your staff to recognize vulnerabilities and reward them when they speak up. If you work with service providers, clearly articulate in your contracts the high standards you demand from them.
- Implement *"security by design."* Rather than grafting security on as an afterthought, build it into your products or services at the outset of your planning process.
- Implement a *defense-in-depth approach* that incorporates security measures at several levels. Walk through how consumers will use your product or service in a day-to-day setting to identify potential risks and possible security soft spots.
- Take a *risk-based approach.* Unsure how to allocate your security resources? One effective method is to marshal them where the risk to sensitive information is the greatest. For example, if your device collects and transmits data, an important component of a risk-based

approach is an up-to-date inventory of the kinds of information in your possession. An evolving inventory serves triple duty: It offers a baseline as your staff and product line change over time. It can come in handy for regulatory compliance. And it can help you allocate your data security resources to where they're needed most. Free frameworks are available from groups like the Computer Security Resource Center of the National Institute of Standards and Technology, or you may want to seek expert guidance.

- Carefully *consider the risks* presented by the collection and retention of consumer information. If it's necessary for the functioning of your product or service, it's understandable that you'd collect data from consumers. But be sure to take reasonable steps to secure that information both when it's transmitted and when it's stored. However, it's unwise to collect or retain sensitive consumer data "just because." Think of it another way: If you don't collect data in the first place, you don't have to go to the effort of securing it.
- *Default passwords* quickly become widely known. Don't use them unless you require consumers to change the default during set-up.

TAKE ADVANTAGE OF WHAT EXPERTS HAVE ALREADY LEARNED ABOUT SECURITY

The product may be brand new, but you're not writing on a blank slate. There's a lot you can pick up from the 20 years of lessons learned by security experts. They've already identified solutions to some common concerns raised by the Internet of Things. Another excellent source of guidance is industry best practices. Here are a few back-to-basics suggestions that have become standard operating procedure for security-conscious companies.

- Standard *encryption techniques* are available for data your device transmits and for what it stores. Select stronger encryption methods over weaker ones (e.g., you can do better than WEP).
- Add *"salt"* – random data – to hashed data to make it harder for attackers to compromise.
- Consider using *rate limiting* – a system for controlling the traffic sent or received by a network – to reduce the risk of automated attacks. Some scammers try to break into networks by using software that

enters possible passwords over and over again until they hit pay dirt. Rate limiting can help thwart that kind of attack.

DESIGN YOUR PRODUCT WITH AUTHENTICATION IN MIND

Authentication – assuring that people are who they say they are – has always been important online. Proper authentication also is a must in the Internet of Things. If a device transmits or receives sensitive data, an authentication failure could allow unauthorized access to that information. But with connected devices, the risk doesn't stop there. An authentication failure could expose sensitive data not just on the device, but on networks to which it's connected. In addition, if an unauthorized person is able to access a device remotely and change how it operates, the safety implications could be profound. Consider investing additional resources in the design, implementation, and testing of authentication. If the risks are substantial, is it appropriate to put two-factor authentication in place – for example, requiring the use of a password and a secure token?

PROTECT THE INTERFACES BETWEEN YOUR PRODUCT AND OTHER DEVICES OR SERVICES

Just as burglars look for unlocked doors, hackers case networks for security soft spots. Even the strongest dead bolt offers no security if the windows are left open. Of course, you've considered all the ways consumers will access your products, but have you thought about whether those entry points might be misused by attackers? A security weakness at the point where a service communicates with your device could give scammers a foothold into your network. That's why each of those interfaces needs to be secured. One example is the interface between a mobile device and the cloud. Here are two particular web-based threats to guard against: cross-site scripting (XSS) attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery (CSRF) attacks, where unauthorized commands are sent from a user the website trusts. Fuzzing – a testing method that sends a device or system unexpected input data to detect possible defects – is a good approach. Consider using manual and automated tools to test interfaces. A simple online search will yield some helpful ones. Just be sure they're from groups you know to be trustworthy.

CONSIDER HOW TO LIMIT PERMISSIONS

When consumers use your product, chances are you'll need access to certain data to make it work as advertised. But given the risk if an interface is compromised, it's wise to be wary of accessing information you don't really need. Experts call it the principle of least privilege – crafting permissions to limit access to the level that will allow for normal functioning. Savvy businesses take time to think through the implications of those choices to strike the balance in a way that promotes utility and security.

TAKE ADVANTAGE OF READILY AVAILABLE SECURITY TOOLS

There's a tool out there for most basic security testing tasks – network scanning for open ports, reverse engineering of programming code or decompiling, checking password strength, and even scanning for known vulnerabilities. Many of these tools are free, and some of them work automatically. Of course, using them can't guarantee security, but they're important – and cost-effective – parts of a comprehensive program.

TEST THE SECURITY MEASURES BEFORE LAUNCHING YOUR PRODUCT

Of course, you're eager to get to market, but make sure your product is ready for prime time. And don't just evaluate the in-the-box item. Try it out in scenarios that replicate how consumers will use the product in the real world – for example, with optional features. Are your security precautions working in those foreseeable situations? Have you closed back doors through which hackers could access information or gain control of the device? If you've turned security measures off during testing, be sure to switch them back on before going live.

SELECT THE SECURE CHOICE AS YOUR DEFAULT SETTING

Choose safer options as your default settings. That offers out-of-the box protection for users new to the technology, but gives experts the alternative to make the selections that best suit their needs.

USE YOUR INITIAL COMMUNICATIONS WITH CUSTOMERS TO EDUCATE THEM ABOUT THE SAFEST USE OF YOUR PRODUCT

Developers aim for a plug-and-play experience for buyers. That's great, but take advantage of just-in-time opportunities to educate consumers about making sensible security choices. For example, the initial registration email you send to new customers offers a timely opportunity to showcase your security features and explain how customers can use them most effectively.

ESTABLISH AN EFFECTIVE APPROACH FOR UPDATING YOUR SECURITY PROCEDURES

If you're going to play in the Internet of Things arena, security can't be a one-and-done proposition. Your company may already conduct security evaluations every so often. That's an important step, but also re-evaluate your security practices as the environment changes – for example, when you deploy new technology, bring on additional service providers, or introduce new products. Other key considerations:

- How will you provide *updates for products* that are already out there? Will you offer them for free? Will updates happen automatically? It's wise to implement a belt-and-suspenders approach to reach as many of your users as possible. For example, if you need to get important security information to consumers, send a message to everyone who registered their product, contact people who signed up for news and updates, *and* put a prominent notice on your website. Some companies use on-the-product alerts – say, a small LED light – that cues users to visit the website for more information.

- Even if your company has moved on to the Next Big Thing, consider your obligations to customers who bought *earlier versions* of your product. How long will you offer security updates and patches?
- If the nature of the product makes updates unfeasible, consider how you'll respond if a significant *security flaw* is identified. How will you contact people to tell them about the problem? Product registration is one solution, but let's face it: Some consumers don't register products out of privacy considerations or concerns that information will be used for marketing. Forward-thinking companies prominently explain up front to consumers why it may be important to contact them in the future with critical security information.

KEEP YOUR EAR TO THE GROUND

Security is a dynamic process, and one advantage is the cross-talk that goes on among tech experts, researchers, and your customers. Some recent law enforcement actions have cited companies' failure to follow up when credible sources warned them about security vulnerabilities in their products. That's why it's wise to take advantage of the wealth of expertise that's already out there and listen to what people are saying about your products and the technologies you use. What else can you do?

- Stay on top of the latest threats by signing up for *email updates or rss feed*s from trusted security sources.
- Mark your calendar to check *free databases of vulnerabilities* identified by vendors and security researchers regularly – for example, the National Vulnerability Database. In particular, check for vulnerabilities in third-party components that are integrated into your products.
- Maintain *a channel where security researchers or consumers can reach you* about a risk they've discovered in one of your products. Rather than relying on a routine "contact us" link that sends an automated reply, consider a hotline approach like an easy-to-find email box on your website that you monitor regularly. Serious

inquiries related to the security of your products should generate serious responses.

- One method some companies have adopted: *bug bounty programs* that offer rewards – perhaps free products or cash – to people who identify significant security vulnerabilities in their products.

INNOVATE HOW YOU COMMUNICATE

You're ready to introduce a first-of-its-kind product. Don't hamper your chance for success by talking to consumers like it's 1999. Experienced marketers know that when you're explaining security or privacy options, dense blocks of fine print, complicated legal or technical jargon, and hard-to-find hyperlinks don't communicate information effectively. What's more, the next generation of products may not even have a screen. Now is the time for companies to put their creative talents to work to meet the communications challenges posed by the Internet of Things. Here are some methods to consider:

- Use a *set-up wizard* to walk consumers through the process of implementing security features.
- Build in a *dashboard* or profile management portal to make it easier for consumers to find the security settings for your device, configure them, and change them later.
- Let consumers set up *"out of band" communication channels*. For example, design your device so people can choose to get important information via email or texts.
- Use icons, lights, or other methods to *signal* when an update is available or when the device is connected to the Internet.

LET PROSPECTIVE CUSTOMERS KNOW WHAT YOU'RE DOING TO SECURE CONSUMER INFORMATION

Right now, many companies still think of security as primarily defensive – behind-the-scenes precautions to help prevent the what-ifs. But the Internet of Things offers entrepreneurs an opportunity to showcase the steps they're taking to keep information safe. The likely winners in the burgeoning Internet of Things marketplace are companies that out-innovate the competition both on the effectiveness *and* security of their products.

ONE FINAL NOTE

Of course, it's important to keep tabs on the latest developments in security, but developers also should consider how long-standing consumer protection principles apply to the Internet of Things. When making objective claims about your product, do you have appropriate proof to support what you say? Are your billing practices transparent? Are you honoring the promises you've made to consumers about their privacy? The FTC has free compliance resources at business.ftc.gov.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 5

TESTIMONY OF MIKE ABBOTT, GENERAL PARTNER, KLEINER PERKINS CAUFIELD & BYERS. HEARING ON "THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS"*

Chairman Thune, Ranking Member Nelson, and distinguished members of the Senate Commerce Committee, I appreciate the opportunity to testify before you today on the exciting and important topic of our connected world and the dynamic role of the Internet of Things ("IoT"). I would also like to thank Senators Fischer, Booker, Ayotte and Schatz for your interest in this topic and for requesting this hearing.

I am here today in my capacity as a general partner at the Silicon Valley-based venture capital firm, Kleiner Perkins Caufield & Byers. Our firm, Kleiner Perkins has more than 40 years of experience helping entrepreneurs deliver world-changing ideas to market. Through our Consumer Digital and Enterprise Digital initiatives alone, we have invested in and are mentoring more than 30 entrepreneurial companies with over $300 million in investments in the IoT space. I am by background an engineer, an entrepreneur, an investor, and a serial optimist about the power of technology and innovation to help improve our lives.

Today I will focus my testimony on 3 key areas:

* This is an edited, reformatted and augmented version of testimony presented February 11, 2015 before the Senate Committee on Commerce, Science, and Transportation.

1. The Internet of Things is a robust and vibrant ecosystem – in both the consumer and enterprise space – with new platforms and applications coming on-line every day and strong venture capital investments to help grow it.
2. The rapid growth in both data and devices leads to a next wave of innovation focused on efficiencies and smart systems using the cornerstones of successful IoT: smart hardware, software and cloud integration.
3. IoT – or “the Third Wave of the Internet” as analysts like to call it, is nascent but very competitive. Consumer confidence is paramount, but we must not over-regulate and stifle innovation.

As we look back on investments in the verticals we called “Bits, Bytes, Bugs, and Drugs,” we now see the rise of the Internet of Things: a connected world that allows us to jump from old platforms of the last decade into a new world in which we can manage every aspect of our lives, from our health to our finances to our home, all with the swipe of a finger on a smartphone. And the market is responding. Overall venture investments ($48 billion) in 2014 reached their highest levels since 2000[1] and the 2014 IPO market was strong, both domestically and globally. Overall IoT investment is harder to immediately qualify since it crosses over so many sectors. So what do we mean by the IoT?

It is my understanding that the primary focus of this hearing is the consumer side of the IoT. But it’s worth mentioning that there are many other applications for IoT including business-to-business and machine-to-machine – applications that will only expand. As such, I tend to categorize IoT in two ways:

- First is the consumer market, what I call “The Internet of Me,” because it enables people to use connectivity to enrich their lives and the lives of their family and friends.
- Second is “The Internet of IT,” consisting of large data generation for enterprises to make smarter systems for everything from precision agriculture to efficiencies in large-scale manufacturing.

IoT enables the collection of an unprecedented quantity and quality of data through sensors and devices. According to an often-cited Cisco report, there will be more than 50 billion connected devices by 2020[2] — approximately 2x growth every 5 years. And as the recent EMC Digital Universe and market research company IDC report noted, data is doubling in size every two years and expected to reach 44 zettabytes by 2020[3] – that's 44 trillion gigabytes. To put that in perspective, we were at 4.4 zettabytes, just over a tenth of that, in 2013.

So how will we deal with our data obesity problem? What are the smart solutions for managing all of this data in a way that improves, rather than complicates, our lives? With many platforms to spur technological advances from the home to the body to the car to the factory to the farm, we must innovate our way into a smarter, connected future. At Kleiner Perkins, we are looking across platforms and enterprises, at disrupters and at incumbents, and at the entire IoT ecosystem to use connectivity to transform how we work, play, and care for our families and ourselves.

We have two critical issues on this front. The first is power management of the devices themselves, and the second is data management, including machine learning. With a growing number of power hungry devices, our firm is looking at innovators working in the Low Power Everywhere space – devices getting lighter, smaller and more efficient. We're also looking at low power processors and energy scavengers that search for energy sources without batteries. There are promising advancements in this space such as the work being done by Ambiq Micro in sub-threshold circuits to improve efficiency in sensors and devices.

As investors, we do extensive analysis before investing in a company. But when you are at the disruptive edge of a new technological revolution, it's hard to fully predict how consumers will react. In order for a technological revolution to take root, you must invest early and work with the company to produce some wins.

A great example of this is our investment in Nest. When we started, we couldn't know for sure that Nest would be an attractive device to consumers. But now, with great technology and smart marketing, it's influencing the development of the smart home. This is because the Nest team got two of the most critical IoT elements right: intuitively designed and aesthetically pleasing hardware, and smart software. Together, these produce a seamless and enjoyable user experience, enabling the customer to easily, and remotely as needed, adjust the temperature in one's home and save on heating and cooling costs.

It's the possibility of more stories like Nest that led Kleiner Perkins to partner with Google Ventures to start the Thoughtful Things Fund. The Thoughtful Things Fund is an initiative to back the ideas and companies that can expand what the conscious homeTM can do. Consumers see immediate benefits from a connected home, whereas the cycle for enterprise systems may take a longer period of time. But the seeds of change for both consumers and enterprises are there, and we've already had thousands of submissions from all over the world.

If great hardware and software are the cornerstones of a robust IoT ecosystem, it is the third element – hardware + software + cloud services that will show major advances and create smarter systems. With all of these new devices, the stream of data will continue to accelerate. Successful systems must provide data-driven intelligence at both the endpoint devices and through machine learning in the cloud. In order for IoT to grow in meaningful ways to keep both consumer and enterprise users engaged, we must have a more intelligent way to manage and rank order data, with real-time usage feedback on what needs a fix or an upgrade. Recent advances in "deep learning" – the use of algorithms in machine learning for modeling abstractions in data – combined with these streams of real-time sensor data, will present enormous opportunities for innovation on which we are focused.

My testimony today is based primarily on my experience as an engineer and investor. I am not an expert in public policy. There is so much promise in this space, but we are in the early days. Consumer confidence is paramount to growth and innovation in the IoT space and reasonable security and best practices should help bolster that confidence.

The FTC has thoughtfully presented ideas, benefits and risks in its Internet of Things: Privacy & Security in a Connected World report. Congress, as evidenced by today's hearing, is also looking at the intersection of technology and public policy. However, I would ask that regulators and legislators proceed with caution when considering over-regulation in this space to prevent stifling innovation. As is common in nascent markets, interoperability in IoT is now a challenge and, over time, standards will emerge from the winners in the market. We are at a critical moment in this industry, in which innovators and entrepreneurs are competing with some of the biggest and most historically successful enterprises in the country – and that is healthy. This competition is creating consumer choice in the marketplace, delivering to consumers much better products and services at a lower cost.

An insightful colleague of mine once said that we'll know that we've succeeded when we no longer use the term the "Internet of Things" – just as we no longer say that we "download MP3s." As we've found with our music and phones, innovators are turning the scientific and technical breakthroughs of our time into products that benefit everyone, changing the way we live and giving us new opportunities to connect with and relate to one another and achieve our goals. Soon, my bet is that these technologies will likewise become unobtrusive, another chapter in how entrepreneurs and their innovations can help improve the quality of life for new generations, in this country and around the world.

I would like to thank the Committee for the opportunity to testify today. I look forward to answering any questions.

End Notes

[1] NVCA, "MoneyTreeTM Report by PricewaterhouseCoopers LLP (PwC) and the National Venture Capital Association (NVCA), based on data from Thomson Reuters," January 16th, 2015. http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highestlevel-decade-according-moneytree-report/

[2] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), April 2011. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] EMC Digital Universe & IDC, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," April 2014. http://www.emc.com/leadership/digital-universe/2014iview/executivesummary.htm

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 6

TESTIMONY OF JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY, CENTER FOR DEMOCRACY AND TECHNOLOGY. HEARING ON "THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS"*

The Center for Democracy & Technology (CDT) is pleased to submit testimony to the Senate Committee on Commerce, Science, and Transportation for today's hearing on the privacy and security implications of the Internet of Things (IoT).

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. I currently serve as the Director of CDT's Consumer Privacy Project. Our project focuses on issues surrounding consumer data, and I have previously testified before Congress on issues such as data breach notification legislation, commercial privacy, and cybersecurity.

The Internet of Things presents amazing opportunities for enriching citizens' lives. As consumer advocates, CDT is extremely enthusiastic about the potential advances to public health, the environment, education, and quality of life that will be brought about by the coming wave of IoT devices. However, in order to achieve this enormous potential for improving the lives of Americans, these sensor- and internet-enabled devices must be purposefully

* This is an edited, reformatted and augmented version of testimony presented February 11, 2015 before the Senate Committee on Commerce, Science, and Transportation.

designed with consumer privacy and empowerment in mind. My testimony today will address four key policy areas that must be addressed for the Internet of Things to be fully realized: weak data security practices, unexpected and unwanted secondary data collection and use, diminishing user control over their own devices, and the potential for law enforcement and intelligence abuse. Companies must respond to these challenges, or user adoption of these valuable and even life-saving technologies will be dramatically stunted.

I. THE TRANSFORMATIVE POTENTIAL OF THE INTERNET OF THINGS

We read about new *smart* technologies seemingly every day: keyless cars that you start with a cell phone, refrigerators that automatically order eggs when you've run out, dog collars equipped with GPS trackers, and even baby booties that monitor a child's heart rate and oxygen levels. This is a remarkable time for innovation and growth. According to recent reports, 26 to 30 *billion* devices will be connected to wireless internet by 2020. This means in just five years, the number of connected gadgets could grow to over 30 times its size in 2009.[1]

In addition to their *cool factor*, smart devices enhance healthcare, education, finance, agriculture, and a number of other fields. Connected cities are also starting to leverage these technologies regularly: Philadelphia has saved over $1 million by placing smart garbage cans around the city that alert sanitation workers when pick-up is necessary; New York City plans to convert outdated public pay phones into free open WiFi hotspots.[2]

In many ways, consumers have already embraced many smart Internet of Things devices. Over 70% of Americans now own a smartphone, giving each of us access to the wealth of the world's information at our fingertips as we go about everyday life.[3] Many of us have smart TVs or smart DVD players, meaning we have access not just to what's on TV or in our video library, but we can connect to Netflix, Amazon, or YouTube to watch virtually anything, or use Skype or Hangouts to call a loved one. In the near future, smart car technologies have the potential to dramatically reduce accidents, improve traffic flows, and reduce greenhouse gas emissions.

Without question, IoT has real revolutionary potential. However efforts to make all of our things smarter raise unique consumer protection concerns. Reports of major electronics companies planning to connect *all* of its consumer devices to the internet in the next five years[4] suggests the question: do consumers want *everything* to be smart? Is there a meaningful use case for a *smart toaster*? Even if there are incremental advantages to some connected devices, might the downsides in some cases outweigh the benefits? Unfortunately, some poor design decisions today are compromising the revolutionary potential of the Internet of Things, with the potential result that many if not most consumers will reject many of these innovations.

Smart technologies often involve the mass collection, storing and sharing individuals' data. While much of this is necessary and unobjectionable —the very nature of some devices (such as health wearables) is to track a user's data for that user's benefit — certain data practices seriously threaten individuals' security and right to privacy.

