INTERNET OF THINGS

HEARING

BEFORE THE

SUBCOMMITTEE ON
COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 29, 2015

Serial No. 114–38

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

95–686 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

DARRELL E. ISSA, California, *Chairman*
DOUG COLLINS, Georgia, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
RON DeSANTIS, Florida
MIMI WALTERS, California

JERROLD NADLER, New York
JUDY CHU, California
TED DEUTCH, Florida
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia

JOE KEELEY, *Chief Counsel*
JASON EVERETT, *Minority Counsel*

CONTENTS

JULY 29, 2015

INTERNET OF THINGS

WEDNESDAY, JULY 29, 2015

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 10:05 a.m., in room 2141, Rayburn House Office Building, the Honorable Darrell E. Issa (Chairman of the Subcommittee) presiding.

Present: Representatives Issa, Goodlatte, Chabot, Poe, Marino, Walters, Nadler, Chu, Deutch, DelBene, Jeffries, Cohen, and Johnson.

Staff Present: (Majority) Vishal Amin, Senior Counsel; Eric Bagwell, Clerk; and (Minority) Jason Everett, Minority Counsel.

Mr. ISSA. The Subcommittee on Courts, Intellectual Property, and the Internet will come to order. Without objection, the Chair is authorized to declare a recess of the Subcommittee at any time.

Today we welcome everyone here for a hearing on the Internet of Things. Throughout its short history, the Internet has been transformative and a powerful tool. It has shaped communication commerce worldwide. Technology, too, has proven to advance at rates that only Moore's law describes with a doubling of capacity so quickly that about the time you run out of your short warranty, you in fact have a product that can out perform the one on your desk.

But the Internet of Things, which broadly refers to a network connected real world items able to exchange data with each other and across existing network infrastructure is a newer portion of what now becomes the future of our lives and our communication in the 21st Century.

It is estimated by 2020 there will be 25 billion connected things, and without a doubt, before we reach 2020, I will be wrong, and there will be more connected things. By inventing devices with electronic sensors, software capable of connecting a market, we in fact have smart devices. Those smarter devices today already include, if you choose, every light switch in your home, the watch you wear, and products throughout the home, whether they be speakers to hear from or in fact sensors to control climate down to a portion of every room.

Data-driven technology is also improving the way we understand healthcare and the introduction of new health monitoring systems can in fact prevent, detect, and treat today any number of afflictions. A generation ago, the insulin pump was an amazing product, but it wasn't a true demand pump, it wasn't connected to your physician, it wasn't in fact sensing other environments. Today, it not only could but it soon will.

At the same time, as we talk about your home, your lighting, your messaging, your voice, and of course, your health and your actual biological function, issues like privacy and data security for these interoperable technologies become, not just something to talk about, but an area in which we in Congress play a large and potentially destructive role if we're not careful in the development of these technologies.

Every day in America somewhere someone is being hacked and somewhere someone is finding out that their personally identifiable information has been compromised. Too often it in fact is the government who we hear it from, the government who controls, if you will, whether or not you can further secure your Internet of Things products or not.

A generation ago I stood with one of our witnesses at a time in which a Member of Congress, a former FBI agent was trying to prevent 256 encryption. He was doing so because the FBI needed to be able to quickly crack the bad guys' transmissions. It had needed to be able to unbundle a floppy disk information in a matter of seconds if they were going to deter organized crime.

Unfortunately, it meant that hackers were taking Microsoft's operating system and quickly duplicating it and denying them millions or billions of dollars. It took a number of years for Congress to realize that that artificial control was not only circumventable by exporting their software to other countries and reimporting it, but it was ludicrous because the bad guys were not going to limit their protection to 256 bits.

Unlicensed spectrum within the Internet of Things is going to be talked about again and again today. I hope my witnesses will feel free to talk about the benefits of greater spectrum for the Internet of Things. I would remind all panelists, however, that the FCC is not within our primary jurisdiction, but to unbundle these and other parts of the Internet of Things will take a coordination between Committees that do control spectrum, those of us who control a great deal of the privacy requirements, and of course, the overseeing of what government allows.

In January, the Federal Trade Commission released a report that followed months of stakeholder roundtables focused on data privacy and security. The report made a broad nonbinding recommendation about how companies should address these issues from the onset and laid the groundwork for future FTC involvement in the Internet of Things.

When Congresswoman DelBene and I launched the congressional caucus on the Internet of Things in January, the first questions we received were usually what is the Internet of Things? And why does Congress care?

To a great extent, we have laid out a number of those even in my opening statement today, but I would be remiss if I didn't say

that the Federal Trade Commission is an agency that has been enforcing breaches in security while in fact until recently providing little guidance. This is yet another example of where we in fact can come in with the heavy hand of government but seldom with a safe haven, and that's an area in which the Internet of Things caucus and this Committee have an obligation to ensure that we do both.

So today we look forward to a hearing which stakeholders in the Internet of Things marketplace and further opportunities to deal with the challenges that Congress brings and those in which we can bring relief.

Thank you. And I look forward to our witnesses, and I now recognize the Ranking Member, the gentleman from New York, Mr. Nadler, for his opening statement.

Mr. NADLER. Thank you, Mr. Chairman. The Internet of Things is the next revolution in our increasingly wired world. Everything from household appliances to transportation systems can harness the power of the Internet to increase productivity, efficiency, and consumer choice. This technology holds great promise for consumers, businesses, and governments alike, but we must also consider the potential threats to security and privacy that are inherent in system relying on wireless connection and massive data collection as its lifeblood.

Today's hearing is an opportunity to examine both the benefits and the risks that the Internet of Things presents. The Internet of Things has experienced explosive growth in recent years. By some estimates, there are already 25 billion connected devices today. By 2020, in 5 short years, there may be as many as 50 billion.

We're already seeing many innovative uses of the Internet of Things across various industries as well as the potential risks that this technology may hold. For example, according to one study, by 2020, up to 90 percent of consumer cars may have an Internet connection, up from less than 10 percent in 2013. With this technology, drivers can monitor whether their car needs maintenance, the safety of their driving, and even the fuel efficiency of various routes.

But these features also leave their cars vulnerable to a cyber attack. As the New York Times described last week, researchers were able to track Internet-enabled cars' location, determine their speed, turn on and off their blinkers from afar, turn on and off their blinkers, lights, windshield wipers, and radios, interfere with navigation devices, and in some cases, control their brakes and steering.

As more and more vehicles use Internet technology, it is vital that automakers install strict security features to ward off potential attacks.

Similarly, so called smart cities are incorporating Internet of Things into their transportation energy and even waste management systems to increase efficiency. For example, traffic lights can be timed to maximize traffic flow and ease congestion in realtime. Street lamps can conserve energy by dimming when sensors tell them that no one is around, and garbage cans can signal when trash ought to be collected. Imagine the garbage can talking to the sanitation department.

Such technology has the potential to revolutionize students that build infrastructure. I don't want to know what they say. But un-

less cities integrate strong security measures when deploying this technology, their infrastructure could be vulnerable to attack by hackers looking to do mischief or terrorists seeking to bring a whole city to a standstill.

In addition to security concerns, the Internet of Things also raises a host of privacy implications, particularly with respect to consumer devices. There is no doubt that Internet-enabled technology can improve a consumer's experience in ways large and small. To maximize energy efficiency, your nest thermostat can be controlled remotely and even adjust temperatures on its own once it learns your patterns.

Amazon has introduced a Dash button which will allow customers to press a button and automatically reorder certain household supplies. But what do these companies do with the massive amounts of data they collect about their customers? What sort of notice do they provide to consumers about their privacy policies, and what choice do consumers have about how their information is used? And how will companies protect their sensitive information from being compromised in a cyber attack? These are all questions that must be considered as this technology continues to expand its reach.

For another example, millions of Americans wear devices that track their physical activity and other health indicators. At least one insurance company is offering its customers a discount if they wear such a device and demonstrate a healthy lifestyle, but beyond encouraging healthier behavior by their customers, it is not clear how else insurance companies may seek to use this personal information in the future. Will it be sold for marketing purposes? Will it be used in a discriminatory manner to determine the use of suitability for credit or employment?

In its examination of these important questions, the Federal Trade Commission made a number of important recommendations that we must consider. It suggested that companies build security into their devices at the outset rather than as an afterthought. It also recommended that they monitor connected devices throughout their expected lifecycle to provide security patches where possible to cover known risks.

In addition, the FTC urged companies to protect consumers' privacy by engaging in data minimization as well as providing notice in choices to consumers as to how their data may be used. Although the FTC did not make any specific legislative recommendations, we should consider whether congressional action is appropriate at this time to address security and privacy concerns. If so, should we seek solutions to these concerns that are specific to the Internet of Things or should they be addressed through broader legislation on these topics?

The Internet of Things has already led to important technological breakthroughs, and as it expands its reach, it has the potential to spur tremendous innovation. Our challenge is to find the proper balance between promoting this innovation and ensuring that our security and our privacy are protected as this valuable technology continues to grow.

I look forward to hearing from our witnesses about how to address these challenges, and I yield back the balance of my time.

Mr. ISSA. Thank you, Mr. Nadler.

I now recognize the gentleman from Virginia, the Chairman of the full Committee, Mr. Goodlatte for his opening statement.

Mr. GOODLATTE. Thank you, Mr. Chairman. Today we're here to learn more about the Internet of Things. I think this technology has the ability to not only improve the more mundane aspects of our everyday lives but transform the healthcare, transportation, and information technology industries.

This new area of technology is of particular interest to the Judiciary Committee considering our longstanding jurisdiction when it comes to issues pertaining to intellectual property, privacy, security, cloud computing, and digital trade.

The Internet of Things refers to machines containing sensors that connect and transmit data to other connected devices and the Internet. Dramatic growth in cloud computing over the past several years has helped enable this technology to reach its full potential. Without the ability for data from an Internet of Things device to be analyzed in realtime, the data itself would serve little value.

The ability to access this information through mobile apps or even our cars, makes these Internet of Things devices a key tool to finding creative solutions for many of the problems of daily life in the 21st Century. Smart agriculture will help us to grow more food and prevent waste. Smart transportation will help prevent traffic jams but can also be used to monitor road conditions and structural components of bridges and overpasses to detect problems immediately.

New wearables not only monitor the number of steps we take but can also include sensors that can catch and alert us to a potential medical emergency before it actually becomes one. As this Committee continues to study this new technology, it is important for us to keep in mind the full scope of the Internet of Things and be cognizant of its effects on public policy today and in the future.

In particular, we need to examine the privacy and security implications of this technology and look into the security and privacy measures industry is building now and the measures they intend to implement as open standards are developed.

I'm hopeful that this new technology will help fuel the engine of American innovation, prosperity, and creativity. I think we have a fantastic panel assembled today. I know all of the witnesses, and I look forward to hearing from them about this exciting new area of technology.

Thank you, Mr. Chairman.

Mr. ISSA. Thank you, Mr. Chairman.

And now on behalf of the Ranking Member, the gentlelady from Washington's First District, Ms. DelBene, will make a short opening statement.

Ms. DELBENE. Thank you. I want to thank my co-chair on the Internet of Things caucus and our Chairman, as well as the Ranking Member for calling this hearing on this important subject. When we examine the way that Internet-connected products and sensors are being used and what's called the Internet of Things from home appliances to personal wearables, it might be easy to conclude that the promise of the Internet of Things is limited only by American ingenuity, but we have an emerging set of challenges

and opportunities to address for both innovators and for consumers.

To start, we need to make sure that we update existing laws to reflect the way the world works today and where we are headed in the future. That means, for example, updating the Electronic Communications Privacy Act to ensure that data on a server is protected by the same warrant standard as a document in a file cabinet. For the multi-billion dollar Internet of Things economy to be successful, we need to be responsible stewards of policy.

For example, consumers must feel they can trust their devices will be secure and private, not vulnerable to hacking or spying. Devices must be able to talk to each other, and that means forging a path to adoption of uniform preferably international standards. Regulatory agencies must find ways to strike the right balance between encouraging innovation and firmly upholding their duty to protect the public health and safety, particularly in the realm of connected cars.

And as all these devices collect unprecedented amounts of data, they hold great promise for things like health research, but we must work with stakeholders to create a privacy landscape that Internet of Things users can understand that provides individuals with control over their own data.

Again, I want to thank the Chairman and the Ranking Member for calling today's important hearing and setting the stage for what I hope will be a productive and informative series of hearings on the role that Congress and our Committee can play and create an environment where Internet of Things innovation can prosper and consumer protection is at the forefront.

Thank you, Mr. Chair, and I yield back.

Mr. ISSA. I thank you, and thank for your leadership on this issue.

It is now my pleasure to introduce our distinguished panel. The witnesses' written statements have been entered into the record and will be placed in their entirety, and I'd ask witnesses to summarize in about 5 minutes their statements so we can leave time for lots of questions.

But before I introduce the witnesses formally, pursuant to the Committee rules, I'd ask that all witnesses stand to take the oath, customarily raising your right hand.

Do you solemnly swear or affirm that the testimony you're about to give will be the truth, the whole truth, and nothing but the truth.

Please be seated. Let the record reflect that all witnesses answered in the affirmative.

Today, our witnesses include Mr. Gary Shapiro, President and CEO of the Consumer Electronics Association; Mr. Dean Garfield, President and CEO of the Information Technology Industry Council; Mr. Mitch Bainwol, President and CEO of the Alliance of Automobile Manufacturers; and Mr. Morgan Reed, Executive Director of ACT|The App Association

Before I go down the row for the witnesses, I have to take a little bit of a personal privilege. The other three know it. Mr. Shapiro and I go back a long time. We were there at the birth of the Modern Consumer Electronics Association, and I once worked for him

on an unpaid, highly compensated, but unpaid position as the Chairman. So if today I rough him up, remember get backs, it takes awhile.

And with that, Mr. Shapiro.

TESTIMONY OF GARY SHAPIRO, PRESIDENT AND CEO, CONSUMER ELECTRONICS ASSOCIATION

Mr. SHAPIRO. Thank you, Chairman Issa. This is indeed a historic moment in my life because I've been referring to you as boss for 25 years, and you, as Chairman, oversaw a good portion of our freedom and our growth. And thank you, Ranking Member Nadler, Chairman Goodlatte, and other Members as well.

The Consumer Electronics Association represents 2,000 technology companies, and we own and produce the CES, which is held each January in Las Vegas, and is the world's largest innovation event. The Internet of Things is a big part of the CES now. In fact, it's so big that some 900 of our 3,600 exhibiters had Internet of Things related products at our recent show.

And the Internet of Things, you should know, exists because of smart phones. Over a billion smart phones have been sold, and they contain something called MEMS, Micro-Electro Mechanical Systems. These are tiny little devices that actually move, and they measure all sorts of things like pressure, temperature, location, movement, and other valuable information.

And because of the billions of sales of these devices in phones, now they cost just pennies apiece, and very smart innovators are putting them together in very clever ways, and what they're doing is creating new services rather rapidly. They use very little energy, and they hook up to the Internet, and that is what the Internet of Things is based on.

From garden soil moisture monitors to baby monitors, from wearables like smart watches and fitness trackers to connected thermostats and lights, from household appliances to connected cars, consumers are using these devices to stay healthy, to increase efficiency, to be secure, and to make better decisions.

You've heard the estimates of how these are going to grow, and they are estimates. I just swore to tell the truth, so I can't say they're factual, but there is definite growth. We see it ourselves. We grew 32 percent in the United States alone in terms of connected home devices. It's already almost a billion dollar marketplace in the United States just in the home area.

And these home control systems allow consumers to manage their security systems, turn on appliances, manage heating and cooling and lighting systems, and they also increase home efficiency and cut bills, they can learn room usage patterns over time, they can adjust temperatures and maximize efficiency even when no one is home.