Internet of Things devices collect extremely sensitive personal information about us. This is especially true about IoT devices *in our homes*. In his majority opinion for *Florida v. Jardines,*[5] Justice Scalia articulated the high level of privacy an individual is entitled to in his or her home, writing "when it comes to the Fourth Amendment the home is first among equals... At the Fourth Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreason-able governmental intrusion'"[6]

The Supreme Court has repeatedly held that people have heightened privacy interests in what happens within their home — even over information[7] that is technologically observable[8] by others. We have "peeping tom" laws to protect against private observation in the home for the same reason — just because someone has the means to watch what you're doing in your home doesn't mean they should. Our homes are our most personal, private spaces and we maintain this expectation even if we bring smart devices into our home.

Internet of Things devices not tied to the home also have the potential to collect sensitive information. Certainly geolocation information — generated by several IoT devices — is extremely sensitive and revealing: unwanted disclosure can endanger one's personal safety by letting an attacker track your physical location. Otherwise, geolocation can reveal other deeply personal information, such as where you worship, where you protest, and where (and with whom) you sleep at night. Other IoT technologies often collect sensitive information on an individual that is not immediately apparent when that person is in a public space — such as his physical or mental health, emotions, and preferences.

In many cases, consumers will gladly share this information with IoT service providers in order to receive a particular service. However, in other cases, consumers won’t want this information collected at all. Internet of Things devices must be designed with this fact in mind, or consumers will reject these products as not worth the risks.

II. THERE ARE CURRENTLY INSUFFICIENT SECURITY PROTECTIONS IN PLACE TO REGULATE IOT DATA COLLECTION

It is no exaggeration to say that academics have documented the security vulnerabilities of the Internet of Things for years. Central to some of these concerns is that IoT devices use *embedded* operation systems, where computing is implanted into the device itself. The computer chips that power these systems are often cheaply produced, rarely updated or patched, and highly susceptible to hacks. Users do not have the expertise to regularly patch the system or install system updates manually, nor are they typically alerted of security updates. As prominent technologist Bruce Schneier succinctly puts it, “hundreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years. ... We have an incipient disaster in front of us. It's just a matter of when.”[9]

While some large, complex, smart IoT systems may have WiFi connections, software updates, and multiple types of functionality and interfaces, many of the more widely deployed IoT systems will be more modest, without such capabilities. These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal. Such incentives have failed certain elements of the smart phone market, resulting in millions of vulnerable devices that will remain so for the remainder of their shelf life.[10] Eventually, we expect to see entirely new types of market events, such as product recalls, based solely on vulnerabilities in the network and computational interface that provide IoT-like communication services. Otherwise, many of these devices and systems may never be updated in their after-market environment, and home networks and IoT-capable communication platforms will have to be designed to deal with errant and outright hostile (e.g., hacked through a flaw or vulnerability) participants on the local network. Compounding this problem is the fact that home routers — the devices that link all these devices together — are also famously vulnerable to attack.[11]

Even at this early stage of IoT development, seemingly every type of connected device has already experienced these vulnerabilities: spy chips have been discovered in tea kettles and irons[12]; hackers have stolen Smart TV login credentials in order to listen in and spy on people in their homes[13]; live streams from baby monitors have been uploaded to public websites[14]; thieves can disable home alarm systems with a tool from 250 yards away[15]; and even smart toilets, refrigerators and printers have been compromised.[16] And a report released this weekend by Senator Markey raises serious questions about whether connected cars are being designed to ensure that their systems are protected from malicious hackers seeking to take physical control over the vehicles.[17]

Currently, the United States does not have a dedicated data security law requiring companies to use reasonable protections to safeguard personal information. Since 2005, the Federal Trade Commission has used its general consumer protection authority under Section 5 of the FTC Act to bring enforcement actions against companies that do not safeguard personal data.[18] The Commission has argued that the FTC Act's prohibition on "unfair" business practices extends to companies using poor data security; two years ago, it brought its first enforcement action against the manufacturer of an Internet of Things device.[19] However, ongoing legal challenges threaten to undermine the agency's efforts in this area: some defendants have argued that they are not, in fact, legally obligated to use reasonable data security practices.[20]

Increased reports of massive data breaches (including the highly publicized Sony studios and Anthem healthcare hacks) have prompted new dialogue around the need for updated data breach notification laws to respond to such incidents. Unfortunately, many of the data breach notification legislative proposals would actually *dial back* legal incentives for companies to properly secure the data they collects from consumers. For example, only requiring agency or consumer notification when a specific "harm" has been identified would discourage companies from fully investigating a breach for fear of triggering the notification requirement. Further, data breach law that omits any affirmative requirement that companies design robust security procedures for their products will ultimately do little to expand upon existing state law protections and deter or prevent future breaches. In order to encourage better security than exists under the law today, a federal breach notification bill would need to offer *new* protections not reflected in existing law, and still allow states to innovate on data sets not covered by a federal standard.[21] For more information on this topic, visit https://cdt.org/insight/cdt-issue-brief-on-federal-data-breach-notificationlegislation/.

III. SENSITIVE PERSONAL DATA MAY BE COLLECTED CONTRARY TO CONSUMER WISHES AND EXPECTATIONS

As noted above, IoT devices have the potential to collect a tremendous amount of detailed personal information about consumers. Some of the data collected is of course expected; if I buy a fitness tracker, for example, I shouldn't be surprised that the device tracks my steps throughout the day — indeed, that's the reason I bought it. On the other hand, I might be surprised if that device were also recording all my conversations with my friends, or transmitting my geolocation to third party data brokers.

As an example of surprising — and potentially unwanted — IoT data collection, last year, an independent researcher noticed that LG was monitoring what TV shows people watched on their smart TVs, and sending that information back to LG's corporate servers.[22] The purpose appeared to be for a future undeveloped advertising product; LG was also collecting and reporting back information about the names of files consumers accessed on computers connected to the same home network, though it's not clear why. In response to user complaints, LG initially directed people to a long, legalistic terms of service that vaguely reserved broad rights to transmit user data. The company backtracked after a host of media attention around its practice, and LG enabled an opt-out feature for users who did not want their information collected in this manner. This was a start, however, it is not clear that opt-out is sufficient to meet reasonable consumer expectations in this case. Should home appliances be monitoring consumers and reporting everything they can detect back to manufacturers *by default*? Certainly, other interconnected devices don't do this today. Your computer doesn't report back to Lenovo or HP everything that you do. Your phone doesn't report everything back to Motorola or Apple. When a consumer buys a TV, they are not typically looking for or expecting *a relationship* with LG or Samsung: they may appreciate additional smart capabilities like connecting to Skype or the web, but their TV is a platform for them to access others' content — it is not a destination in itself. A users' smart phone could have its microphone and camera transmitting 24 hours a day, seven days a week (setting aside battery and bandwidth issues) — it could collect significant amounts of interesting information in the name of "Big Data" but such data collection would go well beyond consumers' reasonable privacy expectations.

This precise scenario arose last week in fact, when it was revealed that Samsung's privacy policy appeared to reserve the right to collect any voice communications in proximity to its Smart TVs and send that information to an unnamed voice recognition service provider.[23] Samsung's actual practices are not easily discernable: perhaps Samsung is only collecting and transferring voice data for the limited times when a consumer is trying to use certain voice recognition commands. This might be consistent with reasonable consumer desires and expectations. Or perhaps Samsung wants to collect and process *all* dialogue in proximity to its televisions in order to refine its (or its partner's) voice recognition software. There certainly would be a benefit — to Samsung and the consumer — from that collection and processing, but query whether most consumers would find the benefit worth the persistent collection of all conversations in a living room or bedroom by an unknown third party. Ultimately, consumers must be empowered to make the determination about what data is collected and why.

We believe that the United States should enact a comprehensive privacy law regarding the collection and use of personal information. Companies should be required to offer consumers reasonable transparency and control over how their data is collected; today, the U.S. is one of the few developed nations not to have such consumer protections in place. The purpose of such a law wouldn't be to ban or prevent particular practices, but should require actionable information and an ability to express real preferences in order for a market to develop for personal information. Today, absent such requirements, too much data collection is opaque and unaccountable; consumers have a vague sense that their privacy is being violated, but don't have the information or tools available to make decisions about their personal information.

With or without a law, companies should set reasonable defaults for data collection and use based on consumer expectations. Some data may require clear opt-in because it's sensitive or the collection or use would be surprising to a user; other information may be collected automatically but consumers should have the ability to opt out of secondary data use, retention, or transfer; and some data consumers shouldn't have control over because it is fundamentally necessary for operation of the device. However, consumers must generally be empowered to make decisions about how their devices work (and what data is collected and shared with other entities). IoT should work *for* the consumer — the person who bought the product; the Internet of Things shouldn't be something that happens *to* a begrudging populace.

IV. DEVICE CONNECTIVITY AND INTELLIGENCE COULD DIMINISH USER AUTONOMY OVER THE DEVICES THEY BUY

Adding sensors and connectivity to IoT devices has the potential to make them much more useful for consumers. On the other hand, these features could also be abused to deprive consumers of continuing services, expected interoperability, or control over their own devices.

Objects included in the "Internet of Things" consist of two basic components: the physical object and the software that connects it to the network. Traditionally, when you buy something, it is yours and you are free to do with it whatever you'd like including altering, repairing, or re-selling it. However, objects within the Internet of Things do not fit into our traditional understanding of ownership. While you still take possession of the physical object, the software is typically licensed to you under an End-User License Agreement (EULA). The implications of this vary with how integral the software is to the functioning of the device — in some cases, like a washing machine that you can monitor/control from your phone, losing access to this feature wouldn't affect the core functionality and value of the machine very much. In other cases, the object itself is essentially useless without the software controlled by licensing agreements, or can quickly become obsolete without updates. For example, imagine a thermostat that only works if you can program the software. In this case, a lapse in software updates could render the physical object useless even if the physical mechanism were still in good repair.

Last year, Keurig — the popular single cup coffee maker — put software controls on its coffee maker to prevent users from using non-Keurig approved coffee pods in their machines. Though this functionality did not rely upon internet connectivity, it did take advantage of increasingly cheap and sophisticated sensors to allow the Keurig machine to detect proprietary codes on approved coffee pods. As result of this technology, consumers were prevented from brewing their preferred brand of coffee in the devices they bought and paid for. In this case, Keurig's decision appears to have backfired: featured reviews for Keurig's new line of coffee makers on Amazon prominently criticize this design feature,[24] and sales fell 12 percent last quarter.[25]

In other cases, policymakers have intervened to mitigate potential monopolistic effects of proprietary software. One example is the repair codes used by automobile manufacturers. Cars include systems that provide a specific diagnostic code that explains, for example, the cause of a “check engine” light. Originally, the guide that explains these codes was withheld from consumers and the majority of auto repair shops, forcing drivers to use specific repair shops for their vehicles. However, some states now require that the explanations for the codes be widely available.[26] In another example, the Librarian of Congress, in consultation with the Copyright Office, eliminated an exemption to laws prohibiting circumvention of digital rights management for users seeking to *unlock* their mobile phones and change wireless providers. Mobile phone unlocking had been an entirely legal and common practice for years before the Librarian eliminated the exemption. More than 114,000 Americans petitioned the White House to overturn the ban and, after both the Federal Communications Commission and the White House recommended doing so, Congress ultimately enacted legislation restoring consumers’ right to unlock their own phones. Unfortunately, the exemption applies only to mobile phones and is examined *de novo* every three years.

In the Internet of Things, digital rights management affects intellectual property accessed through networked devices as much as the devices themselves. For example, users do not own the content they purchase for their e-readers (Kindle, Nook, etc.). The physical tool allows readers to buy rights to access the content of their choice, but readers do not own the book. Additionally, this access is restricted in many users may not fully understand because the relationship is so different from the physical world. For example, there are typically restrictions on *lending* the book to a friend. In this case, if the licensing agreements for that content were revoked because of a perceived or alleged violation of the license, the object itself would be useless to the average consumer who would have no way to load content.

Additionally, connectivity can allow other entities to access and control the device in ways not possible in an un-networked world. One prominent example is lenders who use technology in connected cars to punish those who are late in making payments by disabling the vehicle. In a case reported by the New York Times[27], subprime borrowers were allowed to lease vehicles provided they gave permission for the lender to remotely disable the ignition in the event of a late payment or default. Some argue this technology allows the lender to provide credit to a broader audience than would otherwise be possible; others argue that it is unethical and perilous to put people in a situation where they may have an emergency and cannot access their vehicle, as was the case for the woman in the article who needed to use her car to take an asthmatic child to the doctor. Moreover, vulnerable borrowers might be subject to egregious reconnection fees that had been disclosed only in inscrutable contracts. Regardless of what you believe, it is undeniable that this technology shifts the balance of power from the user to the company or institution that controls the software.

V. Our government Access and Intelligence Laws Must Be Reformed

Finally, the default of IoT devices to phone home by reporting data to a company rather than storing it locally on the device raise concerns about government surveillance as well. Many of the same concerns that apply to in-the-home monitoring devices like smart grid technologies[28] apply to objects in the Internet of Things. IoT systems will, in most cases, be sensing platforms augmenting devices and objects in the home or in businesses. Light sensors can tell how often certain rooms are occupied at night or how often the refrigerator is opened. Temperature sensors may be able to tell when one bathes, exercises, or leaves the home entirely. Microphones can easily pick up the content of conversations in the home and, with enough fidelity, can identify who is speaking. In essence, the privacy and security concerns highlighted by the revelation that law enforcement has access to data stored by private companies are elevated exponentially in a future with increased connectivity and automated collection.

Government access without robust due process protection is already arguably the most significant threat posed by the collection of personal information. As the recent NSA revelations aptly demonstrate, much of the data that governments collect about us derives not from direct observation, but from access to commercial stores of data. Even in the United States and Europe, that data is often obtained without transparent process, and without a particularized showing of suspicion — let alone probable cause as determined by an independent judge. Unfortunately, there is almost nothing that consumers can do to guard against such access or in many cases even know when it occurs.

The revelation that commercial data is tied to government surveillance has the potential to fundamentally change the conversation about IoT. For the vast majority of consumers, unwanted surveillance — quite apart from practical effects of such surveillance — is the harm they’re seeking to avoid. Therefore, considerations of risks associated with IoT must address harms from government surveillance as well as private sector risks.

This loss of consumer confidence has a quantifiable impact on corporate bottom lines and hence the development of these useful new technologies. For example, according to Forrester Research the losses to US technology companies from revelation of the PRISM program (detailing once facet of US surveillance practices) could result in, "a net loss for the service provider space of about $180 billion by 2016 which would be roughly a 25% decline in the overall IT services market by that final year." These costs demonstrate the market value of business practices and government policies that respect privacy.[29]

Nor is the point in sighting this figure to single out the NSA and US surveillance. As CDT has noted repeatedly, all governments are interested in data collection and have extensive legal tools to access that information. In an internet connected future it is not only the US government but also the governments around the world that may be interested in IoT and the information it reveals. For more on legal tools that governments possess to access personal information please see: http://govaccess.cdt.info/.

Government surveillance reform is a much broader topic than the IoT and this committee's hearing today. However, the continuing access by government to commercial information highlights the need to build systems that minimize the amount of information they share and also give consumers control over what information their devices collect.

The potential benefits of the IoT are exciting and profound. It is incumbent upon manufactures of these devices and governments to make sure that those benefits are fully realized while protecting the privacy of consumers.

CONCLUSION

Recognition of the threats to collected personal information is particularly important because in recent years, some have argued for a new definition of privacy where there are no limits on what information companies (and governments) can collect about us or how long they retain it. Privacy is in effect redefined to only prohibit certain harmful uses of personal information. For example, President Obama's Council of Advisors on Science and Technology last year released a report on Big Data making precisely this point: because of the potentially awesome power of personal information, we shouldn't put limitations on what information is collected; instead, we should just make sure that that data is not subsequently misused.[30]

This view, however, presumes a perfect world of unbreakable security, where consumer and company expectations are fully aligned, and where due process protections fully assure there is no potential for government abuse.[31] Obviously, these conditions are not met today, and likely will never fully be realized. As such, consumers have a rational interest in exercising control over how their data is collected and retained. Without affording consumers meaningful control over their own devices, IoT adoption is seriously threatened. Today, the highly sensitive data collected by IoT devices is exposed to a variety of threats, and designers must keep these threats in mind when developing their products for market. Consumers would benefit tremendously from a full-fledged, user-centric Internet of Things. Developers must keep personal privacy and empowerment in the front of their minds in creating these products.

End Notes

[1] Press Release, Gartner, Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 (Dec. 12, 2013), http://www.gartner.com/newsroom/id/2636073.

[2] Sarah Ashley O'Brien, The Tech Behind Smart Cities, CNN Money (Nov. 11, 2014), http://money.cnn.com/gallery/technology/2014/11/11/innovative-city-tech/index.html.

[3] Asymco: Smartphone penetration reaches 70% in the U.S., GSMARENA (Jul. 9, 2014), http://www.gsmarena.com/asymco_pricing_doesnt_affect_smartphone_adoption_in_the_us-news8982.php.

[4] Rachel Metz, CES 2015: The Internet of Just About Everything, MIT Technology Review (Jan. 6, 2015), http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-abouteverything/.

[5] Florida v. Jardines, 133 S. Ct. 1409 (2013).

[6] Id.

[7] Kyllo v. United States, 533 U.S. 27 (2001).

[8] Florida v. Jardines, 133 S. Ct. 1409 (2013).

[9] Bruce Schneier, Security Risks of Embedded Systems, Schneier On Security Blog (Jan. 9, 2014), https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.

[10] Dan Goodin, ACLU Asks Feds to Probe Wireless Carriers over Android Security Updates, Arstechnica, (April 17, 2013), http://arstechnica.com/security/2013/04/wireless-carriers-deceptiveand-unfair/.

[11] Dan Goodin, 12 million home and business routers vulnerable to critical hijacking hack, Arstechnica, (Dec. 18, 2014), http://arstechnica.com/security/2014/12/12-million-home-andbusiness-routers-vulnerable-to-critical-hijacking-hack/; Brian Krebs, Lizard Stresser Runs on Hacked Home Routers, Krebsonsecurity, (Jan. 15, 2015), http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[12] Erik Sherman, Hacked from China: Is Your Kettle Spying on You?, CBS (Nov. 1, 2013), http://www.cbsnews.com/news/hacked-from-china-is-your-kettle-spying-on-you/.

[13] Lorenzo Franceschi-Bicchierai, Your Smart TV Could be Hacked to Spy on You, Mashable (Aug. 2, 2013), http://mashable.com/2013/08/02/samsung-smart-tv-hack/.

[14] Loulla-Mae Eleftheriou-Smith, Baby Monitors, CCTV Cameras and Webcams from UK Homes and Businesses Hacked and Uploaded onto Russian Website, The Independent (Nov. 20, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitors-cctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto-russian-website-9871830.html.

[15] Kim Zetter, How Thieves can Hack and Disable Your Home Alarm System, Wired (Jul. 23, 2014), http://www.wired.com/2014/07/hacking-home-alarms/.

[16] Lily Hay Newman, Pretty Much Every Smart Home Device You Can Think of Has Been Hacked, Slate Blog (Dec. 20, 2014), http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_ being_secure.html.

[17] Report, Tracking and Hacking: Security & Privacy Gaps Put American Drivers at Risk, Office of Senator Ed Markey, (Feb. 2015) http://www.markey.senate.gov/imo/ media/doc/2015-02- 06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[18] Press Release, Federal Trade Commission, DSW Inc. Settles FTC Charges (Dec. 1, 2005), http://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges.

[19] Press Release, Federal Trade Commission, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-homesecurity-video-cameras-settles.

[20] See G.S. Hans, CDT Files Brief in Wyndham Supporting FTC Regulation of Data Security Center for Democracy & Technology Blog (Nov. 13, 2014), https://cdt.org/blog/cdt-files-brief-inwyndham-supporting-ftc-regulation-of-data-security/; See also Press Release, Federal Trade Commission, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), http://www.ftc.gov/news-events/press-releases/2013 /08/ftc-files-complaint-againstlabmd-failing-protect-consumers.

[21] CDT Issue Brief on Federal Data Breach Notification Legislation, Center for Democracy & Technology Insights, (Jan. 27 2015), https://cdt.org/insight/cdt-issue-brief-on-federal-data-breachnotification-legislation/.

[22] Justin Brookman, Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency, IAPP BLOG (Nov. 27, 2013), https://privacyassociation.org/news/a/eroding-trust-hownew-smart-tv-lacks-privacy-by-design-and-transparency/.

[23] Shane Harris, Your Samsung SmartTV is Spying on You, Basically, The Daily Beast (Feb. 5, 2015), http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-youbasically.html.

[24] Keurig 2.0 K350 Brewing System – Black, Amazon.Com, http://www.amazon. com/Keurig-2-0-K350-Brewing-System/dp/B00KYWL34Q/ref=sr_1_1?ie=UTF8&qid= 1423266957&sr=8- 1&keywords=keurig+2.0 (last visited Feb. 9, 2015).

[25] Josh Dzeiza, Keurig's attempt to 'DRM' its coffee cups totally backfired , THE VERGE (Feb. 5, 2015), http://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totallybackfired.