And while these save time and money for ordinary Americans, there's an opportunity here to care for our aging population, as well as the 56 million Americans with disabilities. Assistive technology has previously been customized and costly. Connected home products consumers are buying today provide novel interfaces like voice control that help people with reduced mobility and dexterity. Smoke detectors can now be connected to lighting controls so lights

can flash to a person who can't hear, and they can light up the whole house for a safe exit.

In today's low-cost connected home products are life changing and sustaining for many Americans. Think about our older loved ones. We have limited caregivers with an aging population, and smart home devices will help seniors to live independently and comfortably, retain their quality of life, and they could do this with caregivers watching remotely, and at the same time our older Americans will retain their privacy and share just what they're comfortable sharing.

It's coming quickly in terms of the Internet of Things, but it does face impediments. First, it requires spectrum. Wireless spectrum is a platform on which most of these new devices connect, and we need additional licensed and unlicensed spectrum.

Second, the Internet of Things is changing what skills we need to retain our Nation's competitive advantage. We need experts and people who can analyze data and make things happen, and we don't have enough skilled workers. That's why we are pushing for highly skilled immigration reform.

Third, the Internet of Things requires government restraint. It does require us to consider new challenges. There are legitimate concerns about safety, privacy, security, but—and important questions are being raised as to who actually owns the data, and stakeholders, including government, can and should be discussing these issues in a forum like this today.

As we said in our IoT filing with the FCC over 2 years ago, consumers' adoption hinges on building trust. I just heard that again, Congresswoman. And it's up to manufacturers and service providers to make good decisions about privacy and security or they will fail in the marketplace, and we are passionate that industry-driven solutions are best to promote innovation while protecting consumers, but we recognize and respect the legitimate role of government to encourage transparency, clarity, and experimentation.

CEA itself has been involved already in over 30 standards making operations, activities that produce ANSI-certified standards, that are focussing technical aspects of Internet of Things, and of course, it's just beginning. But we have to be careful of overly prescriptive mandates because that could stymie the growth of the Internet of Things. Any government action should be very narrow and very specific and focus on a real harm.

The Internet of Things is huge. It's an opportunity to change the world, and we look forward to working with this Committee to ensure that government policies and regulations support growth in this dynamic sector. Thank you, and I look forward to answering your questions.

[The prepared statement of Mr. Shapiro follows:]

House Committee on Judiciary

Subcommittee on Courts, Intellectual Property, and the Internet

Hearing on the Internet of Things

Wednesday, July 29, 2015

Statement of Gary Shapiro, CEO and president,

Consumer Electronics Association

Thank you, Chairman Issa, Ranking Member Nadler, Chairman Goodlatte, Ranking Member Conyers, and members of the Subcommittee, for inviting me to testify today on the Internet of Things.

I am Gary Shapiro, CEO and president of the Consumer Electronics Association (CEA).

CEA is the trade association representing more than 2,000 member companies who comprise the $285 billion U.S. consumer technology industry.

We also produce the annual CES, the world's gathering place for the global technology community held each January in Las Vegas, where more than 900 exhibitors displayed IoT devices — a hint of the innovation and imagination to come.

Having a front seat at the latest innovation has allowed me to see the unimaginable. And it isn't far from us.

Imagine a "smart" Capitol Hill, where smart parking, driverless cars, and interactive dining and fitness areas make doing business much easier and better.

It is 5:30 a.m., Congresswoman Smith checks into the Rayburn House gym via biometrics. Before she starts her workout, she records her health vitals at an intelligent-equipment station, which develops today's personalized workout based on past performances.

Afterward, she stops by the Longworth House Office Building cafeteria to grab a cup of coffee from a smart coffee machine. The machine tracks the daily consumption of users, making sure that by the time the congresswoman arrives, her favorite coffee blend is available.

Midday, she jumps into her driverless car to welcome veterans as part of the Honor Flight program.

As the lawmaker returns to Capitol Hill for votes, she opens her smart-thermostat app to begin cooling down her office.

While this is a fictional scenario, it is only a matter of time until it is everywhere. IoT is so big at the CES that we can no longer section it off– it is everywhere!

Some argue our entire show floor constituted the IoT with almost every product connected to the Internet and many able to sense, report on and respond to their surrounding environment.

Over the past several years, we've seen an explosion of connected devices in the market, as consumers embrace the positive impact of these devices on their daily lives.

From wearables like smart watches and fitness trackers, to connected thermostats and automated lights, from household appliances to connected cars, consumers are using the IoT to improve their quality of life – to increase efficiency, improve safety and security, and make faster and better decision-making.

According to a recent study from Juniper Research, 38.5 billion "things" will be connected to the Internet by 2020.

A January 2015 report from Mind Commerce indicates that the global market for connected consumer devices will reach $88 billion by 2020.

A significant and growing category within the IoT is connected home technologies.

A recent CEA study conducted with the research firm Parks and Associates predicts smart thermostats, door locks, smoke detectors and light switches will expand from 20.7 million units in 2014 to 35.9 million units by 2017. These are eye-popping numbers.

CEA also predicts that the U.S. market for Connected Home Technologies will reach $967 million in 2015, jumping 32 percent over last year. This segment will grow to nearly $1.1 billion in 2016.

Home automation systems enable consumers to manage their security systems, turn on appliances, and manage heating, cooling and lighting systems, all from a smartphone.

Smart systems not only provide safety and convenience for a homeowner, but they also increase a home's efficiency and reduce energy consumption and costs.

Many of these devices also learn room usage patterns over time allowing them to adjust temperatures automatically to maximize efficiency when no-one is home.

Today, consumers can purchase refrigerators that can count and display the number of times the door is opened and alert homeowners via an app when the door is ajar - all you late night snackers are hereby warned.

For those like me with limited time, there are now washers and dryers that allow consumers to start their laundry on the way home from work …or the airport.

At my home in Detroit, my family has a washer dryer that's connected to the Internet. We have programmed our window shades to rise based on our sleep patterns, and shut accordingly to maximize our home's heating-and-cooling efficiency.

Our thermostats are also connected to our house fans to minimize energy use.

We have smart locks with codes we can assign to our house guests – beats keeping the door key under the mat – and safety cameras we also use to figure out where we put things we lost.

These connected appliances offer consumers convenience, information to help reduce energy use and costs, and additional control over the appliances in their homes.

While these innovations will save time and money and reduce stress, they provide an even greater opportunity to care for our aging population, as well as the 56 million people with disabilities in the US.

Assistive technology for people with disabilities has previously been customized and prohibitively expensive. The same connected home products consumers are purchasing today provide novel interfaces, like voice control, that are immediately beneficial to people with reduced mobility and dexterity.

Without paying tens of thousands of dollars for a custom home automation system, smoke detectors can now be connected to lighting controls, so lights can flash to alert a deaf or hearing impaired person and light the whole house for safe exit.

The amazing conveniences of today's low-cost connected home products are life-changing and sustaining for a growing population.

I am especially excited about how the IoT will help us care for our older loved ones in years to come.

As our population advances in years, and the number of caregivers shrinks, smart home devices enable seniors to live independently and comfortably at home, retaining their quality of life into their golden years.

Connected devices can remind seniors to take their medication, refill their prescriptions, and help prevent accidental over- or underdoses.

Already, a senior who wakes in the middle of the night can adjust her lighting, confirm the doors and windows are closed and locked (or lock them if they aren't), and adjust the thermostat from the palm of her hand – without the risk of getting up and falling in a dark house.

Caregivers gain peace of mind using systems that allow them, regardless of their location in the country or world, to know that their loved ones are safe and secure.

They can confirm their loved ones are active, they're eating properly and taking their medicines, and their homes are safe and secure, all while allowing the seniors to control the level of information shared to respect their privacy.

The health and quality of life impacts of the IoT will be a game changer for our nation's seniors and for those that care for them.

In fact the IoT is coming quickly, but it does face impediments.

As with so much other innovation, spectrum is the lifeblood of the Internet of Things. Wireless spectrum is the platform on which most of these new devices connect.

The future benefits of the Internet of Things depend directly on our ability to free up additional licensed and unlicensed spectrum.

Disruptive innovation brings excitement and opportunity, and requires us to consider new challenges. Government is raising legitimate concerns about safety, security and privacy.

Healthcare professionals are raising interesting questions about how they are compensated in their existing health care regimens for monitoring remote patient data.

Questions are being asked as to who owns data from these devices.

As the IoT grows, manufacturers and service providers will continue to focus on making good decisions about privacy and the security of information that devices collect and share.

Consumer adoption hinges on building trust. Devices that do not meet consumer privacy and security expectations will fail.

CEA and our members are exploring these issues and how best to ensure consumer privacy and security, while enabling new technologies to develop and flourish.

We believe that industry-driven solutions are the best way to promote innovation while protecting consumers.

The IoT is also creating new jobs.

We now face a shortage of the needed experts and data analysts who can help take this massive amount of information and turn it into useful and actionable results.

The United States simply doesn't have enough high-skilled workers with the technical expertise necessary to fill all of the high-tech jobs our sector is now creating.

The tech industry relies on high-skilled immigrants here on H-1B visas — many educated at U.S. colleges and universities — to fill this void.

Of the 172,000 applications for H-1B visas in 2014, fewer than half were granted, the U.S. Chamber of Commerce reported in April. That's a direct result of a federal cap on the number of H-1Bs issued.

Passing high-skilled immigration-visa reform would go a long way toward solving the high-skilled worker shortfall.

We are just beginning to understand the benefits and challenges of the IoT. In this dynamic and rapidly changing environment, governments should exercise regulatory restraint.

Overly prescriptive mandates will stymie growth and become outdated. If governments must act, then such actions should be narrowly tailored to address tangible harms without creating roadblocks for future innovation.

Government should not attempt to regulate based on hypothetical concerns, but should proceed slowly with targeted solutions to actual problems.

We are already experiencing the benefits of a connected world, as connected technologies and services improve the quality of life, health and safety of consumers.

CEA is proud to represent the companies whose products and services comprise the Internet of Things.

We look forward to working with the Committee to ensure that government policies and regulations support growth and innovation in this dynamic sector.

Thank you, and I look forward to answering your questions.

Mr. ISSA. Thank you, Mr. Shapiro.
Mr. Garfield.

TESTIMONY OF DEAN C. GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. GARFIELD. Thank you, Chairman Issa, Ranking Member Nadler, Members of the Committee. On behalf of 61 of the most dynamic and innovative companies in the world, we thank you for hosting this hearing. We thank you as well for the context, which is outside pending legislation, and as well, Mr. Chairman and Congresswoman DelBene, for your leadership in creating the Internet of Things caucus.

It is our firm view that the Internet of Things has the potential to be one of the most transformative technological innovations in human history. That is, with the right policy environment. To ensure that I'm not accused of engaging in hyperbolic hyperventilation, I would like to focus my testimony on three areas.

One, why we think that's the case; two, what we're doing to enable it; and then third, our humble recommendations on how Congress and the Administration can be helpful.

As to the first, the Internet of Things is essentially the digitization of the physical world through connecting sensors into a network with computing systems. What may sound simple has the potential to be seismic in the creation of new industries as well as disruption of existing ones. Whether we're talking about watches that have the potential to not only help you to be more fit but as well to prevent catastrophic health incidents through monitoring your heart rate, or we're talking about windshield wipers that have the ability to communicate with other windshield wipers and alert your car to an impending storm or alert an autonomous vehicle to the potential for a construction zone that's soon arriving.

There has been much discussion of the home and personal manifestations of the Internet of Things, which are truly exciting. It is important, however, not to ignore the potential, the commercial deployments. Those commercial deployments are real, tangible, and have huge potential economic benefit.

Whether it is the deployment of sensors in our energy grid to ensure greater resiliency and reliance, the deployment of sensors in transportation systems to allow more efficient delivery or in mines to ensure safety for workers, the economic impact, much of the economic impact will come from those deployments, which by 2030 is expected to be almost $7 trillion.

So what are we doing, as the technology sector, to ensure that is the case? We are focused on a multi-facetted approach that heavily emphasize security, privacy, standards as well as investment in infrastructure. With regard to security and privacy, we are working and innovating all the time around those issues, making sure that security and privacy are developed by design so that they are part of our forethought rather than an afterthought.

We're developing bespoke solutions to ensure that both security and privacy are tailored to the particular environment, and as well, we're investing in innovation because consumers demand a high security and privacy and increasing transparency, and it's in our in-

terest, and it's the right thing to do to meet that consumer demand.

As well, we are moving forward on global standards that are driven by the sector and as well that are open standards to ensure that we have high interoperability as well as scalability.

Finally, we're investing in the infrastructure. Mr. Shapiro noted the need for broadband, both wireline and wireless, as well as ensuring that spectrum is available. In reality, the use of spectrum on mobile data, is growing by 55 percent each year. With the Internet of Things and the digitization of physical things, it will only grow more expeditiously, and so spectrum will be increasingly important.

In addition to doing those things, we intend and need to partner with Congress and the Administration to make sure that policy is smartly developed, and there are three things that we think it's important that Congress focus on.

One is we need a national strategy around the Internet of Things. Much in the same way that a national broadband plan was able to focus our attention and drive the deployment of broadband, having a national strategy around the Internet of Things will be incredibly helpful.

Second, we need more spectrum, as Mr. Shapiro and I pointed out earlier. The U.S. Government is the largest holder of spectrum, and hence, has the greatest ability to impact the deployment of spectrum, and we hope that we can work toward making it more efficient.

Finally, we need the exercise of restraint. The Internet of Things is at its nascent stages, and in order to grow to reach its full potential, it's important that we avoid mandates that put the thumb on the scale of particular technologies versus others.

I look forward to your question and look forward to the testimony of my colleagues. Thank you.

[The prepared statement of Mr. Garfield follows:]

Information Technology Industry Council

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

Internet of Things Hearing Testimony of
Dean C. Garfield, President and CEO of the
Information Technology Industry Council

Good morning. Thank you Chairman Issa, Ranking Member Nadler, and Members of the Subcommittee for inviting me to testify this morning. The issue we are discussing today has the potential to positively transform our world more than perhaps any development since the invention of the Internet itself.

My name is Dean C. Garfield, and I am President and CEO of the Information Technology Industry Council (ITI). ITI represents 61[1] of the most innovative and forward-looking companies in the world. Our membership includes companies from all verticals of the technology sector, including semiconductor, network equipment, software, digital services, hardware, mobile device, and Internet companies. This gives ITI a broad perspective on the transformational economic, societal, and commercial opportunities the Internet of Things (IoT) is creating. Note, I say "is creating" because for all of our companies, this market is real. Companies are investing in IoT, and 80 percent of those that do are seeing increased revenue as a result of IoT initiatives, with the average increase in revenue being 15.6 percent.[2] Eighty seven percent of CEOs expect long-term job growth from IoT.[3] But development and innovation will only continue with appropriate support from policy makers, and I look forward to discussing these opportunities with you today.

Definition and Categories of IoT

The IoT is a collection of external devices and sensors that generate data, which, through an Internet connection, can be analyzed to provide actionable information. The range and application of these devices is virtually limitless, but we generally view them in three distinct categories: 1) commercial or industrial, 2) personal or mobile, and 3) household.