[26] Mass. lawmakers approve “Right to Repair” bill, Foxnews, (August 1, 2012), http://www.foxnews.com/leisure/2012/08/01/mass-lawmakers-approve-right-to-repair-bill/.

[27] Michael Corkery & Jessica Silver-Greenberg, Miss a Payment? Good Luck Moving That Car, The New York Times (Sept. 24, 2014), http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/.

[28] CTR. For Democracy & Tech. & Elec. Frontier Found., “Proposed Smart Grid Privacy Policies and Procedures,” before The Public Utilities Commission of the State of California (December 18, 2008), available at https://cdt.org/files/pdfs/CDT_EFF_Policies and Procedures_15Oct2010_OpeningComment_1.pdf.

[29] James Staten, “The Cost of Prism Will Be Larger Than ITIF Projects,” Forrester, August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14- the_cost_of_prism_ will_be_larger _than_itif_projects

[30] Executive Office of the President, Report to the President, Big Data and Privacy: A Technological Perspective (2014). http://www. whitehouse.gov/sites/default/files/microsites /ostp/PCAST/pcast_big_data_and_privacy__may_2014.pdf?utm_content=buffer06b57&ut m_medium=social&utm_source=twitter.com&utm_ca mpaign=buffer.

[31] Justin Brookman & G.S. Hans, Why Collection Matters: Surveillance as a De Facto Privacy Harm (2013), http://www.futureofprivacy.org/wp-content/uploads/BrookmanWhy-Collection-Matters.pdf.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 7

STATEMENT OF DOUGLAS DAVIS, VICE PRESIDENT AND GENERAL MANAGER, INTERNET OF THINGS GROUP, INTEL. HEARING ON "THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS"[*]

Intel Corporation ("Intel") respectfully submits this statement for the record in conjunction with the Senate Commerce, Science & Transportation Committee's hearing on "The Connected World: Examining the Internet of Things." Our statement focuses on the opportunity to unleash the vast potential of the Internet of Things (IoT) through public-private partnerships and to create a leadership opportunity for the U.S. in this multi-industry transformation.

Witness: Doug Davis is the vice president and general manager of Intel's worldwide IoT Group (IOTG). Doug has been an Intel employee for 31 years, and began his career as a product engineer in the company's Military and Special Products Division. Over the last decade, Doug has run Intel's worldwide Embedded and Communications Group, managed wafer factory operations, and now leads the IoT Group. This organization is responsible for the company's IoT strategy and solutions – consisting of hardware, software, security and services across a wide range of market segments, including transportation, manufacturing, healthcare, retail, smart home, smart buildings

[*] This is an edited, reformatted and augmented version of a statement presented February 11, 2015 before the Senate Committee on Commerce, Science, and Transportation.

and smart cities. For the past 30 years, Intel has made significant investments, driven exciting innovations, led standards activities, and supported what has evolved to become the Internet of Things. At Intel, we like to say IoT is an overnight transformation thirty years in the making.

INTEL AND THE INTERNET OF THINGS

Intel's Role

The evolution of IoT goes back more than 30 years with Intel as a leader from the start. In 1972, Intel introduced the Intel 4004, the world's first commercially available microprocessor – an invention foundational to the "computer revolution." In the late 1970s, came the Intel 8048, the world's first commercially available microcontroller, which integrated memory, peripherals and the microcontroller on a single chip. These microcontrollers fueled new business opportunities in a variety of markets. In 1981, IBM launched the IBM 5150, igniting the rapid-paced growth of the "personal" computer (PC) market segment. This first IBM PC ran on an Intel 8088 microprocessor and used Microsoft's MS-DOS operating system.

Initially, microprocessors were used for personal computing, leaving microcontrollers for 'use specific or 'embedded' applications like factory controls. A critical shift occurred in the mid-1990s as customers began using Intel microprocessors in embedded market segments, bringing the power of computing to what had traditionally been based on microcontrollers. Intel began a concerted effort to support the unique attributes of embedded market segments including manufacturing life-cycle support for 7-10 years, extended operating temperatures, and utilization of real-time operating systems.

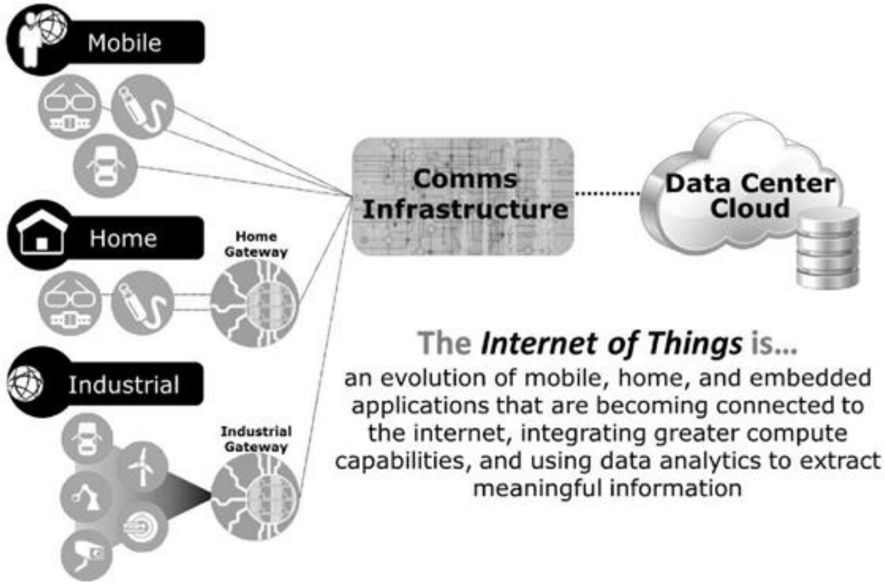
The early 2000s saw an unprecedented uptake in internet usage, as the PC and mobile markets exploded. This "connectivity" trend wasn't limited to connecting people; embedded systems were simultaneously taking advantage of this powerful capability. Over the course of just a few years, industries worldwide were profiting from the scaling benefits of computing and networking and consumers were enjoying the benefits of connected PCs.

In the late 2000s, "Machine to Machine" (M2M) emerged. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. Before M2M, people had to be physically located at the machine to analyze the data to make decisions for managing each machine. With the introduction of M2M, machines could now be managed remotely. All of these innovations within the datacenter, cloud computing, wireless communications and M2M formed the basis of what is now widely known as the IoT.

Moore's Law, the business model that drives the semiconductor industry, states that the number of transistors in an integrated circuit doubles approximately every two years. In essence, the marketplace experiences a doubling of the computing capability at approximately the same price every other year. The observation is named after Intel co-founder Gordon E. Moore. This explosion of networked devices also began to represent another “law” of scaling called Metcalfe’s Law. Metcalfe’s Law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). This enables the Network Effect, whereby the value of a product or service is dependent on the number of others using it. Together, Moore’s Law and Metcalfe’s Law demonstrate how the power of intelligent, connected devices like connected digital signs, cars and homes can unleash innovation, leading to the creation of platforms for new applications and services.

IoT Definition

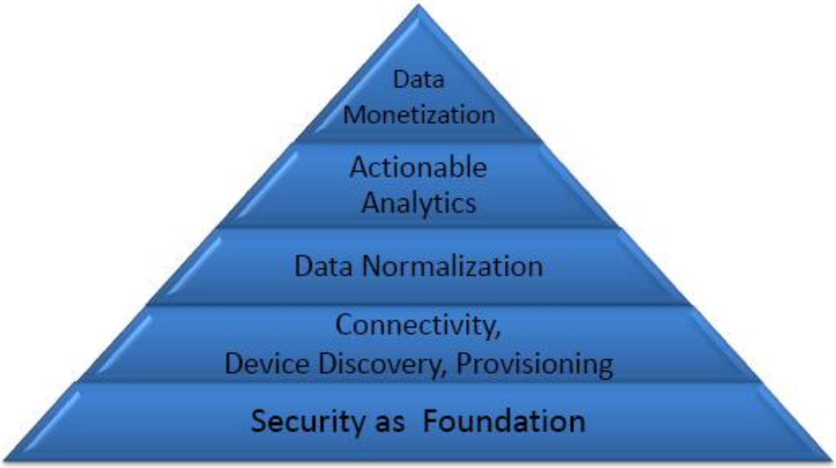
IoT is defined as endpoint devices such as cars, machinery or household appliances that connect to the internet and generate data that can be analyzed to extract valuable information. There are three sub-definitions emerging out of the IoT space, however, all three definitions overlap. The “Mobile IoT” comprises devices like cars, wearables, sensors and mobile phones which all connect directly through broadband wireless networks. The “Industrial IoT” connects devices in industrial environments like factory equipment, security cameras, medical devices, and digital signs. These devices are able to connect to the internet and into the datacenter (cloud) through an industrial “gateway.”[1] Finally, the “Home IoT” connects devices like game consoles, smart TVs, home security systems, household appliances and thermostats through at gateway to the internet.


Mobile
Home
Home Gateway
Industrial
Industrial Gateway
Comms Infrastructure
Data Center Cloud
The *Internet of Things* is...
an evolution of mobile, home, and embedded applications that are becoming connected to the internet, integrating greater compute capabilities, and using data analytics to extract meaningful information

THE FIVE CRITICAL TENETS OF IOT

In September 2014, Intel and key global partners collaboratively identified five critical IoT tenets which describe how endpoint devices should connect to the cloud. Here are the five key tenets, as illustrated in the graphic below:

First, *Security as the Foundation*: With billions of internet-connected devices by 2020, it is important that IoT is secure from the sensor to the cloud, including all hardware and software. Second, *Connectivity, Device Discovery, and Provisioning*: Billions of devices cannot be managed manually. Rather, devices need to be able to communicate their "status" to the rest of the system independently. Third, *Data Normalization*: With so many different data types, there must be some level of interoperability between devices such that they are speaking the same language. Fourth, *Actionable Analytics*: The data must be turned into meaningful information through analytics. Fifth, *Monetize Hardware, Software, and Data Management*: The IoT infrastructure must be built to allow developers to manage and monetize innovative applications and services.



With these tenets in mind, in December of 2014, Intel launched the Intel® IoT Platform,[2] which unifies security and connectivity to enable scalable IoT deployments. The Platform provides a secure device-to-cloud (end-to-end) open reference model for connecting devices to deliver trusted data to the cloud and value through analytics. The Platform enables tenets 1-3 – security, connectivity, and interoperability – by creating a foundation on which to build IoT solutions. This enables tenets 4 and 5 – data analytics and monetization of new products and services, many of which we never could have imagined a decade ago and may not even conceive of today.

IoT: A Transformational Opportunity Built on a Foundation of Security

With respect to the critical element of security, Intel values this first and foremost. We believe that security is the foundation of IOT and it is fundamental to Intel’s roadmap planning. We have dedicated security products and security features embedded into both our hardware and software products. Our hardware and software are being designed from the beginning to be secure. This is important for trusted data exchange in the IoT, as data generated by devices and existing infrastructure must be able to be shared among the cloud, the network, and intelligent devices for analysis. This enables users to aggregate, filter and share data from the edge of the network all the way to the cloud with robust protection. Moreover, data must be accurate to be beneficial. Intel prioritizes the security, accuracy, privacy and integrity of data in all market sectors, and especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. Intel understands that we must deliver and evoke consumer and industry trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

Intel believes it is critical to integrate security into the hardware *and* the software, from the smallest microcontroller (MCU) at the edge of the network to the most advanced server CPU in the data center (cloud) and all gateways and devices in between. These hardware- and software- level security capabilities will create redundancies which prevent intrusions and enable a robust, secure, trusted IoT end-to-end solution.

Hardware. Intel's hardware will provide transistor-level security *on the actual compute device itself*. By integrating security into the device itself from the outset (rather than layering it on top at a latter point in the design cycle with other, less secure external features), Intel's IoT solutions will enable our customers to know the exact unique identity of every device on their network. This technology also has the capability for encrypting that unique identity to provide anonymity properties in addition to hardware enforced integrity. Because each compute device can have an immutable identification to enable secure provisioning, a non-approved device will not be allowed to access the network. The MCU or CPU itself will provide the "baked in" (irremovable, non-changeable) identity of the device, making the level of security significantly more robust.

On top of this immutable device identification, Intel's IoT solutions will employ advanced hardware level security capabilities such as "whitelisting," which prevents harmful applications like viruses, control agents, and malware from ever being activated on the device. What this means is that, if the CPU ever "sees" an application that is not on its known good list ("whitelist") try to run on the device, it will automatically lock out that device and not allow it turn on. At other layers in IoT solutions, Intel also uses another advanced hardware security capability called "blacklisting," which blocks a defined list of known malware from entering the device and the network.

Software. In addition to the advanced hardware security capabilities in Intel's IoT solutions, Intel Security (formerly McAfee) integrates advanced security capabilities that provide robust software-level protection. This means that the software is continually monitoring the activity of its networked devices and looking for any abnormalities or possible threats. If the monitoring software identifies a threat, it proactively notifies users and/or automatically quarantines any devices on the network that could be at risk.

By employing this combination of transistor-level security, along with advanced hardware and software level security, from devices on the edge of the network all the way to the data centers in the cloud, Intel will protect IoT assets and information in ways few others can. Intel knows that security is critical to protect the integrity of IoT solutions, so we will design it in from the outset.

IoT Priorities – Enablers of Scale

Security

As discussed above, security is foundational to the IoT ecosystem and a top Intel priority. With billions of connected devices producing enormous amounts of data –EMC/IDC forecasts that devices will generate more than 44 zeta bytes of data by 2020[3] – security of this data will be critical to enable scale of IoT deployments. That is why we emphasize again the importance of having security designed into the IoT systems from the outset. Secure data delivery systems are critical to enabling trusted data exchange and scale, thereby unlocking the full potential of IoT.

Interoperability

The IoT marketplace is currently aligning around industry sectors/verticals that are starting to deploy IoT solutions to meet their specific business requirements: manufacturing, retail, transportation, healthcare, and others. As early adopters deploy technologies to enable IoT solutions, it is important that the various IoT technologies are "interoperable" with each other as well as being able to adapt and grow to accommodate new and changing business requirements. Proprietary technologies that are inherently antithetical to the concept of the internet of *All* Things will slow down IoT adoption, limit scalability and delay economic benefits.

The Intel IoT Platform's building block components are secure, interoperable, and scalable, enabling "horizontal" end-to-end IoT deployments across industry sectors from transportation to energy to healthcare and beyond. By creating a secure, horizontal, interoperable platform, Intel will enable IoT to scale quickly by creating a repeatable (reusable) foundation that ultimately enables choice and interoperability in the marketplace. For example, Intel offers businesses that use the Intel IoT Platform the choice and flexibility to use some or all of the technology components from Intel, or interchange them with ecosystem partner components. In summary, if the U.S. wants to lead in IoT, we must prioritize interoperability from the start.

Open Standards

How do we drive a secure solution that is interoperable and scales across a global IoT ecosystem? The solution is a voluntary, global, industry-led, open set of standards which enable scale to drive cost-effective solutions. Over the last 10 months, Intel co-founded two industry consortia focused on interoperability and open standards: The Industrial Interconnect Consortium (IIC)[4] and the Open Internet Consortium (OIC).[5]

IIC founding members include major U.S. companies such as AT&T, Cisco, GE, IBM and Intel. The IIC has reached over 135 members since its inception in March 2014. IIC goals are to: (i) build confidence around new and innovative approaches to security; (ii) drive innovation through the creation of new industry use cases and test beds for real-world applications; (iii) define and develop the reference architecture and frameworks necessary for interoperability; (iv) influence the global development standards process for internet and industrial systems; and (v) facilitate open forums to share and exchange real-world ideas, practices, lessons and insights.

The OIC was founded by leading technology companies with the goal of defining the connectivity requirements for devices, and for ensuring interoperability between the millions of devices that will make up the emerging IoT. OIC founding members include Cisco, GE, Intel, MediaTek and Samsung, and membership has reached over 54 members. OIC goals are to: (i) define the specification, certification and branding to deliver reliable interoperability; (ii) ensure this standard will be an open specification that anyone can implement and is easy for developers to use; (iii) include IP protection and branding for certified devices and service-level interoperability; (iv) provide an open source implementation of the standard; and (v) ensure this open source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

Both IIC and OIC recognize that a certain level of standardization and interoperability is necessary to achieve a successful IoT ecosystem. In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Furthermore, open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path. Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, and Intel is taking a leading role.

MARKET TRENDS DRIVING THE EMERGENCE OF IOT

If we've had broad use of the internet for over two decades why is the IOT industry emerging now? Intel believes there are three emerging trends are driving the inflection:

Ease of connectivity – Whether it is an unlicensed (WiFi, Bluetooth) or licensed (3G, LTE, 5G) spectrum, connectivity is becoming more pervasive and inexpensive. The opportunity to add value via increased connectivity is extremely large, as 85 percent of devices are not connected today.

Compute economics – Moore's Law is impacting technologies that range from the cloud to the network to storage to sensors. This means that the economics for "compute" have become much more appealing. Specifically, there has been a huge drop in cost for "compute" technologies over the last 10 years; the cost of sensors has decreased 2X, the cost of bandwidth has decreased 40X, and the cost of processing has decreased 60X.

Big Data and Analytics – The emergence of data science (extracting knowledge from data) combined with the reduction in the cost of high performance computing has created an opportunity to turn data into actionable information, thereby enabling new services and new business model innovation.

These three market trends are generating unprecedented opportunities for the U.S. public and private sectors to develop new services, enhance productivity and efficiency, improve real-time decision making, solve critical societal problems, and develop new and innovative user experiences. All of these opportunities are revolutionizing sectors like smart buildings, transportation, healthcare, and manufacturing. Here are just a few examples of quantitative results already enabled by IoT:

Smart Buildings: The integration of Intel IoT technology with sensors and building automation systems, such as heating and air conditioning, allows for the identification of opportunities in real-time to reduce energy costs. In conjunction with Intel and Cisco, Rudin Management, a large, commercial real estate company in New York City, deployed Intel's Smart Building IoT solution, which saved Rudin $1 million in just one building in the first year of deployment. Consider the U.S. potential opportunity: There are over 5 million commercial buildings and industrial facilities in the U.S.,[6] with a combined annual energy cost of more than $202 billion.[7]

It is estimated that the U.S. could save $20 billion if all commercial buildings and industrial buildings increased their energy efficiency by just 10%.[8]

Smart Transportation: The integration of Intel IoT technology with New York-based Vnomics fleet management solutions enabled real-time monitoring and feedback to Georgia-based SAIA Trucking drivers and headquarters. The goal was to reduce maintenance costs and improve driver safety by monitoring braking in real-time. In the first year, SAIA increased fuel efficiency by 6 percent across a fleet of 3,000 trucks, achieving a savings of $15 million. Consider the U.S. potential opportunity: The U.S. trucking industry accounts for about 13 percent of all fuel purchases in the U.S. and trucks consume about 54 billion gallons/year for business purpose.[9] Extrapolating SAIA's success, a 6 percent improvement in fuel efficiency across all trucks in the U.S. would save more than 3 billion gallons of fuel each year, as well as help reduce CO_2 emissions.

Smart Healthcare: Intel has partnered with the Michael J. Fox Foundation to research the use of big data analytics to help improve the treatment of Parkinson's disease. Our IoT personal healthcare solution enables 300 observations per second per patient, thereby monitoring patients' symptoms and drug effectiveness in real-time. This real-time data collection and analysis allows for the identification of the first signs of disease progression and enables physicians to instantly address changes. Patients can receive better, personalized care, and physicians can make improved decisions for treatment in the event that the patient does not notice slight changes that could cause a decline in health before their next regularly-scheduled appointment. Consider the U.S. potential opportunity: Imagine what real-time monitoring of Parkinson's patients' vitals, as well as the ability to make drug and treatment adjustments in real-time, in addition to better tracking and predictability of disease progression could do to improve the quality of life of Parkinson's patients not only in the U.S., but the world.

Smart Cities: Intel has partnered with the city of San José, California in a public-private partnership to further the city's 'Green Vision' goals. This Smart Cities Project, announced as part of the Smart America Challenge in 2014,[10] is expected to help drive San José's economic growth, foster 25,000 clean-tech jobs, create environmental sustainability and enhance the quality of life for residents. Together, Intel and San José City Management are deploying a network of sensors to create a "sustainability lens" that uses Intel IoT technology to measure characteristics such as particulates in the air, noise pollution and traffic flow. This real-time city data will produce meaningful insights that enable the City to make better management decisions, and lead to improvements in air quality, transportation efficiency, environmental sustainability, health, and energy efficiency. Consider the U.S. potential opportunity: The ten largest U.S. cities alone have an aggregated population of 25,292,500 people.[11] What if we initially focused on 10 cities, 10 counties, and 10 rural towns from across the nation and implemented IoT "smart city" solutions into those communities?

IoT: Extraordinary Positive Impact on U.S. GDP

The IoT presents staggering economic opportunities for the U.S. and the world. Market research firm IDC estimates that there will be 50 billion connected devices in the marketplace by 2020,[12] and Morgan Stanley forecasts 75 billion in that same time period.[13] These estimates would equate to 6 to 10 connected devices for every person on earth. Whether the exact number of devices is 50 billion or 75 billion or something more, one thing is for certain: The number of connected devices will explode in the next five years. In just the automotive industry alone, it is projected that 250 million (or one in five) cars worldwide will be connected to the internet by 2020 – via technologies like WiFi, LTE, Bluetooth, satellite, and 5G communications networks.[14] For perspective, 250 million is roughly the same number of total cars on U.S. roads in 2013.[15]

The reason that policymakers should be excited about this explosion of devices and this technological revolution is the staggering positive impact that the IoT is projected to have on the U.S. and global economy. McKinsey projects that IoT will have an incredible $2.7 trillion to $6.2 trillion global economic impact by 2025.[16] And what should most excite U.S. policymakers is that the U.S. and other developed economies are expected to capture a remarkable 70 percent of this economic impact, if we develop a leadership position.[17] In fact, GE estimates that IoT could boost average incomes in the U.S. by an exceptional 25 to 40 percent over the next twenty years.[18]

Moreover, a recent Accenture survey of CEOs reveals that 87 percent of CEOs expect long-term job growth from IoT.[19] This will positively impact American lives from our nation's farms and factories to markets and Main Street. Indeed, "as the world struggles to emerge from a phase of weak productivity growth, fragile employment and pockets of inadequate demand, the [IoT] offers a chance to redefine many sectors and accelerate economic and employment growth."[20] The U.S. must lead in this technological revolution.

RECOMMENDATIONS FOR POLICYMAKERS

Given the predicted enormous positive impact on the U.S. economy and society, how can policymakers help accelerate IoT and ensure the U.S. leads this next evolution of computing?

- *Continue an open dialogue with industry, experts and stakeholders as you are doing today*. This IoT hearing is a promising start and the right first step. Intel believes that an open, multi-stakeholder process can best enable a secure and vibrant IoT ecosystem. Also, legislators may want to consider encouraging the Department of Commerce to create a nonpartisan National IoT Advisory Board of policymakers, agency representatives, industry leaders, think tanks, academia, and leaders of IoT-focused consortia like IIC and OIC.
- *Encourage focus on security and interoperability as critical foundational elements of IoT.* While industry is in the best position to develop and determine security and interoperability solutions, government can encourage industry alignment around large-scale IoT deployments based on secure, open and interoperable IoT solutions. This will enable deployments to scale quickly and provide both short-term and long-term economic and social benefits to consumers, government, and businesses.
- *Encourage open standards and open architectures* to maintain the long term viability of IoT, based on an approach that is scalable, interoperable and reusable across a variety of use case deployments, vendors and sectors. While 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 the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. 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.

- *Collaborate with the industry to develop a U.S. National IoT Strategy* with time-bound goals for sector-specific IoT deployments over the next 3 to 5 years. These deployments will not only address critical societal issues and save tax payer dollars, but also will demonstrate U.S. leadership. A National IoT Strategy will help align IoT stakeholders and incentivize innovation, ultimately creating value for society by increasing efficiencies and productivity, creating jobs, sustaining our environment, and improving quality of life in our cities and towns.
- *As part of our National IoT Strategy, encourage Public-Private Partnerships (PPPs)* to address societal problems and accelerate more rapid deployment of IoT solutions. Government and industry collaboration can be one of our nation's best assets to accelerate the adoption of a world-class IoT ecosystem. Viable PPPs will make IoT deployments an appealing investment for both government and industry, while ensuring scalability and sustainability of infrastructure and technological innovation over the long term. Notably, countries like China,[21] the UAE,[22] Malaysia,[23] Germany[24], Brazil[25] and others are moving aggressively ahead on IoT deployments – establishing national IoT plans and blueprints establishing time-bound measurable goals, investing substantial funding in IoT research and deployments, and launching PPPs to jumpstart these opportunities and quickly enable IoT scale. As these other countries have recognized, a vibrant and state-of-the-art IoT ecosystem is critical to a nation's global competitiveness and economic stability in the 21st century. By adopting and implementing a National IoT Strategy, the U.S. can seize the leadership position in this next evolution of computing.

PUBLIC-PRIVATE PARTNERSHIPS – MARKET SEGMENT FOCUS

Specifically, over the next 3 to 5 years, the U.S. should focus on industry vertical segments with the potential to have the most impact: transportation, cities (generally communities, urban and rural), and buildings. Here are proposed PPPs for these market segments:

Smart Transportation PPP: The transportation segment is predicted to be valued at more than $351 billion by 2025, with a CAGR of 19.6 percent (2012-25).[26] In FY 2012, the Federal Agency fleet consisted of more than 650,000 vehicles, which collectively drove over 5 billion miles, consumed nearly 400 million gallons of fuel, and had operating costs of approximately $4 billion.[27] The U.S. Postal Service fleet alone is over 190,000 vehicles.[28] Intel recommends encouraging an IoT Smart Transportation PPP around the USPS fleet or another considerably sized government fleet to implement IoT solutions and benchmark increases in fuel economy, logistics and driver efficiency, and improvements in customer service. Focus areas could include, but are not limited to, fleet and freight management, passenger optimization, automatic train protection and control systems and advanced driver assistance and safety.

Impact – Logistics and Transportation was a $1.3 trillion industry in the U.S. in 2012, and represented 8.5 percent of GDP. With almost 9 percent of the U.S. labor force employed in the transportation sector and the U.S. spending roughly $160 billion annually on highway infrastructure (about 1/4 funded by the federal government), a more efficient and effective trucking industry has the potential to yield significant savings to the U.S. economy. For example, the commercial trucking industry in the U.S. uses about 50 billion gallons of fuel each year. A 7 percent increase in fuel efficiency results in more than 3.5 billion gallons of fuel saved. Imagine if we set a national goal for 25 percent of the Federal Fleet in 3 years, and 50 percent in 5 years, be retrofitted with IoT transportation solutions, not just for telematics but to increase fuel economy by a minimum of 5 percent, with incentives for higher efficiency.

Approach – Consistent with existing national goals to improve the fuel efficiency of American trucks – thereby bolstering energy security, cutting carbon pollution, saving money, and spurring manufacturing innovation29 – this proposed PPP would leverage private sector and academia IoT expertise in “Intelligent Transportation” solutions. The PPP would accelerate efforts by

Congress, DOT, DOC, DOE, EPA, and U.S. commercial fleet managers to increase engine efficiency and fuel economy of large fleets traveling our nation's roads and highways. It would realize direct economic savings including increased fuel efficiency, reduction in carbon dioxide emissions, labor savings, improved driver safety, accident savings, productivity and distribution proficiency, and logistics tracking effectiveness. The PPP also would provide insights into improvements and new business models for the U.S. transportation sector at large, leading to more satisfied employees and customers. Notably, this PPP would be an early step toward the ultimate goal of an autonomous trucking industry; the estimated savings to the U.S. freight transportation industry from autonomous vehicles is $168 billion per year, with savings from labor ($70 billion), fuel efficiency ($35 billion), productivity ($27 billion), and accident savings ($36 billion).[30] Funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One possibility could be for public and private partners to share in the transportation fuel savings. For example, if the PPP were to reduce a department', or commercial end user operator's fleet, fuel expenses by 7 percent, the department (operator) could allot 2 percent of that savings to the (other) private partners over a specified period of time until the (other) private partners recoup their upfront investment plus some incremental percent of return. The department operator would retain the remaining percentage of the savings, after which time, the department and U.S. taxpayers (operator) would retain 100 percent of the fuel savings benefit in perpetuity.

Smart Cities PPP: Today's cities consume two-thirds of the world's energy.[31] By 2025, 37 cities worldwide will each have a population of greater than 10 million.[32] To address the escalating demands of existing and future residents, cities are looking for ways to introduce more technology to become "smarter" about the use of limited resources and more flexible in responding to residents' needs. Examples of "Smart Cities" capabilities could include but are not limited to: City Sensing including monitoring and providing IoT data to improve air quality, noise pollution, ambient light, weather, and traffic flow; smart parking which is using IoT to "smartly" guide citizens to open parking spaces; smart roads that enable "smart" traffic navigation and roadside service; smart emergency response which facilitates "smart" public and residential community alert and response for vulnerable areas; and smart energy/grid that facilitates "smart" renewable energy and distributed power.

Impact – IoT technologies could realize direct economic savings for cities and municipalities (and their local tax base) due to more efficient city planning and management. Results would include improvement in city residents' quality of life, health, and safety. Some examples of this benefit could include more efficient traffic flow, real-time public notifications of pollution "hot spots," and early detection and correction of chemical and gas leaks in aging city infrastructure.

Approach – Consistent with the goals of NIST's Smart America and Global Cities Team Challenges33 – to use IoT solutions to improve services, promote economic growth, and enhance quality of life – this proposed PPP would leverage private sector IoT expertise in deploying "Smart Community" solutions. These IoT solutions would accelerate local government and municipality efforts to improve urban management and planning in a variety of ways. For example, the PPP could provide a model to improve operational efficiencies and safety across existing and new city infrastructure by utilizing air quality and traffic flow data to enable sustainable traffic management and planning, and create an innovative tool for urban growth management and planning. The funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One opportunity may include public and private partners to share in new revenue streams by leveraging the IoT sensor network infrastructure to deliver new services to city residents. For example, if the PPP were to deliver new services to city residents (i) via the city sensor network or (ii) by sharing the real-time data generated by the city sensor network, the city could share the new revenue stream with the private partners. The city (and its taxpayers) would enjoy the benefits of improved traffic flow, air quality, and safety, and avoiding the hefty cost to rebuild city infrastructure.

Smart Buildings PPP: The smart building segment is predicted to be valued at almost $249 billion by 2025, with a CAGR of 4.1 percent (2012-25).34 The U.S. government owns or manages more than 900,000 buildings or other structures across the country making it the nation's largest landlord. Smart building examples could include, but are not limited to, Smart Government Buildings enabling "smart energy" (HVAC) management, water flow and usage, predictive maintenance/mechanical operations and building security, and smart military bases facilitating the integration of systems and logistics for "smart" traffic flow, people flow, air quality, retail commerce operations, personnel safety and parking.

Impact – The proposed PPP would help the U.S. save on energy expenses while reducing carbon pollution. The U.S. government – and thus U.S. taxpayers – would realize direct (and possibly significant) economic savings due to improved efficiency in consumption, distribution, and management of energy and utilities across federal government buildings and installations. The PPP also would provide insight into savings opportunities and consumption planning for other federal properties, as well as state and local government properties. In addition, the PPP would introduce new business models that could increase efficiencies and offer new revenue streams for building owners in the public and commercial sectors, while improving services for building tenants and residents.

Approach – Consistent with the goals of the Better Buildings Challenge, to realize building energy savings of 20 percent or more over 10 years[35] and other current initiatives, this proposed PPP would leverage private sector IoT expertise in "Smart Building" IoT solutions to accelerate the U.S. government efforts to improve operational efficiencies across federal buildings and/or military installations. Imagine if we set a national goal for 25 percent of Federal Government buildings to be retrofitted with IoT solutions in three years, and 50 percent to be retrofitted with IoT solutions in five years, to increase energy efficiency by a minimum of 20 percent. Upfront funding for the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. Benefits from the PPP also would be shared among public and private sector partners over the short- and long-term, ensuring PPP viability and creating a win-win scenario. One possibility in this case could be for public and private partners to share in the federal building/installation's energy and utility savings. For example, if the PPP were to reduce a department's energy and utility expenses by 20 percent, the U.S. government could allocate 10 percent of that savings to the private partners over a specified period of time until the private partners recoup their upfront investment plus some incremental percent of return, and the U.S. government (U.S. taxpayers) would retain the remaining 10 percent of the savings. After which time, the U.S. government would retain 100 percent of the energy and utility savings benefit.

CONCLUSION

Intel appreciates the opportunity to share our perspective on the enormous opportunity of the IoT and a proposed strategy for U.S. leadership in the next evolution of computing.

End Notes

[1] A gateway is a node on a network that serves as an entrance to another network.

[2] Intel Unifies and Simplifies Connectivity, Security for IoT, Intel Corp. (Dec. 2014), http://newsroom.intel.com/community/intel_newsroom/blog/2014/12/09/intel-unifies-and-simplifies-connectivitysecurity-for-IoT.

[3] The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, EMC/IDC (April 2014), http://www.emc.com/leadership/digital-universe/ 2014 iview/executive-summary.htm .

[4] http://www.industrialinternetconsortium.org/

[5] http://openinterconnect.org/

[6] Commercial Buildings Energy Consumption Survey (CBECS), US Energy Information Administration (5.6 million commercial buildings in U.S. in 2012), http://www.eia.gov/ consumption/commercial/reports/2012/preliminary/index.cfm?src=%E2%80%B9%20Cons umpt ion%20%20%20Commercial%20Buildings%20Energy%20Consumption%20Survey%20(C BECS)-b1.

[7] http://thesemco.com/about-us/why-energy-efficiency/

[8] Id.

[9] http://www.truckinfo.net/trucking/stats.htm

[10] Intel Helps San Jose Become America's First Smart City: http://www.psfk.com/2014/06/san-jose-intel-smartcity.html

[11] United States Census Bureau: U.S. and World Population Clock http://www.census. gov/ popclock/

[12] Business Strategy: The Coming of Age of the "Internet of Things" in Government, IDC (April 2013), http://www.idc.com/getdoc.jsp?containerId=GIGM01V.

[13] Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, Business Insider (Oct.2 2013) http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013- 10.

[14] Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities, Gartner Inc. (Jan. 26, 2015), http://www. gartner.com/newsroom/id/2970017.

[15] Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive, IHS (June 2014) (253M cars on US roads in 2013), http://press.ihs.com/press-release/automotive/average-age-vehicles-roadremains-steady-114-years-according-ihs-automotive.

[16] Disruptive Technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute (May 2013), http://www.mckinsey.com/insights/business_ technology/disruptive_technologies.

[17] Id.

[18] New “Industrial Internet” Report From GE Finds That Combination of Networks and Machines Could Add $10 to $15 Trillion to Global GDP, GE (Nov. 2012), http://www.gereports.com/post/76430585563/newindustrial-internet-report-from-ge-finds-that.

[19] CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to drive future business strategies, Accenture, at 7 (2015), http://www.accenture.com/Site Collection Documents/PDF/Accenture-IndustrialInternet-of-Things-CEO-Briefing-Report-2015.PDF.

[20] Winning the Industrial Internet of Things, Accenture, at 2 (Jan. 2015), http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDF.

[21] China’s Ministry of Industry and Information Technology is implementing a three-year (2013-15) action plan to establish a National innovation demonstration area of sensor networks in Wuxi, actively promoting pioneer projects of applications such as intelligent manufacturing, agriculture, transportation, medical systems, and environmental protection: http://www.usito.org/news/miit-emphasize-iot-rd-sensors-and-chips-2014.

[22] The Telecommunications Regulatory Authority, in collaboration with the Prime Minister's Office, is working to announce The National Plan for UAE Smart Government Goals: http://www.tra.gov.ae/news_The_TRA_to_announce_The_National_Plan_for_UAE_Smart_Government_Goals636-1.php.

[23] Eyeing a role in global IoT, Malaysia opens CREST centre in Penang (Feb. 2, 2015), http://www.mis-asia.com/tech/applications/eyeing-a-role-in-global-iot-malaysia-opens-crest-centre-in-penang/#sthash.enmSihPu.dpuf.

[24] “As part of its High-Tech Strategy ("Ideas. Innovation. Prosperity.") to consolidate German innovation leadership, Germany is making significant R&D investment in the Internet of Things and new services for the diverse application areas within this new connected world.” http://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Smarter-business/smart-products-industrie-4.0.html

[25] Smart-city to be deployed by Telefonica/VIVO, ISPM in Brazil http://www.smartgridtoday.com/public/Smartcityto-be-deployed-by-TelefonicaVIVO-ISPM-in-Brazil.cfm

[26] Strategic Opportunity Analysis of the Global Smart City Market: Smart City Market to be Worth a Cumulative $3.3 Trillion by 2025, Frost & Sullivan (Sept. 2013) (“Frost & Sullivan”), http://www.frost.com/prod/servlet/reportbrochure.pag?id=M920-01-00-00-00.

[27] Federal Motor Vehicle Fleet Report FY 2012, http://www.gsa.gov/portal/mediaId/ 181179/fileName/FY 2012 Federal Fleet Report.action.

[28] Delivery Vehicle Fleet Replacement (June 10 2014) Office of the Inspector General United States Postal Service [https://www.uspsoig.gov/sites/default/files/document-library-files/2014/dr-ma-14-005.pdf]

[29] Improving the Fuel Efficiency of American Trucks – Bolstering Energy Security, Cutting Carbon Pollution, Saving Money and Supporting Manufacturing Innovation, White House (Feb 18, 2014), http://www.whitehouse.gov/the-press-office/2014/02/18/fact-sheet-opportunity-all-improving-fuel-efficiencyamerican-trucks-bol.

[30] Autonomous Cars: Self-Driving the New Auto Industry Paradigm, Morgan Stanley Research (Nov. 6, 2013), available at http://www.morganstanley.com/public/11152013.html. The authors indicate that $1.3 trillion is a base case estimate and indicate a bear case scenario of $0.7 trillion savings per year in the U.S. and a bull case scenario of $2.2 trillion per year.

[31] World Urbanization Prospects The 2011 Revision, United Nations Department of Economic and Social Affairs (March 2012), http://esa.un.org/unpd/wpp/ppt/CSIS/ WUP_ 2011_CSIS_4.pdf.

[32] Nate Berg, The Uneven Future of Urbanization (April 9, 2012), http://www.citylab. com/ housing/2012/04/unevenfuture-urbanization/1707/.

[33] http://www.nist.gov/cps/sagc.cfm

[34] Frost & Sullivan.

[35] Administration Announces 14 Initial Partners in the Better Buildings Challenge, White House (June 30, 2011), http://www.whitehouse.gov/the-press-office/2011/06/30/obama-administration-announces-14-initial-partners-betterbuildings-chal.

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 8

TESTIMONY OF LANCE DONNY, CHIEF EXECUTIVE OFFICER, ONFARM. HEARING ON "THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS"[*]

Chairman Thune, Ranking Member Nelson, and Members of the Committee my name is Lance Donny. I want to thank you for the opportunity to appear before you today and share my thoughts on how connecting devices and data will enable farmers to meet global agriculture challenges.

I am the Founder and Chief Executive Officer of OnFarm, a company focused on solving the interoperability and use of devices and data in agriculture.

I grew up on my family's farm in California. I've spent more then 20 years in technology and the last half dozen leading companies in agriculture. In that time I've overseen thousands of connected devices and have studied how technology succeeds and often fails farmers.

It is clear, and the time is now, Agriculture is on the march to adopt and use technology, all of it connected, and this trend will enable farmers to make better decisions about how they grow, it will allow them to be globally competitive, it will be the driving force to meeting global food demand.

My testimony aims to highlight challenges and opportunities as we move to adopt connected devices and data:

[*] This is an edited, reformatted and augmented version of testimony presented February 11, 2015 before the Senate Committee on Commerce, Science, and Transportation.

1. as a means to increase agriculture production and profitability;
2. to help farmers afford and easily adopt technology; and
3. to advocate for smart, modern policies that spur adoption, avoid unnecessary regulation, and enable U.S. agriculture to be competitive globally.

Since the 1950s farming has doubled production through the use of supplemental nitrogen, irrigation systems, and mechanization of planting and harvesting.

But those advances, while momentous will not be sufficient to meet the growing global demand for food. By 2050 over 9.5 Billion people on the plant will require 70% more food then we produce today. We will not succeed at meeting this challenge by adding new acres, using more nitrogen or more water. [1]

Connected devices and data fundamentally change how people and industries work and agriculture has not escaped that change.

Agriculture has moved into the information age.

Data is everywhere. It drives decisions and enables farmers that adopt it to be globally competitive. In the day of $4 corn, farm prosperity will occur using technology and data as a competitive advantage against those farmers who don't.

There are two core and interconnected concepts for the Internet of Things in Agriculture. First, is the connected device itself. Today we see sensors on nearly every part of the farm: from soil moisture, to plants, equipment, and people. Sensors are the first step to better management and provide important field data, but sensors on their own will not allow the farmer to change the way they farm.

If you ask a farmer today how much data they have, you will almost always hear "too much" or "it's everywhere". This flood of data has already overwhelmed farmers. Analytics or "Big Data" software that create order and provide insights is the key to delivering the promise of the Internet of Things.

Together, connected devices and analytics give farmers the ability to monitor and use information to manage resources. And as the demand for food increases these solutions will be the tool that farmers use to help meet global demands.

In good years farmers can grow more and more efficiently. In difficult years, like the last several in California due to the drought, connected devices and analytics enable farmers to monitor their fields and to apply the precise amount of water when and where the crop needs it.