Commercial and industrial IoT devices are by far the largest category, and the area where many of our companies see the biggest opportunity to enhance productivity and efficiencies, improve real-time decision making, and solve critical societal problems. Estimates for this specific

[1] See membership list here: http://www.itic.org/membership/member-companies
[2] Tata Consultancy Services, *Internet of Things: The Complete Reimaginative Force*, rel. July 2015.
[3] Accenture, *CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to drive future business strategies*, rel. 2015.

category of IoT are predicted to eclipse $7 trillion by 2030.[4] This category includes predictive maintenance of equipment, facility heating, cooling and lighting management, transportation fleet management and improvement, and many other large scale uses where the aggregate of small changes on a large scale equates to significant cost, energy, and other efficiency and productivity improvements. Exhibit 1 demonstrates how IoT applications can be deployed in a specific industrial setting, namely mining and resource transportation. Roughly 70 percent of the potential value from IoT comes from commercial and industrial IoT applications.[5]

Personal or mobile IoT technologies - probably the most familiar as wearable watches, health monitors, and similar devices that connect to the Internet via wireless broadband or through a mobile phone - are becoming ubiquitous. But the real gross domestic product (GDP) impact from this category will be derived from autonomous vehicles and cars connected to the Internet via cellular or other wireless technologies. The defining characteristic of this group is the mobile nature of the IoT application and the reliance on a wireless broadband connection.

Lastly, household IoT applications range from smart appliances to smart thermostats, and intelligent home monitoring and security systems. These products will connect through a residential broadband connection or home Wi-Fi network to provide energy savings and home automation and security benefits.

IoT Technologies In Action

ITI was pleased to participate in the inaugural Congressional Internet of Things Caucus event last week on "Smart Cites: How IoT is Changing Communities." As that panel discussed, IoT will disrupt nearly every public and private sector function, including trash collection and street lighting, and in so doing will make our cities not only smarter but also more livable, more workable, more resilient, and more competitive. Public and private sector partnerships will be essential in leveraging IoT to make such advancements in our cities. Is there a role for the federal government in doing so? I think so, but as the Chairman stated at an event this spring that I moderated, "Congress' role is to learn to do only what's necessary and no more." We look forward to working with the Chairman and this Committee in an effort to narrowly target only that which is necessary. This will involve focusing on acceleration of efforts and projects that will help the key stakeholders achieve their collaborative maximum. Cities will be a key incubator for the collaborations that we seek, and ITI looks forward to working with this Subcommittee on ideas for how the federal government can be a partner in this regard.

Similarly, ITI and our member companies have been increasingly focused on smart transportation policy as major automotive companies and major technology companies are increasingly partnering to embed complex, computer-based technology in their new vehicles.

---

[4] Accenture, *Winning with the Industrial Internet of Things*; rel. 2015.
[5] McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*; rel. June 2015.

Again, this is an area where Congress and the federal government can play an important role where appropriate, but must be careful not to thwart U.S. innovation and competitiveness. For example, connectivity and communications between vehicles must be secure and reliable, especially for safety applications; this is something that Congress, the Department of Transportation, the Federal Trade Commission (FTC), and other government stakeholders should oversee to protect consumers. Additionally, to advance U.S. global competitiveness, policymakers also must promote investment and development of a wide range of innovative automotive and transportation technologies to improve the safety, mobility, and efficiency of America's roads and highways.

ITI's companies are innovating in this exciting, new area. Advanced driver assistance systems include sensors to provide features such as brake assist and adaptive cruise control. A broad range of wireless communication technologies will allow vehicles to communicate with one another and with infrastructure, which will enable a world of new safety, traffic flow, and other applications. Autonomous driving technology has received significant attention with many companies conducting extensive testing of these technologies around the world – and today's consumers already expect partially-autonomous technologies like parking assist and adaptive cruise control when they buy a new car. These are all very promising technologies that will provide tremendous safety, efficiency, mobility, and economic benefits. It is critical that while the government oversees things like security standards for communications between vehicles, it must also foster innovation. To this end, policymakers should encourage the development of all of these advanced automotive technologies by letting the marketplace evolve, and not promoting one specific technology over others. The safety of our citizens on U.S. roads and highways is paramount, and the U.S. must lead globally with the most innovative, effective, and secure technologies.

The home is another platform familiar to the public where IoT technology will drive significant benefits and cost savings for consumers. Home energy management – smart thermostats and appliances – chore automation, and home security and monitoring systems have the potential to create an economic impact of more than $200 billion per year by 2025.[6]

Enabling IoT Development – a Public-Private Effort

Let me clarify at this point, while I provided statistics from multiple studies predicting immense economic benefits through further development of the IoT, none of this is guaranteed. The estimated economic benefits often cited are dependent on a fertile innovative environment comprised of favorable policies and minimal regulatory barriers. Congress, the Administration, and governments around the globe will play an important role in realizing or, alternatively, falling short of those potential estimates for economic and societal growth.

[6] McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*; rel. June 2015.

To motivate IoT adoption, applications and devices must evoke user trust through hardened security and privacy solutions. ITI's member companies are at the forefront of providing security solutions from the devices at the network edge to the cloud. With billions of additional devices coming online, ITI's companies are embedding security in IoT platforms at the outset of the manufacturing and design process for each new device that extends and expands the network. Security must be built into both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Different systems, products and applications bring very different security needs, and the technology sector addresses those needs on a case-by-case approach. There is not a one-size-fits-all approach to addressing security, particularly in the IoT space given the broad range of applications, and industry stands ready to work with policymakers to develop a policy framework that enhances privacy in the IoT. ITI previously released cybersecurity principles, which are applicable to the IoT in their approach to addressing security.[7]

With the same design and manufacturing phase emphasis, companies build their IoT products to appropriately respect and protect user privacy. This privacy-by-design approach is critical to incentivize consumer adoption of these technologies, thereby enabling the aggregation, filtering, and sharing of data across network and devices. As more data is shared securely, companies and users will certainly find new ways to use that data – especially in the aggregate. In some applications, de-identified aggregate data is what is needed to serve the necessary purpose, thus minimizing privacy implications.[8] New constraints on the collection and use of data may hinder innovation in this area and dampen the promising uses of this aggregated data in areas such as medical research. Resisting new restrictions, however, does not mean the IoT will become the wild west of privacy. IoT technologies collect and utilize a wide variety of data, much of which is already subject to existing laws or rules governing collection, use, and sharing.[9] If the maximum benefit is to be derived from the IoT, policymakers should avoid adding unnecessary layers of regulation or requirements by considering the types of data that will be collected, and instead ensure compliance with existing rules and regulations.[10]

---

[7] See ITI's *Cybersecurity Principles for Industry and Government*: http://www.itic.org/public-policy/CybersecurityPrinciplesforIndustryandGovernment.pdf

[8] This would be the case for an application that reports potholes to a city, either from a user manually entering that data, or from technology in a mobile device or car autonomously reporting that information.

[9] For example, there are existing laws that impose privacy requirements on certain health and financial information, and the FTC has the authority to take action against unfair or deceptive acts or practices in connection with the IoT.

[10] For instance, a sensor on a motor that measures vibrations or heat output to recognize preventative maintenance is significantly different from heart rate, body mass index, or blood pressure data collected by a smart watch.

For the various IoT categories listed above, different types and amounts of data will need to be collected, and used in many different ways. It is incumbent upon ITI's member companies, and all companies offering IoT applications, to be transparent about their practices. We must also ensure that data is appropriately protected. Businesses and consumers will be reluctant to adopt IoT applications if they have privacy concerns, or concerns that their data is not secure. If businesses realize the benefits that can be captured through continuous measurements of their energy use, or consumers understand braking data from their vehicle is being aggregated so autonomous vehicles can more accurately navigate roadways, and this data is being stored securely and used appropriately, there will be greater comfort in embracing these technologies Should industry fail to do this, policymakers should act in a tailored fashion to address the specific problem, recognizing overreach could impact the broader development and potential of the IoT.[11]

The private sector is investing, and must continue to invest heavily in the communications networks and infrastructure that this data will traverse. The explosion of connected devices will expedite the growth trend for mobile data, which already is growing 55 percent year-on-year.[12] Continuous investment in our networks will be necessary to handle this growth. Robust broadband networks are a fundamental building block to the IoT, and only with ubiquitous, high-speed, affordable broadband will the public and private sectors be able to derive the maximum potential the IoT will offer. Congress, and the relevant federal agencies, must continue to make spectrum available for mobile broadband and enable efficient spectrum management. Effective spectrum management will encompass licensed, unlicensed, and licensed shared access regimes that promote spectral efficiency, and enable the diversity of spectrum uses across the broad range of IoT products and services. The federal government must also advance policies that foster private sector investment in wired and wireless networks, and promote build-out to all un- and under-served areas.

To enable broad adoption of IoT technologies and avoid IoT silos, attention must be placed on the ease of connectivity and interoperability of IoT devices, platforms, and infrastructure, as well as streamlined cross-border data flow. Systems of intelligent devices must be connected to each other or the network, often across geographic boundaries, to maximize the potential of the IoT. The private sector is leading the development of open standards that will enable interoperability across the IoT, and partnering with the public sector to encourage the sharing of best practices. Global standards will accelerate adoption, drive competition, and enable the

[11] The FTC's settlement with TRENDnet, Inc., the company that markets video cameras designed to allow consumers to monitor their homes remotely, is an appropriately narrow response to a specific problem. See *In the Matter of TRENDnet, Inc.* FTC File No. 122 3090 (September 11, 2013) (proposed consent order), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security- video-cameras-settles

[12] Ericsson, *Mobility Report, On the Pulse of the Networked Society*, rel. June 2015.

cost-effective introduction of new technologies. Open standards will also promote industry innovation and establish a better defined technology evolution path.

Lastly, but perhaps most importantly, a strategic national IoT plan and funding should be put in place, which encourages public-private partnerships (PPPs), accelerates IoT adoption, and enables vast economic and societal benefits from the IoT in both the near- and long-term. Successful PPPs will make IoT deployments an attractive investment for government and industry, and promote innovation, scalability, and sustainability. By leveraging PPPs, we can expedite IoT research and development and U.S. global IoT leadership. The development of a national IoT plan, and finding areas where the federal government can lead by example in the adoption of IoT, will both foster innovation and enable a multitude of cost savings, efficiencies, and other benefits to the public sector.

Policy Recommendations to Immediately Promote an Innovate IoT Environment

1. **IoT Strategy and Advisory Council** – Creating an advisory board with government and industry partners to produce a National IoT Strategy with ambitious timelines, and more tailored strategies for federal government adoption, smart city promotion, promotion of next generation transportation technologies, and similar efforts to maintain U.S. leadership in the IoT.[13]
2. **Security and Interoperability** – The federal government can encourage industry alignment of private sector developed state of the art security and interoperability solutions, and partner with the private sector to encourage the sharing of best practices.
3. **Public-Private Partnerships** – The federal government should incentivize the use of public-private partnerships as a means to accelerate IoT development and adoption, and U.S. global leadership.
4. **Infrastructure** – The federal government should make additional spectrum available for mobile broadband, implement effective spectrum management programs, and incentivize investment in network infrastructure.

[13] On March 24, 2015, the U.S. Senate unanimously passed S.Res. 110, A resolution expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment, that provided guidance for a national IoT strategy.

Information Technology
Industry Council

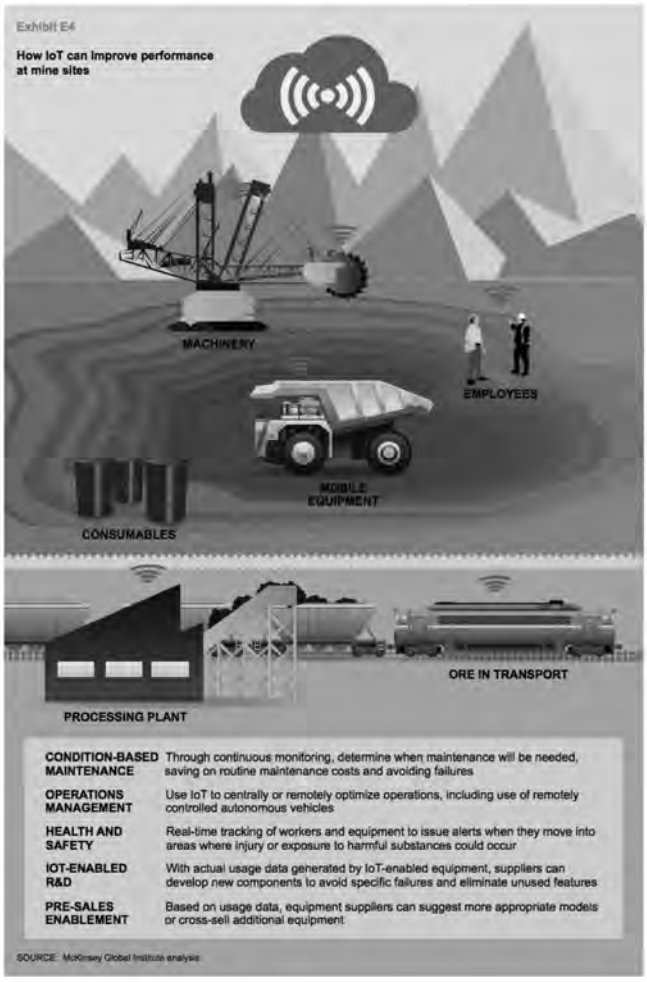
Conclusion

The Internet has transformed the world in ways we could never have dreamed possible, and the IoT is expected to have an even greater transformative impact in our lives, our economy, and our society. Similar to the Internet in the early 1990s, the IoT is in its very nascent stages and presents us with limitless possibilities if we have the vision and environment to achieve them. We look forward to working with Congress to advance these policy recommendations, and maintaining an open dialogue as IoT products, services, and applications evolve. We also ask that lawmakers evaluate existing policy tools and use caution before taking actions that may inadvertently or unnecessarily impede IoT innovation and disadvantage U.S. competitiveness.

I thank the Chairman, Ranking Member, and Members of the Subcommittee for inviting me here to testify and for their interest and examination of this important issue. I look forward to taking your questions.

Information Technology Industry Council

Exhibit 1: McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, p. 10; rel. June 2015.



Mr. ISSA. Thank you.

Mr. Bainwol, you only have to deal with all the questions set up in the opening statement, so I look forward to your 5 minutes.

TESTIMONY OF MITCH BAINWOL, PRESIDENT AND CEO, ALLIANCE OF AUTOMOBILE MANUFACTURERS

Mr. BAINWOL. It's a piece of cake. Chairman Issa, Ranking Member Nadler, Members of the Committee, thank you for the opportunity to testify this morning. I wore a different hat the last time I was here on behalf of another industry that was engaging with the challenge of technology.

During my time at the recording industry, technology upended how music was consumed, and access began to replace ownership, revenues fell sharply, and the fundamental model of business transformed. Now I'm with the Alliance of Automobile Manufacturers for the last 4 years. Instead of fighting with Gary Shapiro, I now mostly team up with him. That's easier. That's a good thing.

Mr. ISSA. Only in Washington.

Mr. BAINWOL. Yeah, right. I represent the Detroit Three, six major European manufacturers, and three major Japanese manufacturers as well.

And for us, the impact of technology is every bit as profound but not threatening. Quite the contrary, technology and connectivity are ushering in a new era and some might even say a golden age in mobility. We've seen enormous safety and environmental gains both in recent years and over the last half century, striking reductions in fatality numbers and emissions, as well as increases in MPG.

The next generation of progress will come from IoT-based technologies. Ownership patterns may evolve somewhat as ride sharing becomes more prevalent, but the truly material impact of technology is the convergence, the convergence of environmental, safety, productivity, and life quality benefits that arise from the connectivity of an IoT world.

It wasn't that long ago that when it came to cars, safety and environmental objectives conflicted. Do you go heavy and safe or light and green? Every parent struggled with that choice for their teenagers. Strategies for safety centered on surviving crashes. Now the combination of automation and connectivity harmonizes, harmonizes safety and green. Crash avoidance from technology that manages the car better than a human can, fosters more efficient mobility because there will be fewer crashes on the road generating congestion. Fewer crashes translates into more economic productivity, more personal time, fewer injuries, fewer fatalities, lower emissions, and less wasted fuel. In an IoT world where connectivity offers the promise of these truly monumental benefits, getting to the future as fast and sensibly as we can is critical.