Technology studies have shown the possibilities for increasing yields by 33% while we reduce water consumption by 20% [3]. Unfortunately that technology can often be cost prohibitive. In order to ensure US farmers are globally competitive we must help farm adoption.

I support both innovation and grants that can dramatically reduce cost and increase adoption. With modest efforts we can solve these fundamental challenges. Today;

1. technology is still too costly for many farmers; we can and should support innovations and incentives that can improve adoption;
2. many farms have no broadband access and cellular coverage is unreliable; we can and should accelerate the availability of low---cost long range communication technology to ensure we can move data from the field to the cloud on every farm; and
3. I support a common sense approach to data rights such as the American Farm Bureau's Privacy and Security Principles [2] that will enable the marketplace to solve conflicts quickly and efficiently.

Technology has shown the ability to increase yield, reduce inputs, and enable more profitable and sustainable farms. If we achieve technology adoption on a wide scale, we can meet global food needs, we can help U.S. farmers maintain global competitiveness, and we can ensure the next generation of farmer is as successful as their parents' generation.

Thank you again for inviting me today, I look forward to your questions.

References

[1] "Towards Smart Farming – Agriculture Embracing the IoT Vision" --- Beecham Research Ltd., January 2, 2015, http://www.beechamresearch.com/download.aspx?id=40

[2] "Privacy and security Principals for Farm Data" – The American Farm Bureau Federation, December 19, 2014 http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciple sForFarmData.pdf

[3] "NEEA Technical Advisory Group Report – NW Agriculture Irrigation Energy Efficiency Initiative" – Northwest Energy Efficiency Alliance, January 26, 2015

[4] “10 Policy Principles for Unlocking the Potential of the Internet of Things” – Center for Data Innovation, December 4, 2014 http://www. datainnovation.org/2014/12/10---policy--- principles---for---unlocking---the---potential---of---the---internet---of--- things/

[5] “The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020,” ABI Research, August 20, 2014, https://www. abiresearch.com/press/the---internet---of---things--- will---drive---wireless---connect.

[6] “Agriculture Water Conservation in the Lower Flint River Basin of Georgia” – Flint River Basin Partnership

[7] “Ag---Tech Challenges and Opportunities for Sustainable Growth” – Kauffman Foundation, April 2014 http://www.kauffman.org/ ~/media/ kauffman org/research%20reports%20and%20covers/2014/04/ agtech whitepaper 42314 final2.pdf

[8] “Agriculture Gets Smart: The Rise of Data and Robotics” – The Cleantech Group, May 2014 http://info.cleantech.com/Ag---Get---Smart---Report---Submit.html

In: The Internet of Things
Editor: Emanuel Delgado

ISBN: 978-1-63482-442-2

Chapter 9

TESTIMONY OF ADAM THIERER, SENIOR RESEARCH FELLOW, MERCATUS CENTER AT GEORGE MASON UNIVERSITY. HEARING ON "THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS"[*]

Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the policy implications of the Internet of Things. My name is Adam Thierer, and I am a senior research fellow at the Mercatus Center at George Mason University, where I study technology policy.

My message today is condensed from a recent book[1] and a forthcoming law review article[2] on the Internet of Things, which refers to a world full of "smart" devices equipped with sensing and networking capabilities.

My research focuses primarily on the privacy and security implications of the Internet of Things and wearable technology. The three general conclusions of my work are as follows:

1) First, the Internet of Things offers compelling benefits to consumers, companies, and our country's national competitiveness that will only be achieved by adopting a flexible policy regime for this fast-moving space.

[*] This is an edited, reformatted and augmented version of testimony presented February 11, 2015 before the Senate Committee on Commerce, Science, and Transportation.

2) Second, while there are formidable privacy and security challenges associated with the Internet of Things, top-down or one-size-fits-all regulation will limit innovative opportunities.
3) Third, with those first two points in mind, we should seek alternative and less costly approaches to protecting privacy and security that rely on education, empowerment, and targeted enforcement of existing legal mechanisms. Long-term privacy and security protection requires a multifaceted approach incorporating many flexible solutions.

I will discuss each point briefly.

BENEFITS OF IOT

First, the Internet of Things will benefit the "3-Cs" of consumers, companies, and our country:

- Consumers will benefit from more of their devices being networked, sensing, and communicating. The Internet of Things offers us more choices and convenience, especially for personal health and productivity.
- Companies will benefit from increased efficiencies and the ability to offer a staggering array of new product and service options to their customers.[3]
- And our country will benefit by maintaining our global competitive advantage in the digital economy.

The magnitude of this opportunity is breathtaking.[4] Technology analysts and economic consultancies have predicted economic benefits in the *trillions* of dollars.[5]

The positive effects of the Internet of Things will reverberate throughout every sector of the economy, and as Progressive Policy Institute economist Michael Mandel notes, it "has the potential to help revive the high-growth economy."[6] It we let it, it could revolutionize manufacturing, health care, energy, transportation, retailing, and various government services.

GETTING POLICY RIGHT

If America hopes to be a global leader in the Internet of Things, as it has been for the Internet more generally over the past two decades, then we first have to get public policy right.

America took a commanding lead in the digital economy because, in the mid-1990s, Congress and the Clinton administration crafted a nonpartisan vision for the Internet that protected “permissionless innovation”—the idea that experimentation with new technologies and business models should generally be permitted without prior approval.[7]

Congress embraced permissionless innovation by passing the Telecommunications Act of 1996 and rejecting archaic Analog Era command-and-control regulations for this exciting new medium.[8]

The Clinton administration embraced permissionless innovation with its 1997 “Framework for Global Electronic Commerce,” which outlined a clear vision for Internet governance that relied on civil society, voluntary agreements, and ongoing marketplace experimentation.[9]

This nonpartisan blueprint sketched out almost two decades ago for the Internet is every bit as sensible today as we begin crafting a policy paradigm for the Internet of Things.[10]

Again, the first order of business is for policymakers to send a clear green light to entrepreneurs letting them know that our nation’s default policy position remains “innovation allowed.” Second, we should avoid basing policy interventions on hypothetical worst-case scenarios, or else best-case scenarios will never come about.[11] Our policy regime, therefore, should be responsive, not anticipatory.

FLEXIBLE SOLUTIONS

Of course, privacy- and security-related challenges exist that deserve attention. Data is going to be moving fluidly across so many platforms and devices that it will be difficult to apply traditional Fair Information Practice Principles[12] in a rigid regulatory fashion for every conceivable use of these technologies.[13]

Specifically, it will be challenging to achieve perfect “notice and choice” in a world where so many devices are capturing volumes of data in real time.

Moreover, while “data minimization” remains a worthy goal, if it is mandated in a one-size-fits-all fashion, it could limit many life-enriching innovations.

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

- Policymakers can encourage *privacy and security “by design”* for Internet of Things developers, but those best practices should not be mandated as top-down controls. Flexibility is essential.[14]
- More *privacy-enhancing tools*—especially robust encryption technologies—will also help, and government officials would be wise to promote these tools instead of restricting them.
- *Increased education* is also essential, and governments can help get the word out about inappropriate uses of these technologies.
- Existing *privacy torts and existing targeted rules* (such as “Peeping Tom” laws) will also likely evolve to address serious harms as they develop.
- Finally, the Federal Trade Commission will continue to play an important backstop role, using its Section 5 authority to *police “unfair and deceptive” practices*. The commission has already been remarkably active in encouraging companies to live up to the privacy and security promises they make to their consumers, and that will continue.

Conclusion: We Can Adapt

In closing, we should also never forget that, no matter how disruptive these new technologies may be in the short term, we humans have an extraordinary ability to adapt to technological change and bounce back from adversity.[15] That same resilience will be true for the Internet of Things.

We should remain patient and continue to embrace permissionless innovation to ensure that the Internet of Things thrives and American consumers and companies continue to be global leaders in the digital economy.

Appendices to Testimony of Adam Thierer

1) Selected Readings from Adam Thierer on the Internet of Things

2) What Is the Internet of Things?
3) Projected Use and Economic Impact of the Internet of Things
4) A Nonpartisan Policy Vision for the Internet of Things
5) Some Initial Thoughts on the FTC Internet of Things Report
6) Why "Permissionless Innovation" Matters
7) How We Adapt to Technological Change

APPENDIX 1: SELECTED READINGS FROM ADAM THIERER ON THE INTERNET OF THINGS

law review article: "The Internet of Things and Wearable Technology Addressing Privacy and Security Concerns without Derailing Innovation," forthcoming, *Richmond Journal of Law Et Technology*, Vol. 21, No. 6, (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494382.

essay: "A Nonpartisan Policy Vision for the Internet of Things," *Technology Liberation Front,* December 11, 2014, http://techliberation.com/2014/12/11/a-nonpartisan-policy-vision-for-the-internet-of-things.

essay: "Some Initial Thoughts on the FTC Internet of Things Report," *Technology Liberation Front,,* January 28, 2015, http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-ofthings-report.

essay: "Striking a Sensible Balance on the Internet of Things and Privacy," *Technology Liberation Front,,* January 16, 2015, http://techliberation.com/2015/01/16/striking-a-sensible-balance-on-the-internetof-things-and-privacy.

slide presentation: "Policy Issues Surrounding the Internet of Things & Wearable Technology," September 12, 2014, http://techliberation.com/2014/09/12/slide-presentation-policy-issues-surrounding-theinternet-of-things-wearable-technology.

essay: "CES 2014 Report: The Internet of Things Arrives, but Will Washington Welcome It?" *Technology Liberation Front,,* January 8, 2014, http://techliberation.com/2014/01/08/ces-2014-report-the-internet-of-things-arrives-but-will-washington-welcome-it.

essay: "The Growing Conflict of Visions over the Internet of Things & Privacy," *Technology Liberation Front,,* January 14, 2014, http://techliberation.com/2014/01/14/the-growing-conflict-of-visions-overthe-internet-of-things-privacy.

op-ed: “Can We Adapt to the Internet of Things?” *IAPP Privacy Perspectives*, June 19, 2013, https://privacyassociation.org/news/a/can-we-adapt-to-the-internet-of-things.

agency filing: My Filing to the FTC in its ‘Internet of Things’ Proceeding, May 31, 2013, http://techliberation.com/2013/05/31/my-filing-to-the-ftc-in-its-internet-of-things-proceeding.

book: *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2014), http://mercatus.org/permissionless/ permissionless inno vation.html.

essay: “What’s at Stake with the FTC’s Internet of Things Workshop,” *Technology Liberation Front,,* November 18, 2013, http://techliberation.com/2013/11/18/whats-at-stake-with-the-ftcs-internet-ofthings-workshop.

law review article: “Removing Roadblocks to Intelligent Vehicles and Driverless Cars,” forthcoming, *Wake Forest Journal of Law Et Policy* (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496929.

APPENDIX 2: WHAT IS THE INTERNET OF THINGS?[16]

Many of the underlying drivers of the Internet and Information Age revolution—massive increases in processing power, exploding storage capacity, steady miniaturization of computing and cameras, ubiquitous wireless communications and networking capabilities, digitization of all data, and massive datasets (or “big data”)—are beginning to have a profound influence beyond the confines of cyberspace. It is cheaper than ever, for example, to integrate a microchip, a sensor, a camera, and even an accelerometer into devices today. “Thanks to advances in circuits and software,” observe Neil Gershenfeld and J. P. Vasseur, “it is now possible to make a Web server that fits on (or in) a fingertip for $1.” As costs continue to fall and these technologies are increasingly embedded into almost all devices that consumers own and come into contact with, a truly “seamless web” of connectivity and “pervasive computing” will exist.

As a result of these factors, mundane appliances and other machines and devices that consumers have long taken for granted—cars, refrigerators, cooking devices, lights, weight scales, watches, jewelry, eyeglasses, and even their clothing—will all soon be networked, sensing, automated, and communicating. In other words, consumers are transitioning to what Alex Hawkinson, CEO and founder of SmartThings, calls a "programmable world" where "things will become intuitive [and] connectivity will extend even further, to the items we hold most dear, to those things that service the everyday needs of the members of the household, and beyond."[17]

This so-called Internet of Things—or "machine-to-machine" connectivity and communications—promises to usher in "a third computing revolution"[18] and bring about profound changes that will rival the first wave of Internet innovation. The first use of the term Internet of Things is attributed to Kevin Ashton, who used it in the title of a 1999 presentation.[19] A decade later, he reflected on the term and its meaning:

> If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best.
>
> We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory. RFID [radio-frequency identification] and sensor technology enable computers to observe, identify, and understand the world—without the limitations of human-entered data.[20]

More recently, analysts with Morrison & Foerster have defined IoT as "the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings."[21] These low-power devices typically rely on sensor technologies as well as existing wireless networking systems and protocols (Wi-Fi, Bluetooth, near field communication, and GPS) to facilitate those objectives. In turn, this reliance will fuel the creation of even more "big data." Many of these technologies and capabilities will eventually operate in the background of consumers' lives and be almost invisible to them.

IoT is sometimes understood as being synonymous with "smart" systems: smart homes, smart buildings, smart appliances, smart health, smart mobility, smart cities, and so on. Smart car technology is also expanding rapidly.[22] The promise of IoT, as described by New York Times reporter Steve Lohr, is that "billions of digital devices—from smartphones to sensors in homes, cars, and machines of all kinds—will communicate with each other to automate tasks and make life better."[23] "Consumers and public officials can use the connected world to improve energy conservation, efficiency, productivity, public safety, health, education, and more," predicts CEA.[24] "The connected devices and applications that consumers choose to adopt will make their lives easier, safer, healthier, less expensive, and more productive."[25] In addition to giving consumers more control over their lives, these technologies can also help them free up time by automating routine tasks and chores.

Appendix 3: Projected Use and Economic Impact of the Internet of Things26

The Internet of Things is already growing at a breakneck pace and is expected to continue to accelerate rapidly. Below is a summary of recent forecasts regarding the growing device connectivity as well as potential economic benefits of the IoT.

A. Connectivity

- *Cisco* projects that 37 billion intelligent things will be connected and communicating by 2020.[27]
- *ABI Research* estimates that there are more than 10 billion wirelessly connected devices in the market today and more than 30 billion devices expected by 2020.[28]
- **I***DC* (International Data Corporation) predicts far greater penetration of 212 billion devices installed globally by the end of 2020.[29]
- *Gartner* anticipates that 25 billion Internet of Things devices will be in operation by 2020.[30]
- *VisionMobile* projects that the number of IoT developers will grow from roughly 300,000 in 2014 to more than 4.5 million by 2020.[31]
- *Business Insider* estimates that will be a total of 23.4 billion Internet of Things devices connected by 2019 and that their adoption will be driven by the enterprise and manufacturing sectors.[32]
- *Harbor* projects that 21.7 billion Internet of Things devices will be connected and in use by 2019.[33]

- *Machina Research* reports that roughly 7.2 billion "machine-to-machine connected consumer electronic devices" will be in global use by 2023.[34]
- *Navigant Research* states that more than 1 billion smart meters will be installed globally by 2022, up from 313 million in 2013.[35]
- *IHS Automotive* anticipates that the number of cars connected to the Internet will grow more than six fold from 2013 to reach 152 million internationally by 2020.36
- *ON World projects* that roughly 100 million Internet-connected wireless lights will be in operation by 2020.37

B. Economic Impact

- *McKinsey Global Institute* researchers estimate the potential economic impact of IoT technologies to be from $2.7 to $6.2 trillion per year by 2025.[38]
- *IDC* estimated in 2013 that this market would grow at a compound annual growth rate of 7.9 percent to reach $8.9 trillion by 2020.[39]
- *Cisco* analysts estimate that IoT will create $14.4 trillion in value between 2013 and 2022.[40]
- *Business Insider* estimates that IoT will add approximately $5.6 trillion in value to the global economy in between 2014 and 2019.[41]
- *Accenture* estimates that the industrial IoT could add $14.2 trillion to the global economy by 2030, and that the US economy will gain at least $6.1 trillion in cumulative GDP by that year.[42]
- *General Electric* projects that industrial IoT technologies will add about $15 trillion to global GDP by 2030 (in constant 2005 dollars).[43]
- *Morgan Stanley* forecasts that driverless cars will save the US economy $1.3 trillion per year once autonomous cars fully penetrate the market, while saving the world another $5.6 trillion a year.[44]

Appendix 4: A Nonpartisan Policy Vision for the Internet of Things[45]

What sort of public policy vision should govern the Internet of Things? I recently heard three public policymakers articulate their recommended vision for the Internet of Things (IoT), and I found their approach so inspiring that I wanted to discuss it here in the hopes that it will become the foundation for future policy in this arena.

On December 4, 2015, it was my pleasure to attend a Center for Data Innovation (CDI) event on "How Can Policy-makers Help Build the Internet of Things?" As the title implied, the goal of the event was to discuss how to achieve the vision of a more fully connected world and, more specifically, how public policymakers can help facilitate that objective. It was a terrific event with many excellent panel discussions and keynote addresses.

Two of those keynotes were delivered by Senators Deb Fischer (R-Neb.) and Kelly Ayotte (R-N.H.). Below I offer some highlights from their remarks and then relate them to the vision set forth by Federal Trade Commission (FTC) Commissioner Maureen K. Ohlhausen in some of her recent speeches. I will conclude by discussing how the Ayotte-Fischer-Ohlhausen vision can be seen as the logical extension of the Clinton administration's excellent 1997 "Framework for Global Electronic Commerce," which proposed a similar policy paradigm for the Internet more generally. This shows how crafting policy for the IoT can and should be a nonpartisan affair.

A. Sen. Deb Fischer's Remarks

In her opening remarks at the CDI event in December 2014, Sen. Deb Fischer explained how "the Internet of Things can be a game changer for the U.S. economy and for the American consumer." "It gives people more information and better tools to analyze data to make more informed choices," she noted.

After outlining some of the potential benefits associated with the Internet of Things, Sen. Fischer continued on to explain why it is essential we get public policy incentives right first if we hope to unlock the full potential of these new technologies. Specifically, she argued that:

> In order for Americans to receive the maximum benefits from increased connectivity, there are two things the government must avoid. First, policymakers can't bury their heads in the sand and pretend this technological revolution isn't happening, only to wake up years down the road and try to micro-manage a fast-changing, dynamic industry.
>
> Second, the federal government must also avoid regulation just for the sake of regulation. We need thoughtful, pragmatic responses

> and narrow solutions to any policy issues that arise. For too long, the only "strategy" in Washington policy-making has been to react to crisis after crisis. We should dive into what this means for U.S. global competitiveness, consumer welfare, and economic opportunity before the public policy challenges overwhelm us, before legislative and executive branches of government—or foreign governments—react without all the facts.

Fischer concluded by noting, "It's entirely appropriate for the U.S. government to think about how to modernize its regulatory frameworks, consolidate, renovate, and overhaul obsolete rules. We're destined to lose to the Chinese or others if the Internet of Things is governed in the United States by rules that pre-date the VCR."

B. Sen. Kelly Ayotte's Remarks

Like Sen. Fischer, Ayotte similarly stressed the many economic opportunities associated with IoT technologies for both consumers and producers alike. Ayotte also noted that IoT is going to be a major topic for the Senate Commerce Committee. She said that the role of the Committee will be to ensure that the various agencies looking into IoT issues are not issuing "conflicting regulatory directives" and "that what is being done makes sense and allows for future innovation that we can't even anticipate right now." Among the agencies she cited that are currently looking into IoT issues: FTC (privacy and security), FDA (medical device applications), FCC (wireless issues), FAA (commercial drones), NHTSA (intelligent vehicle technology), and NTIA (multi-stakeholder privacy reviews) as well as state lawmakers and regulatory agencies.

Sen. Ayotte then explained what sort of policy framework America needed to adopt to ensure that the full potential of the Internet of Things could be realized. She framed the choice lawmakers are confronted with as follows:

> We as policymakers we can either create an environment that allows that to continue to grow, or one that thwarts that. To stay on the cutting edge, we need to make sure that our regulatory environment is conducive to fostering innovation." [. . .] We're living in the Dark Ages in the ways the some of the regulations have been framed. Companies must be properly incentivized to invest in the future, and government shouldn't be a deterrent to innovation and job-creation.

Ayotte also stressed that “technology continues to evolve so rapidly there is no one-size-fits-all regulatory approach” that can work for a dynamic environment like this. “If legislation drives technology, the technology will be outdated almost instantly,” and “that is why humility is so important,” she concluded.

The better approach, she argued was to let technology evolve freely in a “permissionless” fashion and then see what problems developed and then address them accordingly. “[A] top-down, preemptive approach is never the best policy” and will only serve to stifle innovation, she argued. “If all regulators looked with some humility at how technology is used and whether we need to regulate or not to regulate, I think innovation would stand to benefit.”

C. FTC Commissioner Maureen K. Ohlhausen

Fischer and Ayotte’s remarks reflect a vision for the Internet of Things that FTC Commissioner Maureen K. Ohlhausen has articulated in recent months. In fact, Sen. Ayotte specifically cited Ohlhausen in her remarks.