According to NHTSA, about 95 percent of all traffic fatalities result from human error or environmental conditions. Vehicle factors account for just a fraction. Technology is so powerful because it offers the promise of mitigating human error as today's innovations, automatic braking, adaptive lighting, lane departure warnings, blind spot warnings, and tomorrow's technologies, V-to-V and V-to-X and to ultimately self-driving vehicles all penetrate the car park.

This innovation must be embraced and seen as the answer and not the problem, and that means working proactively to address concerns about privacy and cybersecurity. Last year, auto manufacturers became the first in the IoT, a non-pure play Internet sector, to adopt a comprehensive set of privacy principles to protect vehicle owners. The principles have a strong lineage, building on FIPPS, FEC guidance, the White House Consumer Privacy Bill of Rights, and suggestions from privacy advocates. They address, among other elements, transparency, respect for context, data security, and choice. For the most sensitive types of consumer information that are needed for some driver-assist technologies, geolocation, where you're going, driver behavior, how fast you're going, and biometrics, the privacy principles require clear and prominent notice about the collection of such information, the purposes of why it's collected, and the entities with which it can be shared.

Similarly, the industry is working to stay ahead of the threat posed by malicious hackers. Earlier this month we announced the formation of an Auto-ISAC, Information Sharing Analysis Center, to establish an industry-wide portal for sharing information about existing or potential cyber threats and vulnerabilities.

The Alliance supports cyber security bills in the House that would facilitate threat sharing in the private and public sectors while protecting individual security. We hope the Senate acts soon so that we can move the bill to the President.

Mr. Chairman and Members of the Committee, the next 20 years in the evolution of the Internet is enormously exciting and offers the possibility of amazing outcomes on the road, strengthening the quality of life, the environment, and our economy. We look forward to working with you to realize the benefits of innovation and to address the challenges that come along the way.

[The prepared statement of Mr. Bainwol follows:]

STATEMENT

OF

THE ALLIANCE OF AUTOMOBILE MANUFACTURERS

BEFORE THE:

THE HOUSE JUDICIARY SUBCOMMITTEE ON THE COURTS, INTELLECTUAL PROPERTY AND THE INTERNET

JULY 29, 2015

PRESENTED BY:

Mitch Bainwol
President and CEO

On behalf of the Alliance of Automobile Manufacturers and its 12 automakers, I thank you for the opportunity to testify today on the Internet of Things and the importance of connectivity in advancing road safety, energy efficiency, environmental protection and mobility.

Today, automakers have gone beyond simply manufacturing cars; they are high tech companies, too. Nine automakers, along with three suppliers, have opened labs in Silicon Valley. And, automakers now showcase their latest technologies at the annual Consumer Electronics Show, where each year the automotive exhibit space – along with the consumer interest – grows.

Automakers are driving innovation through deep investments in research and development. Recently, the Boston Consulting Group found that half of the world's "Most Innovative Companies" are automakers, with nine auto manufacturers in the top 20. In fact, more automakers made the list than technology and telecom companies. Globally, automakers invested more than $100 billion on R&D in a single year, according to the latest figures from 2013. And that is four times what the entire global aerospace and defense industry invested ($25.5 billion) in that year.

For the automobile industry, technology and connectivity are ushering in a golden age in mobility. We have seen enormous safety gains in recent years. Government data show this is the safest time in our nation's history in terms of motor vehicle safety. Road fatalities are at their lowest since 1949. Traffic-related crashes declined by 18,000 from 1980-2002, even with more licensed drivers on the road traveling more miles.

Historically, automakers have focused on engineering vehicles to enhance occupant protection in the event of a crash. That's why automobiles today have a range of airbags and specially engineered crumple zones.

But the future of vehicle safety is technologies that help prevent or mitigate crashes. Driver error remains the primary cause of more than 95 percent of crashes, according to the National Highway Traffic Safety Administration (NHTSA). Crash avoidance, or "driver assist," technologies employ sophisticated software to interpret data from sensors, cameras, or radar-based technologies that allow vehicles to sense the environment around them and assist drivers to become aware of impending dangers. There many different types of driver assists, including intervention technologies such as electronic stability control and anti-lock brakes, warning technologies such as blind spot warnings and lane departure alerts, and adaptive cruise control and automatic high beams that help drivers in specific situations.

Connected vehicles may help to enhance or enable a host of critical crash-avoidance technologies. According to NHTSA, connected vehicle technology could potentially mitigate or eliminate up to 80% of crash scenarios involving non–impaired drivers. That is why both automakers and the government are investing hundreds of millions of dollars in research, development and testing of connected vehicle technology also referred to as Dedicated Short Range Communications (DSRC).

The phrase "connected car" can mean different things to different people. For the auto industry, when the car moves from being a closed box to a "mobile device" with the ability to gather data and communicate it, that is a "connected car."

In our digital world today, drivers want to be seamlessly connected to the web and all its functionality, including social media, communications, music, navigation and a range of transportation-related content. These are important to consumers, but connectivity in the car can do so much.

Connectivity can help reduce the potential of crashes by getting information on real-time risk factors outside the vision of the driver – or the electronic eyes of the car. This connectivity refers to the exchange of information either among vehicles (V-to-V) or information between vehicles and infrastructure (V-to-I).

Imagine the benefits from cars able to communicate with each other and the road way. Vehicles encountering slippery roads can send messages to cars behind them to slow down. Likewise, a connected driver can know that a car is speeding toward an intersection or stopped over the next hill and take countermeasures.

The future of driving safety is bright with promise, and with the right public policies put in place to support connectivity, industry and government, through working together, can advance safe mobility. Getting there will require many pieces of a large puzzle to fit together in addition to technological advancements, including consumer acceptance and achieving critical mass to enable the "network effect."

Consideration must be given to the necessary legislative and regulatory framework needed to spur development and adoption of advanced technologies. A patchwork of state laws will negatively impact the speed and trajectory of the technologies adopted. Federal leadership is needed to establish a single, long-term national vision for personal transportation in the future.

Finally, complex legal issues associated with cars and trucks capable of operating with increasing levels of automation need to be addressed. These include insurance underwriting and liability issues.

We are pleased with the great vision of this Committee in focusing today on the future. Like you, we share the goal of ensuring the public policy pillars necessary to achieve the full safety value of connectivity and other technological advances be identified and protected.

We believe four pillars of policy are central to maximizing safety through technology in the future: 1) protect the spectrum; 2) invest in infrastructure; 3) ensure consumer acceptance; and 4) maintain vehicle affordability

Protect the spectrum: The most vital pillar is ensuring that the radio frequency spectrum now dedicated to V-to-V and V-to-I, or the 5.9 GHz band, remains solely dedicated to auto communications technologies or any solutions involving sharing maintain the integrity of DSRC. When vehicles are driving at highway speeds, communications must occur virtually instantaneously, without delay and without interference. At the same time that DOT is considering mandating DSRC technology, the FCC is considering whether to open this portion of the spectrum for use by unlicensed wireless devices. It's important as we move forward that regulators be certain that unlicensed users would not compromise the integrity of this vital safety initiative. We think the FCC should adopt a "do-no-harm" position until thorough testing is completed and all parties are certain that the spectrum can be shared without interference with safety critical systems. Importantly, auto manufacturers are moving forward with our supplier partners, Cisco and Denso, to test a potential technological solution that will allow DSRC communications without harmful interference from unlicensed devices. We look forward to sharing our results with the appropriate federal agencies and Congress.

Invest in infrastructure: The second pillar is building out the infrastructure for the V-to-I component of connectivity. Surely this will be a gradual process, but we need the vision and motivation to begin planning today. As is the case with a range of technologies, such as alternative powertrains for environmental gains, infrastructure investment is essential to achieving the maximum safety benefit and inducing buyers to purchase the V-to-I communications functionality.

Ensure consumer acceptance: The third pillar is proactively responding early to consumer acceptance by addressing public concerns about deployment potential. If the advent of connected vehicle technology exposes drivers and owners of equipped vehicles to loss of privacy, security breaches, and/or increased legal liability in the form of automated law enforcement, we will not realize the many benefits that can be gained by its widespread deployment. Similarly, connected and automated vehicle systems entail interactive technologies for which successful outcomes depend not only on drivers' correct response to alerts and information, but on multiple entities in both the public and private sectors correctly and consistently performing their respective portions of the connected enterprise. This creates new

and unprecedented challenges to managing long-term liability which require up-front policy solutions.

Maintain vehicle affordability: The fourth pillar is public policy dedicated to keeping cars and light trucks as affordable as possible by leveraging market forces and utilizing a data-driven approach to regulation if and when needed. The best technology in the world can only help if families are able to replace their old cars with new vehicles. Today, the average age of a car is 11 years old, and we only replace about 6% of the U.S. car park every year. When the safety and environmental benefits of new cars relative to old cars are sizeable, the public policy imperative must be to avoid the temptation to mandate and instead facilitate choices by families in the marketplace. Policies that discourage the purchase of these new technologies should be avoided. As a matter of public policy, we need to encourage the "virtuous cycle of new car ownership."

Finally, we recognize that connectivity in vehicles also may raise questions about privacy and cyber protections. The auto industry is already taking action in both areas.

Last year, the auto industry became the first industry in the Internet of Things to adopt a comprehensive set of Privacy Principles to protect vehicle owners. These Principles have a strong lineage, building on the Fair Information Practice Principles, FTC guidance, the White House Consumer Privacy Bill of Rights and the suggestions of privacy advocates. The principles address transparency, respect for context, data security, choice and more. For the most sensitive types of consumer information, including geo-location, driver behavior and biometrics, the Privacy Principles require clear and prominent notice about the collection of such information, the purposes for which it is collect, and the types of entities with which the information may be shared. These Principles can be viewed at www.AutomotivePrivacy.com, where a list of the 20 leading automakers who voluntarily signed on to them can be found.

Similarly, automakers are working to get ahead of potential threats posed by malicious hackers. Automakers recently announced the formation of an Automotive Information Sharing and Analysis Center (Auto-ISAC). The new Auto-ISAC, planned to begin operation before the end of the year, will establish an industry-wide portal for sharing information about existing or potential cyber threats and vulnerabilities.

In addition, automakers work with many different groups to advance cybersecurity. These relationships help automakers develop vehicle-specific security technologies and practices. This summer, automakers are participating in events with the cybersecurity community like the annual Battelle-SAE International CyberAuto Challenge and the DEF CON and Black Hat Conferences. Recently, the Alliance joined the US Chamber of Commerce's Cybersecurity Leadership Council, a committee of 20 different industry organizations formed to focus on current and emerging best practices.

Finally, there are several government-wide vehicle-specific cybersecurity initiatives, including research activities undertaken by NHTSA's Electronic Systems Safety Research Division, and the Department of Homeland Security's (DHS) Science and Technology Directorate.

We are entering the golden age of mobility through technology and connectivity. A top policy priority for our country is finding smart ways to put more new vehicle technologies on our roads, because more rapid adoption of these new technologies will help keep drivers safer, avoid traffic congestion, save time, save money and reduce fuel use too.

In an Internet of Things world, where connectivity offers the promise of monumental societal benefits, getting to the future as fast as we can is critical.

Many thanks for this chance to share our perspective.

Mr. ISSA. Thank you.
Mr. Reed.

TESTIMONY OF MORGAN REED, EXECUTIVE DIRECTOR, ACT|THE APP ASSOCIATION

Mr. REED. Chairman Issa, Ranking Member Nadler, and distinguished Members of this Committee. My name is Morgan Reed, and I'm the executive director of the App Association. I thank you for holding this important hearing on the Internet of Things.

The App Association represents more than 5,000 companies and technology firms around the globe, making the software that runs the devices you wear and the apps you love. We are current spearheading an effort through our connective health initiative to clarify outdated health regulations, incentivize the use of remote patient monitoring, and ensure environment in which patients and consumers can see an improvement in their health.

This coalition of leading mobile health companies and key stakeholders needs Congress, the FDA, HHS to encourage mobile health innovation and support polices that keep sensitive health data private and secure.

Now, traditionally, this is the moment in my oral testimony where I should recite some interesting numbers about the industry, talk about jobs created, and niches filled, but I'd like to break from that a little bit. I want to tell you a story, and it's one that I know is relevant to many of you and certainly to a huge chunk of your constituents.

Nearly everyone in this room is caring for an aging parent or knows someone who is. Now, imagine that your parents are fortunate, they're living in their own home but significant medical challenges are beginning to face them. The questions begin, do I get a home health attendant? Do we pay as much as $12,000 a month to move them into an assisted living facility? Do they move into my basement? How do I deal with the fact that my parents don't want to move into my basement, and mom feels that a home nurse is infantilizing. What do I do to help them live at home with dignity?

Now, most of you remember Life Alert, you know the product with the tag line, "Help, I've fallen, and I can't get up." Well, that kind of device is known as a personal emergency response system. We called them PERS. These are great devices but incredibly limited to what they can do.

Now, imagine a far more sophisticated PERS packed with sensors that can track blood sugar, blood pressure, heart rate, biomarkers for medication adherence, geo fencing for Alzheimer's patients, and much more. Sensors small enough to fit in a watch like this one or maybe this one, and all of those devices—yeah, I think everyone here has got one. All of those devices connect to a loved one's phone, an alert service, a physician's tablet, and a medical record. Suddenly, mom can stay at home maybe another year, maybe two, maybe three, all while managing her health. And if mom allows the data to be sent to you, you can be part of the solution, staying in touch and on top of her needs. And not insignificantly, your basement gets to keep its big screen TV.

By 2050, there'll be 83.7 million Americans over the age of 65, twice the amount from 2012. Eighty percent will have at least one

chronic condition. Without question, the age group's rapid growth will strain public and private health resources; therefore, the picture I painted you is not a pipe dream but rather is imperative to prevent a cataclysmic economic outcome from this boom in aging adults.

So what's standing in the way of this dream? What is needed to ensure that everyone can benefit from these new innovations? Well, I have three quick messages.

One, innovation in healthcare is happening. It can lead to lower cost, better care, and improve patient outcomes. Two, the future of health IoT will be founded on trust, which requires strong security and privacy measures. Three, regulatory barriers, outdated laws, and lack of clarity around reimbursement are a threat to the advancement of mobile health. Congress can and in some cases must play an important role in improving health outcomes for all Americans through innovative technologies.

Questions about privacy, security, reimbursement, and government regulation have met to create an environment where companies are worried about making devices more medically relevant, and physicians worry about the impact on their practice and their liability. Patients and care providers must know that their information is private and secure. Industry best practices around the treatment of sensitive health data as well as a commitment from government to support these practices are important to establish trust and push this industry forward.

Clarifications on government access to data matter as well, including ECPA reform and the LEADS Act. As most of this health information will eventually end up in the cloud, and Congress should be pushing back on any government pressure to weaken encryption.

Finally, ensuring that doctors are reimbursed for the use of these technologies will be essential. Currently, CMS is statutorily prevented from reimbursing certain kinds of remote patient monitoring because of absurd geographic restrictions and antiquated technology requirements that were state of the art 15 years ago but haven't moved since.

Success will come when technology, trust, and means to pay for it all come together. I ask that Congress help to ensure that that happens now rather than see one more of our family members moving out of the home they love because we failed to act. I look forward to your questions.

[The prepared statement of Mr. Reed follows:]

ACT | The App Association

Testimony

of
Morgan Reed
Executive Director
ACT | The App Association

on
Internet of Things

before the
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

July 29, 2015
2141 Rayburn House Office Building

Chairman Issa, Vice Chairman Collins, Ranking Member Nadler, and distinguished members of the Committee: My name is Morgan Reed and I am the executive director of ACT | The App Association. I thank you for holding this important hearing on the internet of things (IoT).

ACT | The App Association represents more than 5,000 app companies and technology firms around the globe. As the world has quickly embraced mobile technology, our members have been creating innovative solutions to improve workplace productivity, accelerate academic achievement, and help people live healthier lives.

The App Association is spearheading an effort through our group called the Connected Health Initiative to clarify outdated health regulations, incentivize the use of remote patient monitoring, and ensure the environment is one in which patients and consumers can see improvement in their health.[1] This coalition of leading mobile health companies and key stakeholders urge Congress, the Food and Drug Administration (FDA), and Department of Health and Human Services (HHS) to adopt policies that encourage mobile health innovation and keep sensitive health data private and secure.

My goal today is to describe the current landscape of mobile health, how IoT is already dramatically improving the management of personal health and chronic medical conditions, and what is needed to ensure everyone can benefit from these new innovations.

Specifically, there are three key messages for the members of the Committee:

1. Innovation in healthcare is happening; it can lead to lowered costs, better care, and improved patient outcomes.
2. The future of health IoT will be founded on trust, which requires strong security and privacy measures.
3. Regulatory barriers, outdated laws, and lack of clarity around reimbursement are a threat to the advancement of mobile health.

Congress can, and in some cases, must play an important role in improving health outcomes for all Americans through innovative technologies.

Things: A platform for sensors

The widespread use of mobile devices has made consumers comfortable with fitness wearables, smart light bulbs, and connected refrigerators. All combined, the internet of things is projected to be worth more than $947 billion by 2019.[2]

These "things," however, are not what's interesting – the real power comes from the actionable insights gathered by sensors embedded in every connected device. Increasingly used in healthcare, sensors are poised to cut costs and help deliver personalized care that leads to better outcomes.[3]

As sensors become smaller, cheaper, and more accurate, wearables and other connected health technologies are set to accomplish several key milestones. Namely, they will be seamlessly interoperable, and maintenance activities that require human intervention, like syncing and charging, will be reduced or eliminated.

The collection of this information, however, is not an end in itself. Real innovation will come from the ***use*** of our data. Patients and clinicians will place greater value on companies that can best interpret sensor data to provide a clearer understanding of health conditions.

Rather than a yearly update on one's vitals in a doctor's office, sensors will empower people to share it with a care team, have it incorporated in a cloud-based health record, or shown on a dashboard app in just a few taps.

Big platform providers are trying to make this promise a reality – Microsoft's HealthVault now incorporates more than 371 devices into its storage and management system,[4] and Apple has created HealthKit and ResearchKit.

HealthKit allows health apps and devices to work together in one safe, secure place, providing a user with a complete picture of their health via the Health app. The open source ResearchKit platform makes it easy for researchers and developers to create apps that can incorporate the health data collected by devices in medical studies.[5]

Yet, with all this promise, a recent survey of healthcare providers found that only 15 percent are discussing wearables with patients. This, despite the same physicians saying that nearly half of patients not currently using wearables and apps could benefit from doing so.[6]

Why?

Questions about privacy, security, reimbursement, and government regulation meet to create an environment where companies are worried about making devices more medically relevant, and physicians worry about the impact on their practices.

Patients and care providers must also know that their information is private and secure. Industry best practices around the treatment of sensitive health data, as well as a commitment from government to support these practices, are important to establish trust and push this industry forward.

Getting health IoT right

Our members understand the importance that patient trust plays in an effective healthcare system, and work to keep sensitive health data secure and private.

Connected solutions like those made by App Association member AirStrip® provide a model example of health IoT in a care setting. During an emergency situation, AirStrip® technology is critical to keeping doctors informed on patient vitals while they're still in the ambulance. The company's products use Department of Defense-level encryption that allow doctors to remotely view live patient waveform data from multiple devices and systems on a single mobile screen – all before entering a hospital room.

Connected devices have also become an important tool for consumers trying to reach a wellness goal. Whether it's diet tracking and step counting for weight loss, or monitoring heart rate and improving form to train for a marathon, the internet of things has become integral to health and fitness. While wearables and connected health technologies are being purchased at astonishing rates, privacy and security concerns remain.

Sixty-eight percent of consumers say they want a wearable paid for by their insurer in exchange for anonymous data. But if asked to give personally identifiable information, users shift dramatically in the other direction, with most opposing the use of any health data for targeted, interest-based, or behavioral advertising.[7]

It's clear that average consumers and patients with chronic conditions see value in the use of connected health technologies, but they don't want to give up their privacy, and doctors want to know they will be reimbursed for using them. The mobile health industry and other stakeholders must meet these expectations for innovation in this life-saving space to continue.

Once these questions are answered, wearables and other connected devices – including those already on the market – will provide useful insights for care providers. It will lead to earlier detection of irregularities, more accurate diagnoses, and improved care overall.

Wearables improve fitness & provide important insights

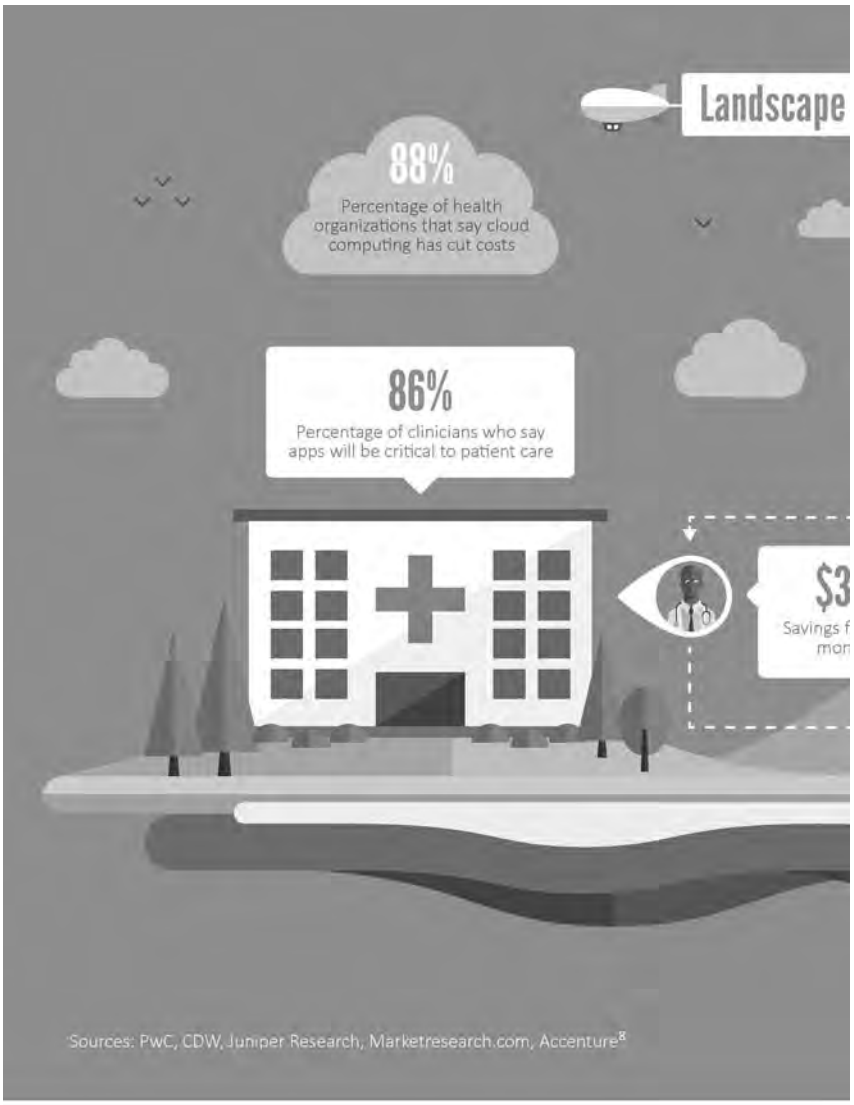
The Microsoft Band includes exercise tracking, guided workouts, and a real-time heart rate monitor

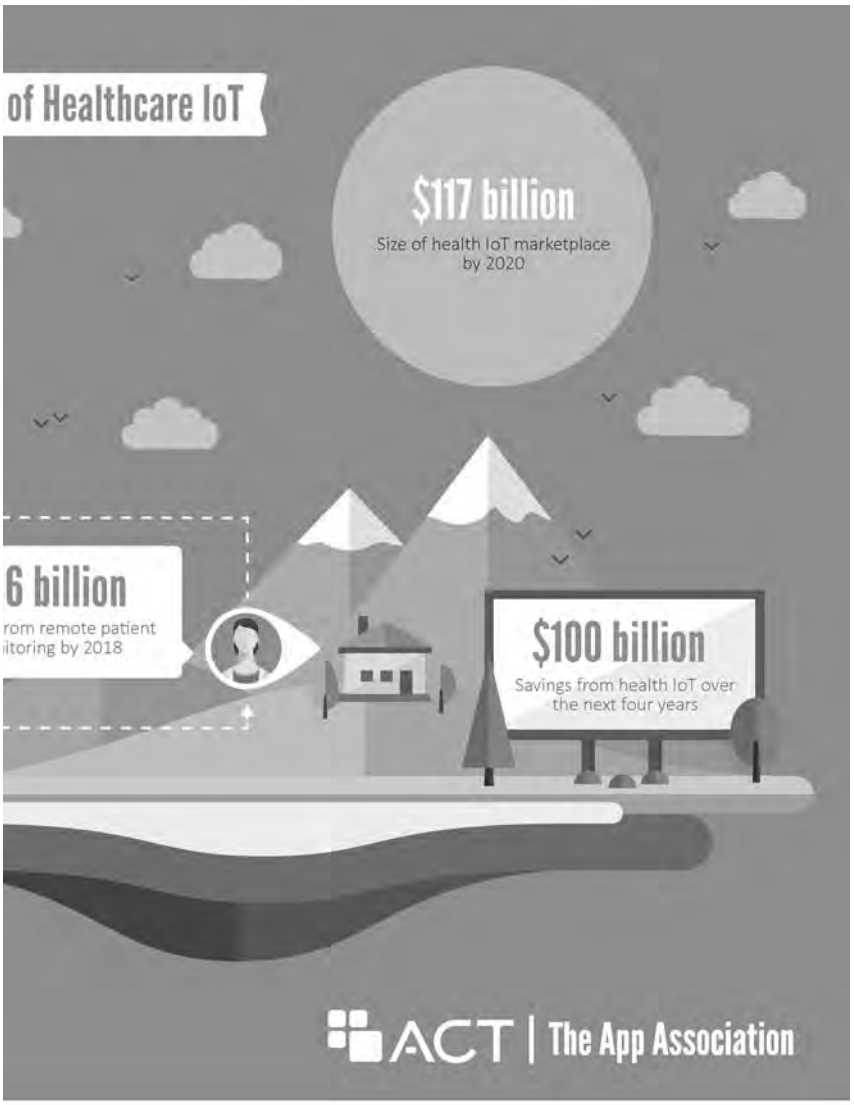
The Apple Watch is packed with sensors that measure movement, heart rate, calories burned, and other vitals

The Netatmo JUNE contains UVA and UVB sensors that precisely measure sun exposure

The MOOV NOW uses motion sensors to analyze and correct a user's form during exercise

Medtronic continuous glucose monitors use sensors embedded under the skin to measure glucose levels every few minutes


Landscape
88%
Percentage of health organizations that say cloud computing has cut costs
86%
Percentage of clinicians who say apps will be critical to patient care
$3
Savings f
mon
Sources: PwC, CDW, Juniper Research, Marketresearch.com, Accenture[8]


of Healthcare IoT
$117 billion
Size of health IoT marketplace by 2020
6 billion
rom remote patient
itoring by 2018
$100 billion
Savings from health IoT over the next four years
ACT | The App Association

Case in point: The aging U.S. population

By 2050, there will be 83.7 million Americans over age 65 – twice the amount from 2012.[9] Eighty percent will have at least one chronic condition.[10] With a large portion living in rural areas or far from loved ones who could offer support, the age group's rapid growth will severely strain public and private health resources.[11]

Advanced personal emergency response systems (PERS) are the key to empowering older populations and helping them live comfortably in their homes years longer than today's norm.

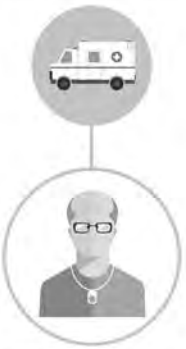
Today, a PERS is typically a single button worn around the neck that directly connects to emergency services when pushed.

A far more sophisticated PERS will be packed with sensors that can track blood sugar, blood pressure, heart rate, biomarkers for medication adherence, geofencing for Alzheimer's patients, and much more. These sensors will be small enough to fit in a watch and will connect to a loved one's phone, a physician's tablet, and a medical record system.

Non-wearables will matter as well, and there are some products already helping our rapidly aging population. The Beddit is a mattress strap that monitors heart rate and sleep patterns.

Even more sophisticated technology, such as the Microsoft Kinect, is used by physical therapists to allow patients to do therapy at home after a knee replacement, while still accurately measuring flex and strength.

This increasingly connected approach to healthcare will lower costs,[12] empower aging populations to live at home longer, and allow physicians and loved ones to help with care in an efficient way. Individuals and their care teams will also have a more complete view of health information, allowing for earlier detection of issues.



PERS of today

PERS of the future

Barriers to health IoT

For this vision of the future to become a reality, there is much work to be done. First, the industry must demonstrate the effectiveness of these technologies. Just as important, innovators must be able to keep sensitive health data private and secure. Lastly, doctors must know that they will be compensated for using these connected solutions.

Our member companies must be able to ensure the security and privacy of sensitive health data to earn the trust of consumers, hospital systems, and care providers. The use of end-to-end encryption is a critical element to accomplishing this.

Recent statements by top law enforcement officials asking companies to weaken security measures threaten that ability. They also reduce the likelihood that health IoT will be implemented in a care setting, and prevent U.S. products from expanding to overseas markets. These requests are coming at the very moment the Office of Personnel Management's (OPM) failure to properly encrypt has led to an incredibly large, potentially harmful, breach. Further, it is in direct conflict with recommendations for encryption of electronic health information by the Department of Health and Human Services (HHS).

Uncertainty around data storage and the cloud is also hampering advancement in IoT. With the grossly outdated Electronic Communications Privacy Act (ECPA) governing electronic data, the law allows for the warrantless search of electronic communications after 180 days – no matter if it's sensitive health information, or private emails.

In the confusion, the U.S. Department of Justice (DOJ) has claimed ECPA gives them the authority to use a warrant to force companies to turn over data of non-U.S. citizens when that data is located outside the United States. This is in stark contrast to the process DOJ goes through to get physical data, creating uncertainty that keeps innovative companies out of the market, therefore hampering advancement in this space.

This problem can't be fixed without action from Congress. The LEADS Act (H.R. 1174) provides the appropriate balance between the needs of law enforcement to conduct criminal investigations and the demand for privacy both at home and by our trading partners overseas.

Having the ability to tell doctors and health systems that a connected health solution is secure, private, and effective is key to moving forward. But, care providers must also know that they will be compensated for the time they spend treating patients using these technologies. There is currently no consistent model for reimbursement around medical devices and apps.

Reimbursing medical practitioners for using connected devices and the data they generate will break down barriers to entry and incentivize companies to go farther, build bigger, and pioneer new things in mobile health. That means better solutions for patients and medical practitioners, reduced healthcare costs, and more opportunities for tech companies.

The pathway to success in the mobile health marketplace requires protecting sensitive information. But for innovators to best achieve this, there must be a commitment from the federal government to update outdated laws, regulation, and guidance.

Conclusion

The internet of things will continue to provide incredible opportunities for innovators. As sensors become more sophisticated, so too will the things in our lives – things that will help lower the cost of healthcare and ultimately improve patient outcomes. We need your help to ensure this future can be a reality for Americans who are eager to embrace connected health solutions.