Ohlhausen has actually delivered several excellent speeches on these issues and has become one of the leading public policy thought leaders on the Internet of Things in the United States today. One of her first major speeches on these issues was her October 2013 address entitled, “The Internet of Things and the FTC: Does Innovation Require Intervention?” In that speech, Ohlhausen noted that, “The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors.”

She also issued a wise word of caution to her fellow regulators:

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

In this and other speeches, Ohlhausen has highlighted the various other remedies that already exist when things do go wrong, including FTC enforcement of "unfair and deceptive practices," common law solutions (torts and class actions), private self-regulation and best practices, social pressure, and so on.

D. The Clinton Administration Vision

These three women have articulated what I regard as the ideal vision for fostering the growth of the Internet of Things. It should be noted, however, that their framework is really just an extension of the Clinton administration's outstanding vision for the Internet more generally.

In the 1997 "Framework for Global Electronic Commerce," the Clinton administration outlined its approach toward the Internet and the emerging digital economy. As I've noted many times before, the framework was a succinct and bold market-oriented vision for cyberspace governance that recommended reliance upon civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve information-age problems. Specifically, it stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry." "[G]overnments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce."

Sen. Ayotte specifically cited those Clinton principles in her speech and said, "I think those words, given twenty years ago at the infancy of the Internet, are today even more relevant as we look at the challenges and the issues that we continue to face as regulators and policymakers."

I completely agree. This is exactly the sort of vision that we need to keep innovation moving forward to benefit consumers and the economy, and this illustrates how IoT policy can be a bipartisan effort.

Why does this matter so much? As I noted in this essay from November 2014, thanks to the Clinton administration's bold vision for the Internet:

> This policy disposition resulted in an unambiguous green light for a rising generation of creative minds who were eager to explore this new frontier for commerce and communications. . . . The result of this freedom to experiment was an outpouring of innovation. America's info-tech sectors thrived thanks to permissionless innovation, and they still do today. An annual Booz & Company report on the world's most innovative companies revealed that 9 of the top 10 most innovative companies are based in the U.S. and that

> most of them are involved in computing, software, and digital technology.[46]

In other words, America had the policy right before and we can get the policy right again. Patience, flexibility, and forbearance are the key policy virtues that nurture an environment conducive to entrepreneurial creativity, economic progress, and greater consumer choice.

Other policymakers should endorse the vision originally sketched out by the Clinton administration and now so eloquently embraced and extended by Sen. Fischer, Sen. Ayotte, and Commissioner Ohlhausen. This is the path forward if we hope to realize the full potential of the Internet of Things.

APPENDIX 5: SOME INITIAL THOUGHTS ON THE FTC INTERNET OF THINGS REPORT[47]

On January 27, 2015, the Federal Trade Commission (FTC) released its long-awaited report on “The Internet of Things: Privacy and Security in a Connected World.” The 55-page report is the result of a lengthy staff exploration of the issue, which kicked off with an FTC workshop on the issue that was held on November 19, 2013.

In this essay, I will offer a few general thoughts on the FTC’s report and its overall approach to the Internet of Things and then discuss a few specific issues that I believe deserve further attention.

A. Big Picture, Part 1: Should Best Practices Be Voluntary or Mandatory?

Generally speaking, the FTC’s report contains a variety of “best practice” recommendations to get Internet of Things innovators to take steps to ensure greater privacy and security “by design” in their products. Most of those recommended best practices are sensible as *general guidelines* for innovators, but the really sticky question here continued to be this: When, if ever, should “best practices” become binding regulatory requirements?

The FTC does a bit of a dance when answering that question. Consider how, in the executive summary of the report, the Commission answers the question regarding the need for additional privacy and security regulation: “Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature.” But, just a few lines later, the agency (1) “reiterates the Commission’s previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach,” and (2) “recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation.”

Here and elsewhere, the agency repeatedly stresses that it is not seeking IoT-specific regulation, merely “broad-based” digital privacy and security legislation.

The problem is that once you understand what the IoT is all about you come to realize that this largely represents a distinction without a difference. The Internet of Things is simply the extension of the Net into everything we own or come into contact with. Thus, this idea that the agency is not seeking IoT-specific rule sounds terrific until you realize that it is actually seeking something far more sweeping—greater regulation of *all* online and digital interactions. And because “the Internet” and “the Internet of Things” will eventually (if they are not already) be consider synonymous, this notion that the agency is not proposing technology-specific regulation is really quite silly.

Now, it remains unclear whether there exists any appetite on Capitol Hill for “comprehensive” legislation of any variety, although perhaps we’ll learn more about that possibility when the Senate Commerce Committee hosts a hearing on these issues on February 11. But at least so far, “comprehensive” or “baseline” digital privacy and security bills have been non-starters.

And that’s for good reason in my opinion: Such regulatory proposals could take us down the path that Europe charted in the late 1990s with onerous “data directives” and suffocating regulatory mandates for the IT and computing sector. The results of this experiment have been unambiguous, as I documented in congressional testimony in 2013. I noted there how America’s Internet sector came to be the envy of the world while it was hard to name any major Internet company from Europe. Whereas America embraced “permissionless innovation” and let creative minds develop one of the greatest success stories in modern history, the Europeans adopted a “Mother, may I?” regulatory approach for the digital economy. America’s more flexible, light-touch regulatory regime leaves more room for competition and innovation compared to Europe’s top-down regime. Digital innovation suffered over there while it blossomed here.

That’s why we need to be careful about adopting the sort of “broad-based” regulatory regime that the FTC recommends in this and previous reports.

B. Big Picture, Part 2: Does the FTC Really Need More Authority?

Something else is going on in this report that has also been happening in all the FTC's recent activity on digital privacy and security matters: The agency has been busy laying the groundwork for its own expansion.

In this latest report, for example, the FTC argues that:

> Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections. ... The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach.

In other words, this agency wants more authority. And we are talking about sweeping authority here that would transcend its *already sweeping* authority to police "unfair and deceptive practices" under Section 5 of the FTC Act. Let's be clear: It would be hard to craft a law that grants an agency more comprehensive and open-ended consumer protection authority than Section 5. The meaning of those terms—"unfairness" and "deception"—has always been a contentious matter, and at times the agency has abused its discretion by exploiting that ambiguity.

Nonetheless, Section 5 remains a powerful enforcement tool for the agency and one that has been wielded aggressively in recently years to police digital economy giants and small operators alike. Generally speaking, I'm alright with *most* Section 5 enforcement, especially since that sort of retrospective policing of unfair and deceptive practices is far less likely to disrupt permissionless innovation in the digital economy. That's because it does not subject digital innovators to the sort of "Mother, may I?" regulatory system that European entrepreneurs face. But an expansion of the FTC's authority via more "comprehensive, baseline" privacy and security regulatory policies threatens to convert America's more sensible bottom-up and responsive regulatory system into the sort of innovation-killing regime we see on the other side of the Atlantic.

Here's the other thing we can't forget when it comes to the question of what additional authority to give the FTC over privacy and security matters: The FTC is not the end of the enforcement story in America. Other enforcement mechanisms exist, including privacy torts, class action litigation, property and contract law, state enforcement agencies, and other targeted privacy statutes. I’ve summarized all these additional enforcement mechanisms in my 2014 law review article referenced above.

C. FIPPS, Part 1: Notice and Choice vs. Use-Based Restrictions

Let’s drill down a bit and examine some of the specific privacy and security best practices that the agency discusses in its new IoT report.

The FTC report highlights how the IoT creates serious tensions for many traditional Fair Information Practice Principles (FIPPs). The FIPPs generally include (1) notice, (2) choice, (3) purpose specification, (4) use limitation, and (5) data minimization. But the report is mostly focused on notice and choice as well as data minimization.

When it comes to notice and choice, the agency wants to keep hope alive that it will still be applicable in an IoT world. I’m sympathetic to this effort because it is quite sensible for *all* digital innovators to do their best to provide consumers with adequate notice about data collection practices and then give them sensible choices about it. Yet, like the agency, I agree that “offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface.”

The agency has a nuanced discussion of how context matters in providing notice and choice for IoT, but one can’t help but think that even they must realize that the game is over, to some extent. The increasing miniaturization of IoT devices and the ease with which they suck up data means that traditional approaches to notice and choice just aren’t going to work all that well going forward. It is almost impossible to envision how a rigid application of traditional notice and choice procedures would work in practice for the IoT.

Relatedly, as I wrote in January 2015, the Future of Privacy Forum (FPF) released a white paper entitled, “A Practical Privacy Paradigm for Wearables,” that notes how FIPPs “are a valuable set of high-level guidelines for promoting privacy, [but] given the nature of the technologies involved, traditional implementations of the FIPPs may not always be practical as the Internet of Things matures.” That’s particularly true of the notice and choice FIPPS.

But the FTC isn’t quite ready to throw in the towel and make the complete move toward “use-based restrictions,” as many academics have. Use-based restrictions would focus on specific uses of data that are particularly sensitive and for which there is widespread agreement they should be limited or disallowed altogether. But use-based restrictions are, ironically, controversial from both the perspective of industry and privacy advocates (albeit for different reasons, obviously).

The FTC doesn't really know where to go next with use-based restrictions. The agency says that, on one hand, "has incorporated certain elements of the use-based model into its approach" to enforcement in the past. On the other hand, the agency says it has concerns "about adopting a pure use-based model for the Internet of Things," since it may not go far enough in addressing the growth of more widespread data collection, especially of more sensitive information.

In sum, the agency appears to be keeping the door open on this front and hoping that a best-of-all-worlds solution miraculously emerges that extends *both* notice and choice and use-based limitations as the IoT expands. But the agency's new report doesn't give us any sort of blueprint for how that might work, and that's likely for good reason: because it probably won't work at that well in practice, and there will be serious costs in terms of lost innovation if they try to force unworkable solutions on this rapidly evolving marketplace.

D. FIPPS, Part 2: Data Minimization

The biggest policy fight that is likely to come out of this report involves the agency's push for data minimization. To minimize the risks associated with excessive data collection, the report recommends that:

> Companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or deidentify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data.

This is an unsurprising recommendation in light of the fact that, in previous major speeches on the issue, FTC Chairwoman Edith Ramirez argued that “information that is not collected in the first place can’t be misused” and that:

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

In my forthcoming law review article, I discussed the problem with such reasoning at length and note:

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

FTC Commissioner Josh Wright issued a dissenting statement to the report that lambasted the staff for not conducting more robust cost-benefit analysis of the new proposed restrictions and specifically cited how problematic the agency’s approach to data minimization was. “[S]taff merely acknowledges it would potentially curtail innovative uses of data . . . [w]ithout providing any sense of the magnitude of the costs to consumers of foregoing this innovation or of the benefits to consumers of data minimization,” he says. Similarly, in her separate statement, FTC Commissioner Maureen K. Ohlhausen worried about the report’s overly precautionary approach on data minimization when noting that, “without examining costs or benefits, [the staff report] encourages companies to delete valuable data—primarily to avoid hypothetical future harms. Even though the report recognizes the need for flexibility for companies weighing whether and what data to retain, the recommendation remains overly prescriptive," she concludes.

Regardless, the battle lines have been drawn by the FTC staff report as the agency has made it clear that it will be stepping up its efforts to get IoT innovators to significantly slow or scale back their data collection efforts. It will be very interesting to see how the agency enforces that vision going forward and how it impacts innovation in this space. All I know is that the agency has not conducted a serious evaluation here of the trade-offs associated with such restrictions. I penned another law review article in 2014 offering "A Framework for Benefit-Cost Analysis in Digital Privacy Debates" that they could use to begin that process if they wanted to get serious about it.

F. The Problem with the "Regulation Builds Trust" Argument

One of the interesting things about this and previous FTC reports on privacy and security matters is how often the agency premises the case for expanded regulation on "building trust." The argument goes something like this (as found on page 51 of the new IoT report): "Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected."

This is one of those commonly-heard claims that sounds so straightforward and intuitive that few dare question it. But there are problems with the logic of the we-need-regulation-to-build-trust-and-boost-adoption arguments we often hear in debates over digital privacy.

First, the agency bases its argument mostly on polling data. "Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices," the report says. Well, of course surveys say that! It's only logical that consumers will say this, just as they will always say they value privacy and security more generally when asked. You might as well ask people if they love their mothers!

What consumers claim to care about and what they actually do in the real-world are often two very different things. In the real-world, people balance privacy and security alongside many other values, including choice, convenience, cost, and more. This leads to the so-called "privacy paradox," or the problem of many people saying one thing and doing quite another when it comes to privacy matters. Put simply, people take some risks, including some privacy and security risks, to reap other rewards or benefits. (See this essay for more on the problem with most privacy polls.)

Second, online activity and the Internet of Things are both growing like gangbusters despite the privacy and security concerns that the FTC raises. Virtually every metric I've looked at that track IoT activity show astonishing growth and product adoption, and projections by all the major consultancies that have studied this consistently predict the continued rapid growth of IoT activity. Now, how can this be the case if, as the FTC claims, we'll only see the IoT really take off after we get more regulation aimed at bolstering consumer trust? Of course, the agency might argue that the IoT will grow *at an even faster clip* than it is right now, but there is no way to prove one way or the other. In any event, the agency cannot possible claim that the IoT isn't already growing at a very healthy clip. Indeed, a lot of the hand-wringing the staff engages in throughout the report is premised precisely on the fact that the IoT is exploding faster that our ability to keep up with it. In reality, it seems far more likely that *cost and complexity* are the bigger impediments to faster IoT adoption, just as cost and complexity have always been the factors weighing most heavily on the adoption of other digital technologies.

Third, let's say that the FTC is correct—and it is—when it says that *a certain amount* of trust is needed in terms of IoT privacy and security before consumers are willing to use more of these devices and services in their everyday lives. Does the agency imagine that IoT innovators don't know that? Are markets and consumers completely irrational?

The FTC says on page 44 of the report that, "If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust." Well, if such a mismatch does exist, then the assumption should be that consumers can and will push back or seek out new and better options. And other companies should be able to sense the market opportunity here to offer a more privacy-centric offering for those consumers who demand it to win their trust and business.

Finally, and perhaps most obviously, the problem with the argument that increased regulation will help IoT adoption is that it ignores how the regulations put in place to achieve greater "trust" might become so onerous or costly in practice that there won't be as many innovations for us to adopt to begin with! Again, regulation, even very well-intentioned regulation, has costs and trade-offs.

In any event, if the agency is going to premise the case for expanded privacy regulation on this notion, they are going to have to do far more to make their case besides simply asserting it.

F. Once Again, No Appreciation of the Potential for Societal Adaptation

Let's briefly shift to a subject that isn't discussed in the FTC's new IoT report at all.

Major reports and statements by public policymakers about rapidly-evolving emerging technologies are always initially prone to stress panic over patience. Rarely are public officials willing to step-back, take a deep breath, and consider how a resilient citizenry might adapt to new technologies as they gradually assimilate new tools into their lives.

That is really sad, when you think about it, since humans have again and again proven capable of responding to technological change in creative ways by adopting new personal and social norms. I won't belabor the point because I've already written volumes on this issue elsewhere. I tried to condense all my work into a single essay entitled, "Muddling Through: How We Learn to Cope with Technological Change." Here's the key takeaway:

> Humans have exhibited the uncanny ability to adapt to changes in their environment, bounce back from adversity, and learn to be resilient over time. A great deal of wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures while both developing new technologies and learning how to live with them. I believe it wise to continue to be open to new forms of innovation and technological change, not only because it provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve — and to learn from it. More often than not, I argue, citizens have found ways to adapt to technological change by employing a variety of coping mechanisms, new norms, or other creative fixes.

Again, you almost never hear regulators or lawmakers discuss this process of individual and social adaptation even though they must know there is something to it. One explanation is that every generation has their own techno-boogeymen and lose faith in the ability of humanity to adapt to it.

To believe that we humans are resilient, adaptable creatures should not be read as being indifferent to the significant privacy and security challenges associated with any of the new technologies in our lives today, including IoT technologies. Overly exuberant techno-optimists are often too quick to adopt a "Just get over it!" attitude in response to the privacy and security concerns raised by others. But it is equally unreasonable for those who are worried about those same concerns to utterly ignore the reality of human adaptation to new technologies realities.

G. Why Are Educational Approaches Merely an Afterthought?

One final thing that troubled me about the FTC report was the way consumer and business education is mostly an afterthought. This is one of the most important roles that the FTC can and should play in terms of explaining potential privacy and security vulnerabilities to the general public and product developers alike.

Alas, the agency devotes so much ink to the more legalistic questions about how to address these issues, that all we end up with in the report is this one paragraph on consumer and business education:

> Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

I applaud that language, and I very much hope that the agency is serious about plowing more effort and resources into developing new consumer and business education materials in this area. But I'm a bit surprised that the FTC report didn't even bother mentioning the excellent material already available on the "On Guard Online" website that it helped create with a dozen other federal agencies. Worse yet, the agency failed to highlight the many other privacy education and "digital citizenship" efforts that are underway today to help on this front.

I hope that the agency spends a little more time working on the development of new consumer and business education materials in this area instead of trying to figure out how to craft a quasi-regulatory regime for the Internet of Things. As I noted in 2014 in this *Maine Law Review* article, that would be a far more productive use of the agency's expertise and resources. I argued there that "policymakers can draw important lessons from the debate over how best to protect children from objectionable online content" and apply them to debates about digital privacy. Specifically, after a decade of searching for legalistic solutions to online safety concerns—and convening a half-dozen blue ribbon task forces to study the issue—we finally saw a rough consensus emerge that no single "silver bullet" technological solutions or legal quick-fixes would work and that, ultimately, education and empowerment represented the better use of our time and resources. What was true for child safety is equally true for privacy and security for the Internet of Things.

It is a shame the FTC staff squandered the opportunity it had with this new report to highlight all the good that could be done by getting more serious about focusing first on those alternative, bottom-up, less costly, and less controversial solutions to these challenging problems. One day we'll all wake up and realize that we spent a lost decade debating legalistic solutions that were either technically unworkable or politically impossible. Just imagine if all the smart people who were spending all their time and energy on those approaches right now were instead busy devising and pushing educational and empowerment-based solutions instead!

One day we'll get there. Sadly, if the FTC report is any indication, that day is still a ways off.

APPENDIX 6: WHY "PERMISSIONLESS INNOVATION" MATTERS[48]

A. Innovation Policy: Attitudes Matter

"Why does economic growth ... occur in some societies and not in others?" asked Joel Mokyr in his 1990 book, *Lever of Riches: Technological Creativity and Economic Progress*.[49] Debate has raged among generations of economists, historians, and business theorists over that question and the specific forces and policies that prompt longterm growth.

As varied as their answers have been, there was at least general agreement that *institutional* factors mattered most: it was really just a question of what mix of them would fuel the most growth. Those institutional factors include: government stability, the enforceability of contracts and property rights, tax and fiscal policies, trade policies, regulatory factors, labor costs, educational policies, research and development expenditures, infrastructure, demographics, and environmental factors.[50]

This leads many scholars and policymakers to speak of innovation policy as if it is simply a Goldilocks-like formula that entails tweaking various policy dials to get innovation *just right*.[51] Such thinking animates the Obama administration's "Strategy for American Innovation," which catalogs "policies to promote critical components of the American innovation ecosystem."[52] The White House claims its strategy plays a "critical role in guiding the development of new policy initiatives that can help unleash the transformative innovation that leads to long-term economic growth."[53]

Unfortunately, far less attention has been paid to the role that *values*—cultural attitudes, social norms, and political pronouncements—play in influencing opportunities for entrepreneurialism, innovation, and long-term growth.[54] Does a socio-political system respect what Deirdre McCloskey refers to as the "bourgeois virtues" that incentivize invention and propel an economy forward?[55] "A big change in the common opinion about markets and innovation," she has argued, "caused the Industrial Revolution, and then the modern world. ... The result was modern economic growth."[56]

There are limits to how much policymakers can influence these attitudes and values, of course. Nonetheless, to the extent they hope to foster the positive factors that give rise to expanded entrepreneurial opportunities, policymakers should appreciate how growth-oriented innovation *policy* begins with the proper policy *disposition*.[57]

As Mokyr notes, "technological progress requires above all tolerance toward the unfamiliar and the eccentric."[58]

For innovation and growth to blossom, entrepreneurs need a clear green light from policymakers that signals a general acceptance of risk-taking, especially risk-taking that challenges existing business models and traditional ways of doing things.[59] We can think of this disposition as "permissionless innovation." If there was one thing every policymaker could do to help advance long-term growth, it is to first commit themselves to advancing this ethic and making it the lodestar for all their future policy pronouncements and decisions.

B. Permissionless Innovation vs. the Precautionary Principle

While it would seem self-evident that pro-innovation attitudes matter and that a general embrace of risk-taking and commercial pursuits is crucial to unlocking entrepreneurial creativity and opportunities, scholars have typically failed to put a name on this disposition. "Permissionless innovation" is a phrase of recent (but uncertain) origin that nicely summarizes that vision. Permissionless innovation refers to the notion that experimentation with new technologies and business models should generally be permitted by default.[60] Unless a compelling case can be made that a new invention or business model will bring serious harm to individuals, innovation should be allowed to continue unabated, and problems, if they develop at all, can be addressed later.