The success of mobile health is founded on trust. To establish trust, our companies must be able to keep sensitive health data secure and private. While there's currently no legislation on encryption, we ask that you take seriously any government efforts that would require companies to put citizens' data at risk.

Further, we ask that you support the LEADS Act, which would provide clear legal framework for law enforcement agencies to access data stored abroad. It will provide clarity for innovators in this space, and help keep private health data secure.

I thank you again for the opportunity to present testimony about the extraordinary health IoT marketplace. I look forward to our continued work together and pledge our support to help advance measures that promote innovation and foster growth in this space.

End Notes

1 "Connected Health Initiative." Available at: http://connectedhi.com

2 "Internet of Things Market and M2M Communication by Technologies, Platforms and Services (RFID, Sensor Nodes, Gateways, Cloud Management, NFC, ZigBee, SCADA, Software Platform, System Integrators), by M2M Connections and by IoT Components - Global Forecasts to 2019," MarketsandMarkets (November 2014). Available at: http://www.marketsandmarkets.com/Purchase/purchase_report1.asp?id=573.

3 "Digital Health Solutions Expected to Save U.S. Healthcare System More Than $100 Billion Over Next Four Years," Accenture (June 2015). Available at: https://www.accenture.com/us-en/Pages/insight-patient-engagement-colossal-clash-disrupt-infographic.aspx.

4 "HealthVault," Available at: https://account.healthvault.com/us/en-US/Directory.

5 "ResearchKit," Available at: https://www.apple.com/researchkit/.

6 "Physician recommendations of personal health wearables and apps: a channel to drive consumer adoption?" MedPanel (June 2015). Available at: http://medpanel.com/Expert-Insight/Reports-Tools.aspx.

7 "Health wearables: Early days," PWC (2014). Available at: http://www.pwc.com/us/en/health-industries/healthcare-new-entrants/index.jhtml

8 "117 Billion Market For Internet of Things In Healthcare By 2020," MarketResearch.com (April 2015). Available at: http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/?ss=tech; "Issue 2: Making the leap from mobile app to medical device," PwC (2015). Available at: http://www.pwc.com/us/en/health-industries/top-health-industry-issues/mhealth.jhtml; "Remote Patient Monitoring: Can it Be A Solutions to a Key Healthcare Problem?," Juniper Research (2013). Available at: http://www.healthcare-informatics.com/blogs/rajiv-leventhal/remote-patient-monitoring-can-it-be-solution-key-healthcare-problem?page=2; "Top health industry issues of 2015," PwC (December 2014). Available at: http://www.pwc.com/en_US/us/health-industries/top-health-industry-issues/assets/pwc-hri-top-healthcare-issues-2015.pdf; "Digital Health Solutions Expected to Save U.S. Healthcare System More Than $100 Billion Over Next Four Years," Accenture (June 2015). Available at: https://www.accenture.com/us-en/Pages/insight-patient-engagement-colossal-clash-disrupt-infographic.aspx.

9 "An Aging Nation: The Older Population in the United States," United States Census Bureau (May 2014). Available at: http://www.census.gov/prod/2014pubs/p25-1140.pdf.

10 "Healthy Aging: Improving and Extending Quality of Life Among Older Americans," Center for Disease Control and Prevention (2009). Available at: http://www.cdc.gov/nccdphp/publications/aag/pdf/healthy_aging.pdf.

11 "Housing an Aging Rural America: Rural Seniors and their Homes," Housing Assistance Council (October 2014). Available at: http://ruralhome.org/storage/documents/publications/rrreports/ruralseniors2014.pdf.

12 "The Boomer Challenge," Hospitals & Health Networks (January 2014). Available at: http://www.hhnmag.com/Magazine/2014/Jan/cover-story-baby-boomers.

ACT | The App Association
1401 K Street NW Suite 501
Washington DC 20005
202.331.2130 @ACTonline
ACTonline.org /actonline.org

Mr. ISSA. And on that note, I have questions.

I recognize myself for a series of questions.

Mr. Shapiro, you're not an engineer. You're a long recovering lawyer, but I'll ask you this question because I think your industry is well aware of the answer.

As we sit here in air, what percentage, more or less, of the bandwidth are we using in this room, of the entire spectrum?

Mr. SHAPIRO. What percentage as us——

Mr. ISSA. If we are to look at the radio waves being used, the AM, the FM, the old bandwidth from television, what percentage of the spectrum is actually being used as we sit here today?

Mr. SHAPIRO. Well, it's all spoken for, but the actual use is a small percent.

Mr. ISSA. Less than 1 percent will actually be in these air waves. So if we're trying—and I said I wasn't going to dwell too much on spectrum, but if we're trying to create the ability for almost an unlimited amount of communications between large and small devices, isn't one of our greatest tasks to recognize that we have allocated all the bandwidth virtually and not used hardly any of it in any given time in any given room?

Mr. SHAPIRO. Yes. Now I realize you gave me a softball. Thank you.

Mr. ISSA. And you can follow up with devices that can recognize those voids and take advantage of them.

Mr. SHAPIRO. Right. Thank you. So as you know, there are two types. Actually all spectrum is pretty much the same, but we, through the laws, categorize it differently, and we categorize it by whether it's licensed or unlicensed. Licensed means that someone has bought it or they've gotten it for free, a broadcast license, and unlicensed means that, subject to good neighbor rules, anyone can use it.

Unlicensed spectrum is very valuable because it promotes innovation. We calculated, in a study we did last year, that there's about $62 billion of activity created by unlicensed spectrum, so we are advocates for increasing the amount of unlicensed spectrum because it does allow entrepreneurs and innovators to do really cool things that will produce economic activity and provide benefits, but there's a lot of spectrum that the government uses.

And what we're asking, and I know there's legislation pending, which is simply that the government catalog and figure out what could be available and repurposed for commercial purposes because that alone would not only take some of the pressure off a very crowded field right now in spectrum, but it would also create a huge amount of economic activity, and if sold, it will make a tremendous amount of money for the Treasury.

Along the way, though, there is technology being developed which allows spectrum to be split finer and finer and used, and I know that's some of the issues involving going forward, like we are passionate about driverless cars and all the benefits and all the great things that are there, but we think there's an opportunity there to look and test some of that spectrum that's being purposed for that area and split it up a little bit and share it, and that's what Mitch and I love to have wonderful conversations about.

Mr. ISSA. Following up with Mitch. Mr. Bainwol, there's going to be a lot of questions about obviously whether or not automobiles that are communicating with the Internet are safe or not, and that's topical, but would it be fair to say that whether or not you share the bandwidth has virtually nothing to do with whether or not you're going to be effectively hacked on your encrypted signals?

Mr. BAINWOL. That's a question that——

Mr. ISSA. That's a softball.

Mr. BAINWOL. Well, it may be, and like Gary, sometimes I can't see softballs, and I'm also not an engineer. I think I'd say a few things. One is, as it relates to spectrum, we've heard the message from Congress and the notion of sharing, if we can make that work, is something that we really want to do, and field testing is going to happen this year, in 2015, and the notion, is to find a way to satisfy the use for spectrum but also meet safety imperatives is something—that balance has to be struck, and we're prepared to try to test to succeed rather than test to fail, so we're committed to the notion.

I do want to set context, though, in terms of V-to-V. NHTSA estimates that V-to-V could mitigate or eliminate up to 80 percent of all crashes on the road, and so the promise of V-to-V is overwhelming. The implications for life, for injury, for productivity are enormous, so I think the predicate for moving forward has to be do no harm. Move forward aggressively, find a way to share, but do no harm.

Mr. ISSA. And I want to quickly follow up. The history of data in the automobile has been one of the automobile manufacturers having proprietary data buses, keeping them closed, not publishing. As a representative, is that going to be different—and it's a self-asking question or answering question, in the vehicle-to-vehicle world, it has to be an open standard that in fact is published so that your windshield wipers on one vehicle talk efficiently to another; isn't that true?

Mr. BAINWOL. So I think it's both true that interoperability matters, but I think it's also true that in a world, a dangerous world where you have malicious hackers, that system integrity matters a ton, and finding a balance for both is the test.

Mr. ISSA. Well, as I recognize the Ranking Member, I will tell you at least from this part of the dais that working on legislation that makes the penalties specific, high, and enforceable against those who try to maliciously hack automobiles is an area in which I believe our jurisdiction is not only appropriate but our need for action is immediate.

Mr. GARFIELD. If I may add one point.

Mr. ISSA. With Mr. Nadler's permission, yes.

Mr. GARFIELD. It's actually just the point that we have a history of driving open consensus based standards that fully integrate privacy and security protections and can do that in this context as well.

Mr. ISSA. Thank you. Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chairman.

Mr. Shapiro, you argue for a market approach to addressing the privacy and security concerns raised by the Internet of Things. We all hope that companies will act responsibly and that the market

will punish bad actors, but isn't it important that the government set forth clear rules on what is and is not permissible?

Mr. SHAPIRO. Thank you, Congressman Nadler. It is important, I think, that companies know what is legal and not legal, but there is a—something between the two, which is what is right and will get customers or not, and we've heard many people talk about the importance of trust for companies, and their brand and their reputation relies entirely upon trust.

Everyone wants privacy. Look, HIPAA was passed to protect medical privacy, but sometimes there's different types of information and how far it goes, and even HIPAA has some down sides to it. There has been research that's been lost, there's been records which have not transferred easily because of HIPAA, so there's a trade-off that goes on. If you put too much of a line around privacy, you're trading off opportunities for new services that consumers will desire.

I think what companies have an obligation to provide is transparency in what they're offering, and the consumers could be able to make a reasoned decision about what they're willing to give up in return for sharing some of their privacy. So it is, I think, premature for Congress to say this is the line we're drawing, but having the discussion is really important, and I think that there should be a national consensus about what should be protected and what should not and also what consumers should be allowed to give up freely and make that choice.

Mr. NADLER. Should there at least be notice to consumers required?

Mr. SHAPIRO. In terms of giving up what you—if you are sharing something which you shouldn't expect normally to share, I think there should be notice, and it should be clear and conspicuous. I think our companies have an obligation——

Mr. NADLER. So you do think that government should mandate notice?

Mr. SHAPIRO. I think there's a difference—the Federal Trade Commission has some significant jurisdiction in this area. There's a lot of private lawyers who will be more than happy to sue those that don't give sufficient notice. If the law is unclear, which I do not believe it is yet——

Mr. NADLER. So the law is clear enough, the FTC should require notice, and we should leave it at that for the time being?

Mr. SHAPIRO. Well, the FTC is taking a case-by-case approach, which has provided sufficient guidance. I don't think there's a need yet.

Mr. NADLER. Okay. That's what I'm getting at. There's not a need yet for Congress to do anything because the FTC can handle it and is handling it so far.

Mr. SHAPIRO. I think the case-by-case approach is a good approach because this is a quickly evolving area, and before we foreclose new services and new information, all these great things that are happening, rather than jump in, I think we should take a——

Mr. NADLER. Okay.

Mr. SHAPIRO [continuing]. Deep breath and see our consensus.

Mr. NADLER. Let's assume that Congress chooses to disagree with what you just said and chooses to enact privacy and security

measures. In that case, are there any ways in which we should treat products connected to the Internet of Things differently from other companies that collect data or connect to the Internet?

Mr. SHAPIRO. Well, I'd like to think about that answer and perhaps provide it in writing, but my off-the-cuff answer is that I would say the Internet of Things does allow easy connectivity quickly and rapidly, and there is clearly sometimes when knowledge is appropriate and permission, but sometimes there isn't.

For example, the Internet of Things allows police forces to monitor crowds in a public area. It allows them to monitor conversations and see whether people are being angry or not in a public area. It provides an opportunity to have video and see whether there's bad people the FBI wants through identification of not only faces but also by voice. There's a tremendous opportunity here in many different areas.

And to me, what's most important is we let it play out a little bit, and if we're going to legislate—or you're going to legislate; I don't have that right—it would be very specific and narrow and address a real problem.

Mr. NADLER. Thank you. Mr. Bainwol, in your testimony, you reference the consumer privacy protection principles released by the Alliance of Automobile Manufacturers.

Can you briefly describe these principles in some detail? Briefly in detail.

Mr. BAINWOL. Well, the written testimony goes into some depth, but it focuses on things like transparency, context, data minimization, and clearly the notion of express consent for marketing. So we provide heightened protection for things like biometrics, driving behavior, and geolocation.

So we think this works as a floor. We've provided it to the FTC, so it is enforceable, and I think I'd build on Gary's point of—and this applies to privacy and it applies to everything else as we enter an era of massive innovation.

Mr. NADLER. We should be careful and wait for experience.

Mr. BAINWOL. I'm sorry?

Mr. NADLER. We should be careful and wait for experience.

Mr. BAINWOL. Well, I think the fundamental challenge that I've got is that the pace of innovation far outstrips the pace of regulation, and that's just a fundamental truism. We're seeing that in the area of distraction at NHTSA, and I'll give you a specific example.

Mr. NADLER. Well, don't, because I have other questions.

Mr. BAINWOL. Okay. Sorry.

Mr. NADLER. But thank you, but especially given what you just said, do you think that the principles you've enumerated in the consumer privacy protection principles should apply to all prior to the Internet of Things technology or are they uniquely relevant to the automobile industry?

Mr. BAINWOL. Well, they're based on FIPS and pretty generally accepted notions, so I think they're more broadly applicable, but I'm testifying today on behalf of the auto industry, and I'm reluctant to impose my judgment on others.

Mr. GARFIELD. I can give you my perspective on it.

Mr. NADLER. Please.

Mr. GARFIELD. Which is——

Mr. NADLER. That saves me from answering other questions since my time has run out, but go ahead.

Mr. GARFIELD. I'll be brief. We're talking about the Internet of Things as if it's a single thing, but it is not. So what are the privacy or security regime that we would have in place for a windshield wiper versus a watch that's monitoring you personally. So the sectoral approach that we are taking is one that works.

In addition, we shouldn't assume that this is the wild, wild west, and there is no one out there monitoring today. The FTC has been very engaged in this space and is actually taking action.

Mr. REED. I know you're out of time, but if the Chairman will—I want to point out something very important in the health context. I think you are about to see some very significant industry best practices that rise up because ultimately what's happened right now is we aren't seeing the kind of growth.

An interesting study came out that shows that only 15 percent of doctors are talking about wearables to their patients, yet nearly 50 percent of doctors think their patients would benefit from the use of those. When asked as to why——

Mr. NADLER. Why the difference?

Mr. REED. Privacy. The questions that they have about privacy, how it will affect them when the data comes back, and with an aging population that's concerned about how their information might be used for marketing or other purposes, they hate those late night telephone calls, I think that the industry right now is—well, I know. We are working very closely with a lot of folks to come with some industry best practices that give some more bright lines. We believe the FTC will be a good enforcement mechanism for those industry best practices, but that's where we are today.

Mr. NADLER. Thank you very much. My time has expired.

Mr. ISSA. Thank you. And you didn't even get to the questions of what does the garbage man say to the garbage can and what does the garbage can say back.

Mr. NADLER. No, I have to do that in the second round.

Mr. ISSA. I'm assuming it's you stink. That's going to cost me. With that, we go to the gentleman from Pennsylvania, Mr. Marino for his questions.

Mr. MARINO. Thank you, Chairman.

Mr. Garfield, could you—you know, today it's estimated that the average home has 11 WiFi devices. In my house with my tech savvy kids, it's triple that, and I'll give you an example.

My children have a different taste in music than I do, this just happened last week. I am in the study, I'm listening to this music, and the next thing I hear is, Captain Jean Luc Picard's voice saying, "This does not compute." My son found a way to connect into my system and switch the music that I was playing compared to what he wants to play, and tell me that he just didn't like this music, so it's fascinating what these kids can do with this equipment.

But be that as it may, you know, this unprecedented boom will require significantly more wireless spectrum, I think beyond what we realize at this point, that is commercially available today. Could you expand on the implications of how this might impact the con-

nection for consumers as well as the overall growth of the sector of the economy?

Mr. GARFIELD. Yeah, I think both are significant. Your household actually sounds a lot like mine, so I empathize with you. I agree with what my colleagues have said about the need for more spectrum, whether it's wireless or wireline or whether it's licensed or unlicensed. In this context, wireless is particularly important.

Given the lack of optimization in the use of spectrum today and how much spectrum is held by the government, I think there's a significant opportunity both in the deployment of IoT and economically as well to more efficiently use spectrum and make more of it available, and so I think there's a huge opportunity there.

The reality is that it's absolutely necessary because as we think about all of the physical world essentially being digitized, then the growth that we've experienced today in the use of spectrum will certainly explode, and so it's something that we need to plan for, anticipate, and take action to deal with.

Thank you. We realize now that I can raise my garage door up and down from 2,000 miles away. I can turn my lights on. But what is to prevent the hacker, the state-of-the-art thief from checking in on my software on my computer system in my house? For example, when I go on vacation, I will turn the heat down. So they could tap into my thermostat, read when the heat is reduced over a certain period of time, come to the conclusion even though there are lights going on and off all over the house that no one is there. And this is open to anyone. What is the industry doing to protect us from that?

Mr. REED. First of all, thank you for your question, and thank you for your work on a lot of the encryption and privacy issues, Congressman. First off, welcome to encryption. End-to-end encryption is a critical element of preventing that from happening. Yes, there are technological things you can do, man in the middle, et cetera, forms of attacks that we can run. But, you know what, once you start getting about 256-bit encryption, 512-bit encryption, it takes an enormous amount of power to break it.

So one of the questions that the consumer electronics side of the world, as well as the cloud computing side of the world is looking at is, how do I put end-to-end encryption in every device and make it so no one can mess with your lights, or more importantly, other things in your house that might have a direct impact on the people living there.

So first off, we need to make sure the government doesn't weaken encryption. Second of all, we need to continue to see the growth in the kinds of research around encryption that is in some cases supported by the government.

Mr. MARINO. Yeah. Anyone else?

Mr. SHAPIRO. Can I answer that?

Mr. MARINO. Yes, sir.

Mr. SHAPIRO. I share Mr. Reed's comments. Also, going back to the garage door opener, when that was first introduced it was very primitive. And a fun thing to do, was to drive around the neighborhood and open up other people's garage doors, or similarly with cordless telephones. If you played it right, you could listen to other people's phone conversations because it was so, by today's stand-

ards, relatively primitive even though it was novel then. As we have gotten more sophisticated, as memory chips have grown, as encryption has grown, there are solutions and we don't even hear about those problems anymore so it has not been an issue.

Mr. MARINO. Okay. Thank you.

Mr. GARFIELD. The reality is, is that a significant investment is being made in innovating around privacy and security because it's the right thing to do and because consumers are demanding it. So that explains, in part, the shift that you have seen that both Gary, Mr. Shapiro and Mr. Reed have articulated.

Mr. MARINO. Okay, just let me know when you have a device where I can block my son from changing my music as——

Mr. REED. I can help you with that.

Mr. MARINO. Thank you. I yield back.

Mr. SHAPIRO. It is called handcuffs.

Mr. REED. Wow, that is primitive. Yes.

Mr. ISSA. Mr. Marino, did you get to your question of the launching of your trade secrets bill today?

Mr. MARINO. Here?

Mr. ISSA. No, you didn't. Okay. Well, Mr. Collins will be announcing it, so hopefully you will get to talk on that next.

I'm sorry, did I mention that there will be an announcement on trade secrets bill today? Okay. Did anyone not hear that? Thank you.

We now go to the gentlelady from California, Ms. Chu.

Ms. CHU. Mr. Bainwol, I recently read an article about two security researchers that were able to wirelessly hack into a Jeep Cherokee, first taking control of the entertainment system and windshield wipers, and then disabling the accelerator. They were able to slow down the car to stop on a busy highway. This experience reminds us that connectedness flows in both directions and that hackers could actually manipulate these devices for evil if they so chose.

What specific best practices does the industry have in place to ensure that something like this does not come about and how are automobiles being designed to prevent exactly this from happening? And what role do you see the Federal Government playing in this scenario?

Mr. BAINWOL. And I have 5 minutes? Great questions, and the Jeep hack of a week or two ago, obviously, received enormous national attention. I'm struck here about the need to both take the threat very seriously, and we do, but also not to get caught up in the sensationalism that sometimes accompanies a story like this. So both things are true.

Our companies are designing and building to meet security risks from the very start. That's point one. They are working with government, with academia, with third-party security technologists to address the hack risk, and the hack risk is real. It's palpable, and we need to address it and we need to take it very seriously. We have also formed an ISAC, and this began more than a year ago. And the ISAC is a mechanism for the industry to voluntarily share risk and how to address those risks. So there is a mechanism that is in formation for specifically this challenge.

The risk here from a governmental side is the one that we touched on before, and that's what's the touch? How heavy a touch should there be? And in a world in which innovations happen so rapidly, how do you make it work so that it is not rigid? And that's a challenge. I think what you have done thus far is to facilitate sharing of risk threat and that's great and we hope that moves forward.

Ms. CHU. Okay, Mr. Garfield, you stated that connectivity and communications between vehicles must be secure and reliable, especially for safety applications. That's something that Congress, the Department of Transportation, the Federal Trade Commission and other government stakeholders should oversee to protect consumers. You are referring there to the consumer's physical safety.

But when it comes to another kind of safety, which is privacy, and data security, you urge the Federal Government to essentially take a wait-and-see approach, and asking that if we should only step in, if industry fails at self-governance. So what in your mind is the difference between these two kinds of safety that would warrant such a divergent approach?

Mr. GARFIELD. I guess two points. Our suggestion is not that the government do nothing. Our suggestion is that the government exercise restraint, and that the approach that has been taken today on privacy, that is sectorially driven, that includes monitoring and enforcement by the FTC is working. In the first instance, there is a significant market failure that may not be being met and so immediate action is clear. In the second instance, that is less clear. I guess the third and final point is the point that we have all made about the innovation that's taking place in this space, not only around IoT, but around ensuring that we are driving privacy and security by design at the very beginning of these processes is actually making significant headway and we worry about the unintended consequences of legislation at this stage.

Ms. CHU. Mr. Shapiro, you acknowledge in your testimony several important concerns about privacy and the collection of data, and then go on to state that industry-driven solutions are the best way to promote innovation. But how do we rely on the industry to self-govern, and avoid the problems implicit in the fox guarding the henhouse? And I ask the question particularly in the context of one concern you raised which is, who owns the data from these devices? Isn't the industry incentivized to claim ownership over the data?

Mr. SHAPIRO. Thank you for that question. It is true that a lot is going on vertically. We have our own wireless health company group that is focusing on creating rules that everyone can live by. In part, because it's the right thing to do; in part because there's Congress, which will probably or a government agency will do it if they don't. But there are already free-market solutions which are happening quickly in different other verticals.

For example, in the automobile, hundreds of thousands, if not millions of consumers are already choosing to give up their data to insurance companies in return for a lower insurance rate. So the insurance company is essentially monitoring how fast they drive and what they do and what kind of driving they do because the consumers feel it is valuable to give up that information. That's informed consent. It's a free market decision, et cetera.

Also there's solutions coming up for parents. If they want to give the kid the keys to the car, they have the ability to monitor their children now with many different solutions that are coming out quickly.

My point is not that it is not a legitimate area for government conversation. It's that there's so much happening from an innovation point of view, that there's different directions that we can go in. And if industry goes in the wrong direction, we are fully confident that the government will be there saying this is wrong, and consumers will be there, trial lawyers will be there. Even in the distracted driving area where the Federal Government has stepped in rather vociferously and said to industry, you know, you should really do everything you can to ban a driver from using any product while in that driver's seat. There's at least 80 different solutions and more developing every day which basically cut down on distracted driving through monitoring lanes, through monitoring the head falling asleep, watching your eyes, or even technology produced locally which monitors your cell phone as a driver and figures out if you are not paying attention to the road.

Mr. ISSA. Would the gentlelady yield for just a followup question very quickly?

Ms. CHU. Certainly.

Mr. ISSA. I think, Ms. Chu's question, though, was who owns the data? And wouldn't you agree that, in fact, data which comes from an individual inherently government does have a role in defining what rights they have to retain, protect, or retrieve their own personally identifiable data, which I think was your question, wasn't it?

Ms. CHU. That's true.

Mr. SHAPIRO. Well, then I blew the answer.

Mr. ISSA. It was a good answer, it just wasn't quite to that question.

Mr. SHAPIRO. I would say, obviously, a consumer that creates data should have some rights in that data. The question is the service provider, if they do own data. And this goes into a lot of areas of the Internet and not just the Internet of Things. If there are apps providing services, et cetera, what is the tradeoff that's involved? And I think it's fair to say there should be transparency as to who is using the data. As to who actually owns it and can retain it, I guess I would say that depends on the level of personal information in the data. I think whether or not you are using your windshield wipers, for example, is a type of data that can be easily collected and shared to provide information on where it's raining without a lot of consumers saying that's fine, as opposed to something much more personal when you get into the health sphere where you should, of course, own and determine what happens with your data.

Mr. ISSA. Thank you. I think that will at least start a dialogue that will continue. The gentleman from Texas. Mr. Poe.

Mr. POE. I thank the Chairman. Gentlemen, thank you for being here. I'm going to try to break this down and try to keep it less complex, very simple. The issue is privacy. The time of the Dick Tracy watch is here. In fact, our gentleman here on the end has

two Dick Tracy watches. I don't even wear a watch, so that will help you in the answers, I hope.

Mr. ISSA. Ted, what time is it?

Mr. POE. It's up there and I can't even see the clock. So anyway, the data that is stored, is stored by a provider and it's information about an individual. The privacy of that individual is paramount to me, and I think the law, the Constitution, the right of privacy.

And it has to be protected by Congress because it's a constitutional right. Privacy. Congress needs to set the expectation of privacy for individuals that have shared their information with different entities, and I'm concerned about the privacy of the individual two ways: One, the provider or the service provider sharing it with other nongovernment agencies. And the service provider providing that information to the government. Especially the government. I think there should be—we should update the ECPA law, which right now, information stored on the cloud for 6 months is private. But 6 months and 1 day, the government can have it. There is no expectation of privacy; absurd protection of the constitutional right of privacy for 180 days only.

I don't think that we should leave it up to the FTC to set the guidelines or the FCC, or the FEC, or any other government agency to determine what the right of privacy should be.

So I'm not through asking the question yet. So how do you know the answer already? Anyway, should not we in Congress update the ECPA law to provide whatever rules we think should be provided so that citizens know that the government, to get this information, and you can use geolocation and all other information, has got to have a search warrant based on the Fourth Amendment of the Constitution before they order you to give the government that information about the citizens out there in the fruited plain.

Shouldn't we be proactive to do that, or are you recommending that we just wait for all of these different things to happen out there, and try to solve them, get the lawyers to sue and all of these things before we get the right of privacy, or should Congress be proactive? I have been working on this for years, and we haven't been able to get anywhere with updating the ECPA law so that people know the expectation of privacy that the government knows you cannot get that information without a search warrant. Should not we do that, Congress do that? And it's kind of like a yes or no answer on that.

Mr. REED. Yeah, the reason I was coming in there is because I wanted to say amen. The reality of the situation is, yes, ECPA reform is absolutely essential; 289 cosponsors. This is something the Committee absolutely has to do.

Congressman Marino was here, Congresswoman DelBene is here as well with the LEADS Act that you cosponsor. We absolutely need these kinds of legislation to move forward so we know what we can tell our customers, what I will protect, how I will protect it, and when I will be forced to share it. Absolutely.

Mr. POE. And a person may not be a customer for this very reason. Well, I like all this stuff out there. This is wonderful, but I don't want the government getting it. And right now you say, well, then maybe they can have it, maybe they can't have it. How about the rest of you?

Mr. REED. Yes.

Mr. POE. Got an amen here on the right. Good.

Mr. GARFIELD. We support ECPA reform; strongly support ECPA reform.

Mr. SHAPIRO. I think you are totally right to distinguish between what government has a right to, and what private parties can exchange with each other. So when the government says we have been burned as an industry pretty seriously to the tunes of billions of dollars of sales in Europe, and other countries are using the fact that our government took information, is a total competitive disadvantage now to say that cloud servers and things like that should not be based in the United States, you know, that they are not secure, government can take the information and it has been very harmful to the U.S. technology industry and it has been used against us.

And under the Fourth Amendment, yes, it is about as clear in the Constitution as you can get about the government must have only—will not do unreasonable searches and seizures, and that's been interpreted—ECPA needs an update. I agree with that.

On a private basis, I think it's a much more complex discussion. The reasonable expectation of privacy is set by the Supreme Court, is almost like the definition of obscenity in a way. It changes with time. It changes with community, and it changes with technology. And I think your reasonable expectation of privacy in some data, if you are out in public and I'll use the windshield wiper example again, is not perhaps the same as perhaps other data, and that's a much longer conversation.

Mr. POE. In the privacy era, it goes into whether it's voluntary, whether you volunteer to give that information to another person. And that's a different—I'm interested about the government, the Federal Government, State government, local government, which all right now can seize that information in the cloud without a warrant. And the person involved doesn't have notice about it. One more comment.

Mr. BAINWOL. I'm in on the government side. I would note, as Gary indicated, and this is on the nongovernmental side, that data is necessary to provide services that consumers want. So whether it's the insurance example, we plug in, I'm one of those consumers. I know exactly how my kids drive because I get a report every month from the insurance company that tells me how fast they are driving, how fast they are braking, when they are driving. And as a parent, that's a useful thing and it's a disincentive for them to drive poorly. So that's a good thing, and I wouldn't want to get in the way of services like that that are pro-consumer.

Mr. POE. All right. I yield back to the Chairman.

Mr. ISSA. I thank the gentleman, and we now go to the gentlelady from Washington's First District, Ms. DelBene.

Ms. DELBENE. Thank you, Mr. Chair. Thanks to all of you for being here. I want to follow up a little bit on the Electronics Communications Privacy Act conversation here. Myself and Congressman Poe and Congresswoman Lofgren have also sponsored legislation that would also create a warrant standard for geolocation information as well as electronic communications.

And when we talk about issues of making sure there's a legal framework to protect information, and so that consumers feel like they understand what's happening with their information, and law enforcement is clear on how they would access information, what do you think about expanding that to include geolocation and the international issues that we face in terms of access to information? Anyone? Or I guess I will start with Mr. Reed.

Mr. REED. Well, first of all, thank you for your support of the LEADS Act. Thank you for your introduction. It's a very valuable thing to figure out how we move forward. I know we are all Americans here and we are in America, but one of the things to realize from my members who are developing the applications, is just how much our opportunities are overseas.

And so when the issues that you raise about U.S. Government access to that data start harming our sales, it hurts jobs here in the United States. So I think you're precisely right. This is an issue that Congress has to step in on. It can't be done through industry best practices or standards. And so the question of geolocation, once again, is something that we will have to work both with you and with law enforcement because law enforcement does have a duty to work and protect the citizenry.

The problem comes when I have to tell a customer, I don't know about the answer to the question of when I have to hand over that information. The difference between the Sixth Circuit and the Ninth Circuit and this idea that I have to tell my customer I don't know, is enormous.

I think the other element that should be raised on this is how other countries look at what's happening.

If the United States Government says we have access to any cloud data, at any time, on any person, any way we darn well please, regardless of where the data is stored or who it's on, we have to expect that Russia will want the same privileges from our companies; that China will want the same privileges from our companies. And so legislation like what you're proposing is what we need because we need to have a strong stance that we can look at those countries and say, no, I won't hand over that information without some better legal authority. So thank you very much.