Permissionless innovation is not an absolutist position that rejects any role for government. Rather, it is an aspirational goal that stresses the benefit of "innovation allowed" as the default position to begin policy debates. It switches the burden of proof to those who favor preemptive regulation and asks them to explain why ongoing trial-and-error experimentation with new technologies or business models should be disallowed.

This disposition stands in stark contrast to the sort of "precautionary principle" thinking that often governs policy toward emerging technologies. The precautionary principle refers to the belief that new innovations should be curtailed or disallowed until their developers can prove that they will not cause any harms to individuals, groups, specific entities, cultural norms, or various existing laws, norms, or traditions.[61]

When the precautionary principle's "better to be safe than sorry"[62] approach is applied through preemptive constraints, opportunities for experimentation and entrepreneurialism are stifled. While some steps to anticipate or to control for unforeseen circumstances are sensible, going overboard with precaution forecloses opportunities and experiences that offer valuable lessons for individuals and society. The result is less economic and social dynamism.

Innovation is more likely in systems that maximize breathing room for ongoing economic and social experimentation, evolution, and adaptation. Societies that appreciate those values—and allow them to influence both social norms and policy decisions—are likely to experience greater economic growth.[63] By contrast, those that deride such values and adopt a more precautionary policy approach are more likely to discourage innovation and languish economically.

Unlocking long-term growth opportunities, therefore, depends upon a rejection of precautionary principle thinking and an embrace of permissionless innovation as the default policy disposition.

C. The Secret Ingredient that Powered the Information Revolution

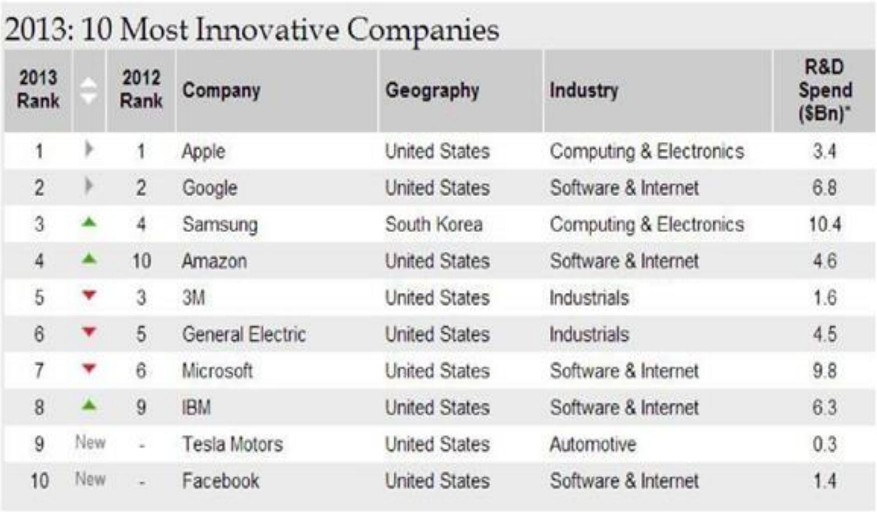
Consider how permissionless innovation powered the explosive growth of the Internet and America's information technology sectors (computing, software, Internet services, etc.) over the past two decades. Those sectors have ushered in a generation of innovations and innovators that are now the envy of the world.[64] This happened because the default position for the digital economy was permissionless innovation. No one had to ask anyone for the right to develop these new technologies and platforms.[65]

A series of decisions and statements in the mid-1990s paved the way, beginning with the Clinton administration's decision to allow commercialization of what was previously just the domain of government agencies and university researchers. Shortly thereafter, Congress passed, and President Clinton signed, the Telecommunications Act of 1996, which notably avoided regulating the Internet like earlier communications and media technologies. Later, in 1998, the Internet Tax Freedom Act was passed, which blocked governments from imposing discriminatory taxes on the Internet.

Perhaps most important, in 1997, the Clinton administration's released its "Framework for Global Electronic Commerce," outlining its approach toward the Internet and the emerging digital economy.[66] The framework was a succinct and bold market-oriented vision for cyberspace governance that recommended reliance upon civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve information age problems.[67] Specifically, it stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry."[68] "[G]overnments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce."[69]

This policy disposition resulted in an unambiguous green light for a rising generation of creative minds who were eager to explore this new frontier for commerce and communications. As Federal Trade Commission Commissioner Maureen K. Ohlhausen observes, "the success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."[70]

The result of this "freedom to experiment" was an outpouring of innovation. America's info-tech sectors thrived thanks to permissionless innovation, and they still do today. A 2013 Booz & Company report on the world's most innovative companies revealed that 9 of the top 10 most innovative companies are based in the United States and that most of them are involved in computing, software, and digital technology.



2013: 10 Most Innovative Companies

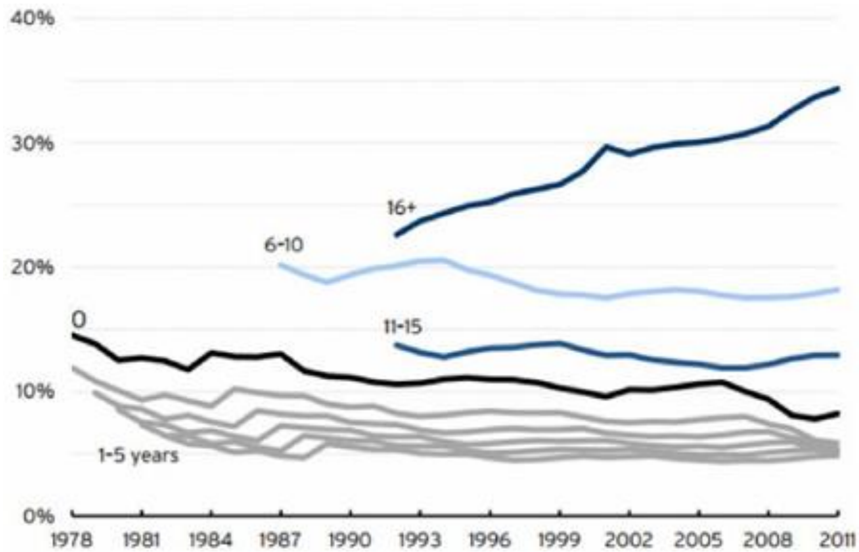
2013 Rank	⇕	2012 Rank	Company	Geography	Industry	R&D Spend ($Bn)*
1	▸	1	Apple	United States	Computing & Electronics	3.4
2	▸	2	Google	United States	Software & Internet	6.8
3	▲	4	Samsung	South Korea	Computing & Electronics	10.4
4	▲	10	Amazon	United States	Software & Internet	4.6
5	▼	3	3M	United States	Industrials	1.6
6	▼	5	General Electric	United States	Industrials	4.5
7	▼	6	Microsoft	United States	Software & Internet	9.8
8	▲	9	IBM	United States	Software & Internet	6.3
9	New	-	Tesla Motors	United States	Automotive	0.3
10	New	-	Facebook	United States	Software & Internet	1.4

D. And What's Good for the Goose ...

What's even more powerful about this story is how the information technology and "data-driven innovation" became the goose that laid the golden eggs for the broader US economy.[71] Brink Linsdey has noted that "economists generally agree that information technology (IT) was behind the decade of high TFP [total factor productivity] growth that ran from the mid-1990s to the mid-2000s."[72] It also boosted overall economic growth during that period.[73]

If an embrace of permissionless innovation can unlock this sort of entrepreneurial energy within the information technology sectors, it can also provide a shot in the arm to other sectors. The rest of the economy could certainly use such a boost since "the evidence of a real decline in business dynamism keeps stacking up."[74]

Recent studies "suggest that incentives for entrepreneurs to start new firms in the United States have diminished over time"[75] and that this is hurting job creation and productivity.[76] Two recent Brookings Institution studies by Ian Hathaway and Robert E. Litan also documented a decline in business dynamism in the American economy across a broad range of sectors—including a "precipitous drop since 2006 [that] is both noteworthy and disturbing"[77]— as well as the increased "aging" of businesses, with the share of older firms in the US economy increasing by 50 percent over the past two decades.[78]



Source: U.S. Census Bureau, BDS; authors' calculations.

Figure 1. Distribution of Total Firms by Age in Years (1978-2011).

Many different institutional factors affect business dynamism, especially the regulatory environment that new startups face. "If you look over time, the number of rules has just proliferated," says Litan. "The cumulative weight of regulation—federal, state and local—is probably the most important impediment to starting a business."[79]

Unfortunately, many current public policies "are rife with barriers to entrepreneurship, competition, innovation, and growth," notes Lindsey.[80]

As a result, "the regulatory environment in the United States has become less favorable to private-sector activity in recent years compared to other countries," a Mercatus Center report concluded.[81] This is especially true for new start-ups.[82] Even if it is the case that "established firms that have the experience and resources to deal with [regulatory burdens]," Litan notes, the cumulative effect of regulations ends up hampering innovation by new, smaller firms. [83]

The reason this is important is not just because "business dynamism is inherently disruptive," as Hathaway and Litan note, "but [that] it is also critical to long-run economic growth" since "a dynamic economy constantly forces labor and capital to be put to better uses."[84] Thus, because economists widely acknowledge that "young firms are known to play a central role in job creation,"[85] it is especially important that policymakers get their signals right.

Again, an embrace of permissionless innovation is the way out of this conundrum.

E. Operationalizing the Vision

Patience, flexibility, and forbearance are the key policy virtues that nurture an environment conducive to entrepreneurial creativity. As the FTC's Ohlhausen argues, it is "vital that government officials ... approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required."[86]

Beyond its importance as an aspirational vision, permissionless innovation can guide policy in concrete ways, especially regulatory policies. Possible reforms include regulatory streamlining[87] and flexibility requirements[88], "sunsetting" provisions,[89] better benefit-cost analysis,[90] and a greater reliance on potential non-regulatory remedies—education, empowerment, transparency, industry self-regulation, etc.—before resorting to preemptive controls on new forms of innovation. Relying on common law solutions is also preferable to top-down administrative controls.[91]

F. Conclusion: Reasons for Optimism

In sum, attitudes matter as much as institutional factors in understanding what drives innovation and long-term growth, and there are reasons for optimism if policymakers embrace permissionless innovation as their default policy disposition.

Pessimists who predict permanent productivity and growth slowdown shouldn't forget that "the rate of growth of productivity at the frontiers of knowledge is especially difficult to predict; and it is unwise to underestimate human ingenuity," as Federal Reserve Vice Chairman Stanley Fischer noted in a 2014 speech.[92] While "it is difficult to know exactly in which direction technological change will move and how significant it will be," Joel Mokyr reminds us that, "something can be learned from the past, and it tells us that such pessimism is mistaken. The future of technology is likely to be bright."[93] Contrary to the belief that all the "low-hanging fruit" has already been picked, Mokyr notes that "we can also plant new trees that will grow fruits that no one today can imagine."[94]

Getting the disposition right will be more important than ever with so many exciting—but potentially highly disruptive—technologies starting to emerge, including the "sharing economy;"[95] 3D printing; the "Internet of Things" and wearable technology;[96] digital medicine; virtual reality and augmented reality technologies; commercial drone services;[97] autonomous vehicles;[98] and various robotic technologies.[99]

Permissionless innovation can help spur the next great industrial revolution by unlocking amazing opportunities in these and other arenas, boosting long-term growth in the process.

APPENDIX 7: HOW WE ADAPT TO TECHNOLOGICAL CHANGE[100]

A. From Resistance to Resiliency

Citizen attitudes about these technologies will likely follow a cycle that has played out in countless other contexts. That cycle typically witnesses initial *resistance*, gradual *adaptation*, and then eventual *assimilation* of a new technology into society.[101] Some citizens will begin their relationship with these new technologies in a defensive crouch. In the extreme, if there is enough of a backlash, the initial resistance to these technologies might take the form of a full-blown "technopanic."[102]

Over time, however, citizens tend to learn how to adapt to new technologies or at least become more resilient in the face of new challenges posed by modern technological advances. Andrew Zolli and Ann Marie Healy, authors of *Resilience: Why Things Bounce Back*, define *resilience* as "the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances."[103] They continue:

> To improve your resilience is to enhance your ability to resist being pushed from your preferred valley, while expanding the range of alternatives that you can embrace if you need to. This is what researchers call *preserving adaptive capacity*—the ability to adapt to changed circumstances while fulfilling one's core purpose—and it's an essential skill in an age of unforeseeable disruption and volatility.[104]

Consequently, they note, “by encouraging adaptation, agility, cooperation, connectivity, and diversity, resilience-thinking can bring us to a different way of being in the world, and to a deeper engagement with it.”[105]

Those who propose more precautionary solutions to challenging social problems often ignore this uncanny ability of individuals and institutions to “bounce back” from technological disruptions and become more resilient in the process. Part of the reason precautionary thinking sometimes dominates discussions about emerging technologies is that many people hold a deep-seated pessimism about future developments and a belief that, with enough preemptive planning, they can anticipate and overcome any number of hypothetical worst-case scenarios. Consequently, their innate tendency not only to be pessimistic but also to want greater certainty about the future means that “the gloom-mongers have it easy,” notes author Dan Gardner.[106] “Their predictions are supported by our intuitive pessimism, so they *feel* right to us. And that conclusion is bolstered by our attraction to certainty.”[107] Clive Thompson, a contributor to *Wired* and the *New York Times Magazine*, also notes that “dystopian predictions are easy to generate” and “doomsaying is emotionally self-protective: if you complain that today’s technology is wrecking the culture, you can tell yourself you’re a gimlet-eyed critic who isn’t hoodwinked by high-tech trends and silly, popular activities like social networking. You seem like someone who has a richer, deeper appreciation for the past and who stands above the triviality of today’s life.”[108]

Luckily, as science reporter Joel Garreau reminds readers, “the good news is that end-of-the-world predictions have been around for a very long time, and none of them has yet borne fruit.”[109] Doomsayers have a bad track record because they typically ignore how “humans shape and adapt [technology] in entirely new directions.”[110] “Just because the problems are increasing doesn’t mean solutions might not also be increasing to match them,” Garreau correctly notes.[111]

In their 2001 “Response to Doom-and-Gloom Technofuturists,” John Seely Brown and Paul Duguid note that “technological and social systems shape each other. ... [They] are constantly forming and reforming new dynamic equilibriums with far-reaching implications.” “Social and technological systems do not develop independently,” they continue. Rather, “the two evolve together in complex feedback loops, wherein each drives, restrains, and accelerates change in the other.”[112]

This is how humans become more resilient and prosper, even in the face of sweeping technological change. Wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures while both developing new technologies and learning how to live with them.[113] Citizens should remain open to new forms of technological change not only because doing so provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve—and to learn from that change. More often than not, citizens find creative ways to adapt to technological change by using a variety of coping mechanisms, new norms, or other creative fixes. Although some things are lost in the process, something more is typically gained, including lessons about how to deal with subsequent disruptions.

CASE STUDY: THE RISE OF PUBLIC PHOTOGRAPHY

Consider the jarring impact that the rise of the camera and public photography had on American society in the late 1800s.[114] This case study has implications for the debate over wearable technologies. Plenty of critics existed, and many average citizens were probably outraged by the spread of cameras[115] because "for the first time photographs of people could be taken without their permission—perhaps even without their knowledge," notes Lawrence M. Friedman in his 2007 book, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*.[116]

In fact, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay "The Right to Privacy," decries the spread of public photography. The authors lament that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claim that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[117]

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

Although some limited legal responses were needed to address the most egregious misuses of cameras, for the most part the gradual evolution of social norms, public pressure, and other coping mechanisms combined to solve the "problem" of public photography. In much the same way IoT and wearable technology will likely see a similar combination of factors at work as individuals and society slowly adjust to the new technological realities of the time. The public will likely develop coping mechanisms to deal with the new realities of a world of wearable technologies and become more resilient in the process.

That being said, resiliency should not be equated with complacency or a "Just get over it!" attitude toward privacy and security issues. With time, it may very well be the case that people "get over" *some* of the anxieties they might hold today concerning these new technologies, but in the short run, IoT and wearable technologies will create serious social tensions that deserve serious responses.[118]

End Notes

[1] Adam Thierer, Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom (Arlington, VA: Mercatus Center at George Mason University, 2014).

[2] Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the Richmond Journal of Law and Technology 21, no. 6 (2015), http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.

3 Michael E. Porter and James E. Heppelmann, "How Smart, Connected Products Are Transforming Competition," Harvard Business Review, November 2014, https://hbr.org/ 2014/11/how-smart-connected-products-are-transforming-competition.

4 Emily Adler, "The 'Internet of Things' Will Soon Be a Truly Huge Market, Dwarfing All Other Consumer Electronics Categories," Business Insider, July 10, 2014, http://www.businessinsider.com/internet-of-things-will-soon-be-a-truly-huge-market-dwarfing-allother-consumer-electronics-categories-2014-7.

5 Gil Press, "Internet of Things by the Numbers: Market Estimates and Forecasts," Forbes, August 22, 2014, http://www.forbes.com/ sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts.

6 Michael Mandel, "Can the Internet of Everything Bring Back the High-Growth Economy?" (Policy Memo, Progressive Policy Institute, Washington, DC, September 2013), 9, http:// www.progressivepolicy.org/2013/09/can-the-internet-of-everything-bring-backthe-high-growth-economy. ("No one can predict the ultimate course of innovative technologies, but it appears that the Internet of Everything has the potential to help revive the high-growth economy.")

7 Adam Thierer, "Embracing a Culture of Permissionless Innovation" (Cato Online Forum, Cato Institute, Washington, DC, November 2014), http://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.

[8] Adam Thierer, "The Greatest of All Internet Laws Turns 15," Forbes, May 8, 2011, http://www.forbes.com/sites/adamthierer/2011/05/08/the-greatest-of-all-internet-laws-turns-15.

[9] Specifically, the Clinton framework stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry." It also argued that "governments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce." White House, "The Framework for Global Electronic Commerce" (July 1997), http://clinton4.nara.gov/WH/New/Commerce.

[10] Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," Forbes, February 12, 2012, http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remainthe-perfect-paradigm.

[11] As analysts at the Center for Data Innovation correctly argue, policymakers should only intervene to address specific, demonstrated harms. "Attempting to erect precautionary regulatory barriers for purely speculative concerns is not only unproductive, but it can discourage future beneficial applications of the Internet of Things," they say. See Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2014, http://www.datainnovation.org/2014/12/10-policy-principles-for-unlocking-the-potential-of-the-internet-of-things.

[12] The Fair Information Practice Principles (FIPPs) traditionally include (1) notice, (2) choice, (3) purpose specification, (4) use limitation, and (5) data minimization.

[13] Adam Thierer, "Some Initial Thoughts on the FTC Internet of Things Report," Technology Liberation Front, January 28, 2015, http:// techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report.

[14] Adam Thierer, "Striking a Sensible Balance on the Internet of Things and Privacy," Technology Liberation Front, January 16, 2015, http://techliberation.com/2015/01/16/striking-a-sensible-balance-on-the-internet-of-things-and-privacy. See also Adam Thierer, "Muddling Through: How We Learn to Cope with Technological Change," Medium, June 30, 2014, https://medium.com/tech-liberation/muddling-through-how-we-learn-to-cope-with-technological-change-6282d0d342a6.

[15] Adam Thierer, "Muddling Through: How We Learn to Cope with Technological Change," Medium, June 30, 2014, https://medium. com/tech-liberation/muddling-through-how-we-learn-to-cope-with-technological-change-6282d0d342a6.

[16] This section adapted from Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the Richmond Journal of Law and Technology 21, no. 6 (2015), http://mercatus.org/publication/internet-things-and-wearable-technology-address ing-privacy-and-security-concerns-without.

[17] Alex Hawkinson, "What Happens When the World Wakes Up," Medium (Sept. 23, 2014), https://medium.com/@ahawkinson/whathappens-when-the-world-wakes-up-c73a5c931c17.

[18] Timothy B. Lee, "Everything's Connected: How Tiny Computers Could Change the Way We Live," Vox (Aug. 13, 2014), http://www. vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live.

[19] Kevin Ashton, "That "Internet of Things" Thing," RFID Journal (June 22, 2009), http://www.rfidjournal.com/articles/view?4986.

[20] Ibid.

[21] Amy Collins, Adam J. Fleisher, D. Reed Freeman Jr., and Alistair Maughan, "The Internet of Things Part 1: Brave New World," Client Alert (Morrison Foerster), March 18, 2014, 1, http://www.jdsupra.com/legalnews/the-internet-of-things-part-1-brave-new-23154.

[22] See Patrick Thibodeau, "Explained: The ABCs of the Internet of Things," Computerworld, May 6, 2014, http://www.computerworld. com/s/article/9248058/Explained_ The_ABCs_ of_the_Internet_of_Things_.

[23] Steve Lohr, "A Messenger for the Internet of Things," N.Y. Times Bits, April 25, 2013, http://bits.blogs.nytimes.com/2013/04/25/amessenger-for-the-internet-of-things.

[24] Consumer Electronics Association, Comment to the Federal Trade Commission on Internet of Things, Project No. P135405 (June 10, 2013), 7.

[25] Ibid.

[26] This section compiled with the assistance of Andrea Castillo, Program Manager of the Technology Policy Program at the Mercatus Center.

[27] Dave Evans, "Thanks to IoE, the Next Decade Looks Positively 'Nutty,'" Cisco Blog, February 12, 2013, http://blogs.cisco.com/ioe/ thanks-to-ioe-the-next-decade-looks-positively-nutty.

[28] "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020" (Press Release, ABI Research, May 9, 2013), https://www.abiresearch.com/press/ more-than-30-billion-devices-will-wirelessly-conne.

[29] Antony Savvas, "Internet of Things Market Will Be Worth Almost $9 Trillion," CNME, October 6, 2013, http://www.cnmeonline. com/news/internet-of-things-market-will-be-worth-almost-9-trillion.

[30] "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015" (Press Release, Gartner, 2014), http://www.gartner.com/newsroom/id/2905717.

[31] Matt Asay, "The Internet of Things Will Need Millions of Developers by 2020," ReadWrite, June 27, 2014, http://readwrite. com/2014/06/27/internet-of-things-developers-jobs-opportunity.

[32] John Greenough, "The Enterprise Internet of Things Report: Forecasts, Industry Trends, Advantages, and Barriers for the Top IoT Sector," Business Insider, 2014, https://intelligence.businessinsider.com/the-enterprise-internet-of-things-report-forecasts-industrytrends-advantages-and-barriers-for-the-top-iot-sector-2014-11.

[33] Harbor Research, Smart Systems and the Internet of Things Forecast (2013), http://harborresearch.com/wp-content/uploads/2013/08/Harbor-Research_2013-Forecast-Report_Prospectus.pdf.

[34] "The Connected Life" (Press Release, Machina Research, 2014), https://machinaresearch. com/static/media/uploads/machina_research_press_release_-_ce_report_-_2014_07_28.pdf.

[35] Smart Electric Meters, "Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts," Navigant Research, November 2013, http://www.navigantresearch.com/research/smart-meters.

[36] "Emerging Technologies: Big Data in the Connected Car" (Press Release, IHS Automotive, November 2013), http://press.ihs.com/ press-release/country-industry-forecasting/big-data-drivers-seat-connected-car-technological-advance.

[37] Mareca Hatler, Darryl Gurganious, and Charlie Chi, "Smart Wireless Lighting," ON World, 2013, http://onworld.com/smartlighting.

[38] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," McKinsey, May 2013, http://www.mckinsey.com/ ~/media/ McKinsey/dot-

com/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_tech-nologies_Full_report_May2013.ashx.

[39] Antony Savvas, "Internet of Things Market Will Be Worth Almost $9 Trillion," CNME, October 6, 2013, http://www.cnmeonline. com/news/internet-of-things-market-will-be-worth-almost-9-trillion.

[40] Joseph Bradley, Joel Barbier, and Doug Handler, "Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion," CISCO, 2013, http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[41] John Greenough, "The Enterprise Internet of Things Report: Forecasts, Industry Trends, Advantages, and Barriers for the Top IoT Sector," Business Insider, 2014, https://intelligence.businessinsider.com/the-enterprise-internet-of-things-report-forecasts-industrytrends-advantages-and-barriers-for-the-top-iot-sector-2014-11.

[42] "Winning with the Industrial Internet of Things" (Positioning Paper, Accenture, 2015), http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDF.

[43] Peter C. Evans and Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, 2012, http://www.ge.com/docs/chapters/ Industrial_ Internet.pdf.

[44] Ravi Shanker et al., "Driverless Cars: Self-Driving the New Auto Industry Paradigm" (Blue Paper, Morgan Stanley, November 6, 2013), http://www.wisburg.com/wp-content/uploads/2014/09/%ef%bc%88109-pages-2014%ef%bc%89morgan-stanley-blue-paperautonomous-cars%ef%bc%9a-self-driving-the-new-auto-industry-paradigm.pdf.

[45] This section is adapted from Adam Thierer, "A Nonpartisan Policy Vision for the Internet of Things," Technology Liberation Front, December 11, 2014, http://techliberation.com/2014/12/11/a-nonpartisan-policy-vision-for-the-internet-of-things.

[46]. Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," Forbes, February 12, 2012, http://www.forbes.com/sites/ adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remainthe-perfect-paradigm.

[47] This section is adapted from Adam Thierer, "Some Initial Thoughts on the FTC Internet of Things Report," Technology Liberation Front, January 28, 2015, http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report.

[48] This section is adapted from Adam Thierer, "Embracing a Culture of Permissionless Innovation" (Cato Policy Forum, Cato Institute, Washington, DC, November 2014), http://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.

[49] Joel Mokyr, Lever of Riches: Technological Creativity and Economic Progress (New York: Oxford University Press, 1990), 8–9.

[50] For a listing and discussion of these and other factors, see Robert D. Atkinson, "Understanding the U.S. National Innovation System," Information Technology and Innovation Foundation, June 2014, http://www.itif.org/publications/understanding-us-nationalinnovation-system.

[51] Michael Nelson, "Six Myths of Innovation Policy," The European Institute, Washington, DC, July 2013, http://www.europeaninstitute. org/EA-July-2013/perspectives-six-myths-of-innovation-policy.html. ("On Capitol Hill and in Brussels, there seems to be a belief that if only governments adopt the right tax policies, adequately fund R&D, enforce patents and copyrights, and support manufacturing, innovative, then start-ups will pop up everywhere and supercharge economic growth. Unfortunately, that misses an underlying problem: In

many parts of the U.S. and Europe, innovation is not really welcome. It is misunderstood and even feared.")

[52] White House, "Notice of Request for Information: Strategy for American Innovation," Federal Register, July 29, 2014, https://www. federalregister.gov/articles/2014/07/29/2014-17761/strategy-for-american-innovation.

[53] Ibid.

[54] Donald J. Boudreaux, "Deirdre McCloskey and Economists' Ideas about Ideas,'" Online Library of Liberty, July 2014, http://oll. libertyfund.org/pages/mccloskey.

[55] Deirdre N. McCloskey, The Bourgeois Virtues: Ethics for an Age of Commerce (Chicago: University of Chicago Press, 2006).

[56] Deirdre McCloskey, "Bourgeois Dignity: A Revolution in Rhetoric" (Cato Unbound, Cato Institute, Washington, DC, October 4, 2010), http://www.cato-unbound.org/2010/10/04/deirdre-mccloskey/bourgeois-dignity-revolution-rhetoric.

[57] Randall Holcombe, "Entrepreneurship and Economic Growth," The Quarterly Journal of Austrian Economics 1, no. 2 (Summer 1998):

[58] http://mises.org/journals/qjae/pdf/qjae1_2_3.pdf, ("When entrepreneurship is seen as the engine of growth, the emphasis shifts toward the creation of an environment within which opportunities for entrepreneurial activity are created, and successful entrepreneurship is rewarded.")

[59] Mokyr, Lever of Riches, 182.

[60] Mokyr, Lever of Riches, 12 ("Economic and social institutions have to encourage potential innovators by presenting them with the right incentive structure."); Bret Swanson, "More disruption, please," TechPolicyDaily, August 20, 2014, http://www.techpolicydaily. com/technology/disruption-please/#sthash.PVUNga9N.dpuf ("To reignite economic growth, we need a broad commitment to an open economy and robust entrepreneurship.").

[61] Thierer, Permissionless Innovation.

[62] Ibid., vii. See also Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," Minnesota Journal of Law, Science and Technology 14 (2013): 309–86, http://conservancy.umn.edu/handle/144225.

[63] Indur M. Goklany, The Precautionary Principle: A Critical Appraisal of Environmental Risk Assessment (Washington, DC: Cato Institute, 2001), 3.

[63] Joshua C. Hall, John Pulito, and Benjamin J. VanMetre, "Freedom and Entrepreneurship: New Evidence from the 50 States" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, April 17, 2012), http://mercatus.org/publication/freedom-and-entrepreneurship-new-evidence-50-states ("There is a positive and statistically significant relationship between the level of economic freedom in a country and that country's total entrepreneurial activity.")

[64] See Bret Swanson, "The Exponential Internet," Business Horizon Quarterly (Spring 2014): 40–47, http://www.uschamberfoundation.org/sites/default/files/article/foundation/BHQ-Spring 12-Issue3-SwansonTheExponentialInternet.pdf.

[65] Ibid., 46. ("The entrepreneurship and investment that has sustained such fast growth for so long is due, in substantial part, to light-touch government policies (at least compared to other industries. ... There have been mistakes, but for the most part, scientists, entrepreneurs, and big investors have been allowed to build new things, try new products, challenge the status quo, cooperate, and compete. They have also been allowed to fail.") See also Bret Swanson, "Long Live the Risk Takers," Business Horizon Quarterly 8 (2013): 30, http://www.uschamberfoundation.org/bhq/long-live-risk-takers ("Failure is a core competency of capitalism and a key component of resilience. Wealth is about creating new

ideas. New ideas can only emerge through experiments of science, technology, and enterprise, all of which must be capable of failure in order to generate newness. Failure flushes away bad ideas and points us toward good ones. The failures may at times harm individuals and waste resources—people lose jobs and investments can be lost. The larger effect, however, is to lift the economy to a higher plane of knowledge, efficiency, and resilience.")

[66] White House, "The Framework for Global Electronic Commerce," July 1997, http://clinton4.nara.gov/WH/New/Commerce.

[67] Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," Forbes, February 12, 2012, http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remainthe-perfect-paradigm.

[68] White House, "Framework for Global Electronic Commerce." (The document added that, "parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. . . . Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.")

[69] Ibid.

[70] Maureen K. Ohlhausen, "The Internet of Things and the FTC: Does Innovation Require Intervention?" Remarks before the US Chamber of Commerce, Washington, DC, October 18, 2013, http://www.ftc.gov/speeches/ohlhausen/131008internetthingsremarks.pdf.

[71] A study commissioned by the Direct Marketing Association, John Deighton of Harvard Business School and Peter Johnson of Columbia University found that data-driven marketing added $156 billion in revenue to the US economy and fueled more than 675,000 jobs in 2012. See also John Deighton and Peter A. Johnson, "The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy," Data-Driven Marketing Institute, New York, NY, 2013, http://ddminstitute.thedma.org/#valueofdata. Major reports from economic consultancies Gartner and McKinsey Global Institute have also documented significant consumer benefits from "big data" across multiple sectors. See Gartner, "Gartner Says Big Data Will Drive $28 Billion of IT Spending in 2012," October 17, 2012, http://www.gartner.com/newsroom/id/2200815; James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey, May 2011, 97-106, http://www.mckinsey.com/insights/business_technology/ big_data_ the_next_frontier_for_innovation.

[72] Lindsey, "Why Growth Is Getting Harder," 14.

[73] Harold Furchtgott-Roth and Jeffrey Li, "The Contribution of the Information, Communications, and Technology Sector to the Growth of U.S. Economy: 1997–2007" (Research Paper, Center for the Economics of the Internet, Hudson Institute, Washington, DC, August 2014), http://hudson.org/content/researchattachments/attachment/ 1425/ m0810_2.pdf ("For the years 1997–2002, we find the sector contributed 19% of measurable economic gross output growth, or more than 582 billion 2013 dollars. For the period 2002-2007, we find the sector contributed 9.3% of gross output growth, or more than 340 billion 2013 dollars.")

[74] Richard Florida, "The Troubling Decline of American Business Dynamism," The Atlantic City Lab, July 31, 2014, http://www.citylab. com/work/2014/07/the-troubling-decline-of-american-business-dynamism/375353.

[75] Ryan Decker, John Haltiwanger, Ron Jarmin, and Javier Miranda, "The Role of Entrepreneurship in US Job Creation and Economic Dynamism," Journal of Economic Perspectives 28, no. 3 (Summer 2014): 4, http://pubs.aeaweb.org/doi/pdfplus/ 10.1257 /jep.28.3.3.

[76] Robert J. Samuelson, "Where have all the entrepreneurs gone?" Washington Post, August 6, 2014, http://www.washingtonpost. com/opinions/robert-samuelson-where-have-all-the-entrepreneurs-gone/2014/08/06/e01e7246-1d7c-11e4-82f9-2cd6fa8da5c4_story.html.

[77] Ian Hathaway and Robert E. Litan, "Declining Business Dynamism in the United States: A Look at States and Metros" (Economic Studies at Brookings, Brookings Institution, Washington, DC, May 2014), http://www.brookings.edu/research/papers/2014/05/declining-business-dynamism-litan.

[78] Ian Hathaway and Robert E. Litan, "The Other Aging of America: The Increasing Dominance of Older Firms" (Economic Studies at Brookings, Brookings Institution, Washington, DC, July 2014), http://www.brookings.edu/research/papers/2014/07/aging-americaincreasing-dominance-older-firms-litan.

[79] Quoted in Rick Newman, "What Obama Gets Wrong about Corporate America," Yahoo Finance, August 4, 2014, http://finance. yahoo.com/news/what-obama-gets-wrong-about-corporate-america-200338595.html.

[80] Lindsey, "Why Growth Is Getting Harder," 18.

[81] See also Steven Globerman and George Georgopoulos, "Regulation and the International Competeveness of the U.S. Economy" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, September 18, 2012), 4, http://mercatus.org/ publication/regulation-and-international-competitiveness-us-economy.

[82] Jason J. Fichtner and Jakina R. Debnam, "Reducing Debt and Other Measures for Improving U.S. Competitiveness" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 13, 2012), http://mercatus.org/publication/ reducing-debt-and-other-measures-improving-us-competitiveness ("Regulations have been historically biased toward existing technologies and increasing regulatory burdens on new entrants to a sector. This negatively impacts growth, and increases prices for consumers.")

[83] Quoted in Robert J. Samuelson, "Where Have All the Entrepreneurs Gone?" Washington Post, August 6, 2014, http://www. washingtonpost.com/opinions/robert-samuelson-where-have-all-the-entrepreneurs-gone/2014/08/06/e01e7246-1d7c-11e4-82f9-2cd6fa8da5c4_story.html.

[84] Hathaway and Litan, "Declining Business Dynamism," 1.

[85] Chiara Criscuolo, Peter N. Gal, and Carlo Menon, "DynEmp: New Cross-Country Evidence on the Role of Young Firms in Job Creation, Growth, and Innovation," Vox, May 26, 2014, http://www.voxeu.org/article/dynemp-new-evidence-young-firms-role-economy.

[86] Maureen K. Ohlhausen, "The Internet of Things and the FTC: Does Innovation Require Intervention?," Remarks before the US Chamber of Commerce, Washington, DC, October 18, 2013, http://www.ftc.gov/speeches/ohlhausen/131008internetthingsremarks.pdf.

[87] Sherzod Abdukadirov, "Evaluating Regulatory Reforms: Lessons for Future Reforms" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, May 29, 2014), http://mercatus.org/publication/evaluating-regulatory-reforms-lessons-future-reforms; Joshua C. Hall and Michael Williams, "A Process for Cleaning Up Federal Regulations" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, December 20, 2012), http://mercatus.org/publication/process-cleaning-federal-regulations.

[88] Richard Epstein, "Can Technological Innovation Survive Government Regulation?" Harvard Journal of Law and Public Policy 36, no. 1 (Winter 2013), http://www.harvard-jlpp.com/wp-content/uploads/2013/01/36_1_087_Epstein_Tech.pdf ("What is at stake in this area is nothing less than the question of how to preserve technical innovation in the face of wall-to-wall regulation. The prognosis is grim. Unless we reform agencies like the FDA and their procedures and operations, this country will suffer from a long-term drag on innovation that could, if the trend is not abated, lead to long-term mediocrity, as inventors and scientists flee our shores for friendlier environments. The pace of regulation is one of the central issues of our time.")

[89] Adam Thierer, "Sunsetting Technology Regulation: Applying Moore's Law to Washington," Forbes, March 25, 2012, http://www. forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington; Patrick McLaughlin, "A Solution to the Old Rules vs. New Tech Problem," The Hill, July 8, 2014, http://mercatus.org/expert_commentary/solution-oldrules-vs-new-tech-problem.

[90] See Susan E. Dudley and Jerry Brito, Regulation: A Primer, 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2012).

[91] See Thierer, Permissionless Innovation, 74-78.

[92] Stanley Fischer, "The Great Recession—Moving Ahead," a Conference Sponsored by the Swedish Ministry of Finance, Stockholm, Sweden, August 11, 2014, http://www. federalreserve.gov/newsevents/speech/fischer20140811a.htm.

[93] Joel Mokyr, "The Next Age of Invention," City Journal, Winter 2014, http://www.city-journal.org/2014/24_1_invention.html.

[94] Ibid.

[95] Adam Thierer, "The Debate over the Sharing Economy: Talking Points & Recommended Reading," Technology Liberation Front, September 26, 2014, http://techliberation.com/ 2014/09/26/the-debate-over-the-sharing-economy-talking-points-recommendedreading.

[96] Adam Thierer, "Slide Presentation: Policy Issues Surrounding the Internet of Things & Wearable Technology," Technology Liberation Front, September 12, 2014, http://techliberation.com/2014/09/12/slide-presentation-policy-issues-surrounding-the-internet-ofthings-wearable-technology.

[97] Jerry Brito, Eli Dourado, and Adam Thierer, "Federal Aviation Administration: Unmanned Aircraft System Test Site Program Docket No: FAA-2013-0061" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, April 23, 2013), http://mercatus.org/publication/federal-aviation-administration-unmanned-aircraft-system-test-site-program; Eli Dourado, "The Next Internet-Like Platform for Innovation? Airspace. (Think Drones)," Wired, April 23, 2013, http://www.wired.com/opinion/2013/04/then-internet-now-airspace-dont-stifle-innovation-on-the-next-great-platform; Adam Thierer, "Filing to FAA on Drones & 'Model Aircraft'," Technology Liberation Front, September 23, 2014, http://techliberation.com/2014/09/23/filing-to-faa-on-drones-model-aircraft.

[98] Adam Thierer and Ryan Hagemann, "Removing Roadblocks to Intelligent Vehicles and Driverless Cars" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, September 17, 2014), http://mercatus.org/publication/removing-roadblocks-intelligent-vehicles-and-driverless-cars.

[99] Adam Thierer, "Problems with Precautionary Principle-Minded Tech Regulation & a Federal Robotics Commission," Medium, September 22, 2014, https://medium.com/@ AdamThierer/problems-with-precautionary-principle-minded-tech-regulation-a-federal-robotics-commission-c71f6f20d8bd.

[100] This section adapted from Adam Thierer, “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation” (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the Richmond Journal of Law and Technology 21, no. 6 (2015), http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.

[101] See Adam Thierer, “Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle,” Minn. J. L. Sci. & Tech. 14 (2013): 309.

[102] Ibid., 53–60.

[103] Andrew Zolli and Ann Marie Healy, Resilience: Why Things Bounce Back (New York: Simon & Schuster, 2012).

[104] Ibid., 7–8.

[105] Ibid., 16.

[106] Dan Gardner, Future Babble: Why Pundits Are Hedgehogs and Foxes Know Best (New York: Plume, 2012), 140–1.

[107] John Seely Brown and Paul Duguid, “Response to Bill Joy and the Doom-and-Gloom Technofuturists,” in Albert H. Teich, Stephen D. Nelson, Celia McEnaney, and Stephen J. Lita, editors, AAAS Science and Technology Policy Yearbook (Washington, DC: American Association for the Advancement of Science, 2001), 79.

[108] Clive Thompson, Smarter Than You Think: How Technology Is Changing Our Minds for the Better (New York: Penguin, 2014), 283.

[109] Joel Garreau, Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies—and What It Means to Be Human (New York: Broadway Books, 2006), 148.

[110] Ibid., 95.

[111] Ibid., 154.

[112] Brown and Duguid, supra note 106, 79, 82, 83.

[113] Thierer, Permissionless Innovation, viii.

[114] This section was condensed from Thierer, “Technopanics.”

[115] For a discussion of the anxieties caused by photography during this time, see Robert E. Mensel, Kodakers Lying in Wait: Amateur Photography and the Right of Privacy in New York, 1885–1915, Amer. Quar. 43 (March 1991): 24.

[116] Lawrence M. Friedman, Guarding Life’s Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy (Palo Alto, CA: Stanford University Press, 2007), 214.

[117] Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” Harv. L. Rev. 4 (1890): 193, 195.

[118] Adam Thierer, “Can We Adapt to the Internet of Things?,” Privacy Perspectives, June 19, 2013, https://www.privacyassociation. org/privacy_perspectives/post/can_we_ adapt_ to_ the_internet_of_things.

INDEX