Ms. DELBENE. Mr. Garfield.

Mr. GARFIELD. Yes, your question also gives us another opportunity to raise something that Congress can do in this area which is legal redress. The lack of legal redress rights in the United States is something that creates great challenges internationally, and this Committee and Congress generally has the opportunity to do something and so that's another step that can be taken that would help internationally.

Ms. DELBENE. Folks, also, you were earlier talking about encryption, and we have been having a conversation recently about whether there should be a backdoor for law enforcement access to encrypted data, and whether that should be mandated. If such a policy were mandated by the Federal Government, what would, you know, the impact be specifically on user data and what do you think the impact would be for your customers?

Mr. GARFIELD. I think the impact would be quite negative both here and internationally for a host of reasons. It's important to

keep in mind that security is a part of advancing privacy. And if you create any kind of door, it won't only be used by those who you intend it to be used by. And so I think in many respects you create a Pandora's Box of challenges that would be highly problematic for both privacy and security interest and is something that should absolutely not be done.

Mr. Bainwol and I both worked in the recording industry years ago, and one of the things we realized was rather than fighting technology, the best solution is to poyne the use of technology, and I would suggest for the Federal agencies in this context, those answers may hold some merit in this context as well.

Mr. REED. We learned hard lessons. I feel like we are a little bit of deja vu right now with the Clipper Chip reducts here that we are facing. The reality is is that over 40 of the leading security experts have already come out and said, the idea of the government mandating or creating a, as the FBI director said, a front door into our devices and our systems, is an anathema to the idea that we want to create by telling our customers and our users that we have secure systems. So we have done this dance before. It was already figured out to be a mistake. I'm disappointed that we are having to revisit it again when we know the answer. And that is, end-to-end encryption with as few openings as possible is the best solution we can provide to all citizens in every country.

Ms. DELBENE. As you may know, we have a piece of legislation to prevent there from being such a backdoor.

Mr. Shapiro, did you want to add something?

Mr. SHAPIRO. Yeah, I think we are all Americans and we sympathize with law enforcement in what they are trying to do and so it is a different question. It is not that black and white. But I think history has shown that having given government a backdoor is not the best approach as technologies evolve quickly.

On the other hand, as Americans, when a super crisis evolves, I think you will see companies step up and try to help government. I think we saw it in Boston in the bombing where technology companies worked very closely to try to find out who it was that did this dastardly act, and I think we have to recognize there's some flexibility and does not require an act of Congress to say that there must be a backdoor. If there is a backdoor and everyone must have it, it gets not only having the technology industry very uncomfortable, but our consumers very uncomfortable.

Ms. DELBENE. Thank you. My time is expired. I yield back, Mr. Chair.

Mr. ISSA. I thank the gentlelady and I thank her for her important questions. With that, we go to the gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman. Thank you for hosting this very important hearing.

Mr. Garfield, your testimony mentioned the desire of the industry to be free from new regulation without becoming a wild west of privacy. Earlier this year the Federal Trade Commission reinforced this message in its staff report on the Internet of Things, where it recommended, among other things, that companies build privacy and security into the designs of their connected devices.

Last Congress I introduced the APPS Act, a commonsense approach to an urgent problem that would protect consumers without disrupting functionality or innovation through a safe harbor, and other mechanisms to promote trust through self-regulation. I viewed this legislation as reinforcing of the FTC staff recommendations on privacy and security for connected devices, and I plan to reintroduce the APPS Act during this current session of Congress.

Privacy is an issue that should unite us, not drive us apart. In an always-on ecosystem where over 25 billion connected devices store and transmit information about consumers, it's time that we have some rules of the road. What steps will private industry take to keep Congress informed and address legislative concerns regarding security and privacy of these emerging technologies?

Mr. GARFIELD. Thank you for your question, Congressman Johnson. The point you made at the beginning about the FTC's recommendations, particularly around privacy and security by design, I think are, in fact, is occurring. The industry is spending billions to invest and innovate around privacy and security, in part, because it's the right thing to do, but also because consumers are demanding it.

As well, we are advancing, as Mr. Bainwol pointed out, sector-specific principles around privacy and security as well. And so there is much action happening right now in this space and we are committed to making sure that Congress is fully aware of the steps that the private sector is taking to advance those issues. It is in our business interest to be aligned with both you and consumer interest around these issues.

Mr. JOHNSON. Thank you. Mr. Bainwol, I want to focus on the portion of your testimony regarding advanced driver assistance systems. I understand the benefits that you're explaining about these systems, the sensors that provide braking assist, and adaptive cruise control. I understand newer software will go far beyond just those actions. My concern revolves around the encryption of this technology. If these systems are being operated on a broad range of wireless communication technologies between vehicles, how are these frequencies being protected?

Mr. BAINWOL. I will give you an answer, and I will come back to you with a vetted engineer's answer. So V-to-V is based on DSRC which is a technology that was built for the purposes of communications between vehicles. And I will come back to you again with the specifics of the security that is embedded in that.

We are obviously not at a point of full deployment. This is being tested. There has been an expansive test out of Ann Arbor over the last several years. It has been tested abroad. And the fundamental point I would make is that the benefit stream here, if you do a cost-benefit analysis here, the benefit stream is absolutely enormous. And yes, we have got to address the cyber risks and the security risks, and they are being dealt with from the design phase on up. But in terms of the security embedded in DSRC, I will have to come back to you.

[The response from Mr. Bainwol follows:]

Hearing on Internet of Things
July 29, 2015
Mr. Mitch Bainwol, President and CEO, Alliance of Automobile Manufacturers

Johnson: My concern revolves around the encryption of advanced driver assist systems / technology. If these systems are being operated on a broad range of wireless communication technologies between vehicles, how are these frequencies being protected..?

Vehicle to vehicle or vehicle to infrastructure technologies are based off of what is called Dedicated Short Range Communications (DSRC). These are communications are one-way or two-way short-range to medium-range wireless communication channels specifically designed for vehicles to communicate between each other and with infrastructure. These communications occur every tenth of a second and are constantly changing. DSRC broadcast messages, like the Basic Safety Message, or intersection map and signal state messages, are not encrypted. The information is not secret. The sender wants every other device close by to hear and use the information so that an accident can be avoided or traffic can be mitigated.

Mr. JOHNSON. Okay, if end-to-end encryption is being utilized, how will law enforcement access the information stored within a vehicle? Do you have an answer to that question?

Mr. BAINWOL. So we would require a warrant of some sort. This is, again, this is the point that Mr. Poe was making earlier.

Mr. JOHNSON. Okay, I'm sorry, go ahead.

Mr. BAINWOL. And so we are very careful and our principles articulate very specifically that the information will not be shared with entities unless there's a compelling, specific reason.

Mr. JOHNSON. But there will be an ability to counter the encryption or to kind of a backdoor, if you will, for lack of a better term.

Mr. BAINWOL. Yeah, I'm going to have—I'm not an engineer, and this is a zone that I'm not going to be able to give you a great specific answer on, so let me come back to you in writing shortly.

[The response from Mr. Bainwol follows:]

Hearing on Internet of Things
July 29, 2015
Mr. Mitch Bainwol, President and CEO, Alliance of Automobile Manufacturers

Johnson: If end to end encryption is being utilized, how will law enforcement access the information stored within a vehicle? Will there be an ability to counter the encryption..?

DSRC communications are not stored in any location or within the vehicle. Data communicated is used for a brief time period by vehicles and infrastructure to provide short term information. Short term information is, for example, distance measurements used to determine time to a potential collision with another vehicle, which is used by a crash avoidance application in real time to send a driver a warning. The crash avoidance data is then released and erased, not retained and encrypted. Once the vehicle has changed locations then new information is received and released. This information process continues to occur as the vehicle travels from one location to the other.

Mr. JOHNSON. All right, thank you. And I yield back.

Mr. ISSA. I thank the gentleman. You know, I have had two of you gentlemen tell me about how you are not engineers, but I want

to talk about something for a moment that's a little complex, and then make it simple.

In the aviation space, collision avoidance of all sorts has been around for a long time. It started with the large commercial scheduled aircraft and then little by little has come down. One of those technologies, ADS-B is, in fact, mandated now in just a few years for all aircraft. And it's a cute name, I have said it forever, but now I have to say it's automatic dependent surveillance broadcast, ADS-B, or ADS-B out.

Now, that technology, in short, says, here is where I am, and it sends it out to everybody. The FAA regulates it. Other aircraft while they are sending out where they are, receive where you are. It makes for a very exact GPS-based within a few feet of knowing exactly where you are, and of course, which way you are going, how fast, making a collision almost an impossible thing to do if you're simply monitoring the product which has alerts.

The question and I want to make sure I ask it to Mr. Bainwol and others, when the FAA, having jurisdiction over this, they made a decision that only those who send out a signal can, in fact, receive a signal. So today, systems that cost anywhere from 6- at the very low end, plus installation, to hundreds of thousands of dollars, equipped in aircraft, they communicate by sending out and receiving information where others are.

Mobile devices, devices that could be bought for a matter of a few hundred dollars that only receive are blocked from receiving that information. Meaning that as you roll out a new technology, and Mr. Bainwol, clearly these kinds of technologies are what big auto is looking at rolling out, countless millions of automobiles will not be equipped with those systems for decades to come. The 1965 Mustang or any of the classic cars that Congressman Juan Vargas has, will not ever been equipped with them.

Can you comment on the need to make sure that any standard allows for aftermarket retrofitting of products that to the greatest extent possible enjoy the benefits of newer technology brought to market in new automobiles?

Mr. BAINWOL. I'm happy to comment. There is a challenge in the auto space with fleet penetration. The average age of a car is 11 years old. So when you introduce a new technology, it takes a long time to wind it's way through the entire fleet.

Mr. ISSA. Not with Mr. Shapiro's aftermarket products.

Mr. BAINWOL. So, in the example of antilock braking, it took 30 years to go from introduction to 95 percent penetration. So you're point about fleet, penetration I think, is a valid one.

And in the case of these technologies that offer such value to society, I think you raise a legitimate point that we have to find a way to fill the gap now. The truth of the matter is, in part that gap is filled with this phone that Gary peddles so brilliantly. Just to give you an example——

Mr. ISSA. I'm not sure Gary wants to be called a peddler, but he appreciates you calling many of his members peddlers.

Mr. BAINWOL. So Waze is a wonderful app, okay, and it's crowdsource based, and it provides many of the benefits that V-to-V provides, but not with the same absolute standard of certainty. So we have got to find a way to fulfill the marketplace. And I think the

app world does a good job of bridging that, and then ultimately to fill the fleet. And so I think your point is a valid one and we have got to find a way to make it work.

Mr. ISSA. Thank you, and Gary, just Mr. Shapiro, the question more was as new innovative items come out of the OEM market and new fleet, and there's an ability to get, perhaps, some but not all of those benefits, government, at least in the case of aviation, has blocked the ability of thousands of small pilots, pilots with a Piper Cub made before you and I were born, in which your mobile device can be put on board today are blocked from knowing that there's a fast mover heading for them because the FAA has saw fit to block it unless you are sending a signal. That's really the question of enabling as much benefit from potentially low-cost handheld devices.

Mr. SHAPIRO. Mr. Chairman, as a member of the flying public, I never quite understood that decision, and I'm glad that it's being rectified and albeit after dozens of years.

Mr. ISSA. It is being rectified. All aircraft in a matter of a few years will have ABS, or I'm sorry, ADS out. However, today somebody can carry a few hundred dollar product and if it were allowed to receive the signal, they would be part of knowing where a fast mover is, and avoiding it even if they are not putting out that signal.

Mr. SHAPIRO. Well, I am thrilled to hear you are focusing on it because I fly almost every other day, but——

Mr. ISSA. And the Cessna 150 needs to know.

Mr. SHAPIRO. Sir, the reason I have been so excited for years about driverless cars is the level of death and injury that's caused by cars is so huge, and of course we all drive them, they are necessary.

But it can be avoided. We are on the verge of this technology and several car companies and Google have proven it. And it would be an absolute tragedy if it was delayed in any way because an aftermarket was not allowed to develop to move it along. And I think that you are absolutely correct in indicating that we will get there in two different ways: One, the car manufacturers themselves will do everything they can to get this technology in the public hands, but along the way as we have seen with almost every other automotive technology, including I might add, car security, the aftermarket is quicker. It can get greater penetration and provide competition.

And what my concern is about some of the privacy discussions is when it comes to matters of losing your limb and losing your life which is what we are talking about with collisions in cars, it is a little less important to have privacy than it is in some other areas. So the privacy discussion is important. I don't want to denigrate it, but when it comes time to our physical safety, it takes a backseat.

Mr. BAINWOL. I just need to address——

Mr. ISSA. Mr. Bainwol, just remember, the two of you did take a picture earlier standing next to each other smiling.

Mr. BAINWOL. This is not to contradict Gary, but just to clarify. So Gary used the words about fatalities in cars as the cars are killing people. I just want to clarify, 95 percent, maybe 98 percent, maybe 99 percent of the fatalities on the road are a result of both

environmental challenges and human error. The car itself works rather beautifully, and the critical point that we would both embrace, is that——

Mr. ISSA. I certainly think Mr. Shapiro was talking about antilock brakes, traction control, all of the items that have come out that have reduced the death rate in all-too-flawed drivers.

Mr. BAINWOL. We are very proud of those technologies. We want to see them move into the fleet as rapidly as possible, and those technologies are the answer to human error which is a huge problem.

Mr. ISSA. Thank you. And Mr. Reed, since you were given credit for the development of those apps, your members wanting to be able to develop apps depend on either an open standard or in the alternative, being able to, if you will, hack in order to create interfaces because otherwise you're locked out of interfaces with the automobile and other products. Isn't that true?

Mr. REED. So open standard would be a significant part of how this moves forward.

Mr. ISSA. Or published standards.

Mr. REED. But I also think you will end up with published standards, and you will also end up with what I believe will be interfaces where I won't have to hack it. There is the connotation to hack which is a little odd.

What will end up happening is, is that APIs will be published by the car manufacturers that will allow me to the tie into the existing system, or I will do it through the phone, and the phone manufacturer will have done a deal with the auto dealer and then I will have a secure, safe, API platform that I can build out the apps on.

So I'm actually quite hopeful about the connected car. And I think that's a place where you are going to see an explosion of apps that will be really helpful and beneficial, especially those with kids in the back seat.

Mr. ISSA. Well, earlier on I mentioned in the opening statement that we do not have in this Committee the jurisdiction over the bandwidth necessary for many of your products. We do, however, have a mandated seat at the table in consultation with the Ways and Means Committee and with the Administration in trade. Under Trade Promotion Authority for both the European trade and the TPP in the Pacific.

I would like any of you that want to comment on the importance of global standards of getting the Internet of Things to, in fact, be embraced in a way around the world that allows either for economy of scale, or consistency of service, and I will go right down the line on that. Mr. Shapiro.

Mr. SHAPIRO. Global standards are nice, but they are not essential. We have seen in technology that politics and ego often play as to whose country's standards, you know, there's several——

Mr. ISSA. I wasn't necessarily only talking about standards. I was also talking about the access that trade promotion is intended to have, the acceptance without tariff for barrier of American products.

Mr. SHAPIRO. Okay. So standards is one issue, but the fact is, is that trade promotion is good. The ITA is great. We are very excited with the direction things have taken in the last month. It's posi-

tive. Obviously, to the extent that these devices get out there, and they are improving people's lives and saving lives, it is an important thing.

If there's an international low tariff approach, that's always preferred to one which is country-by-country, high tariff.

Mr. ISSA. Mr. Garfield.

Mr. GARFIELD. I think the opportunity that you highlighted, that trade agreements provide for driving global consensus-based standards that help to advance scaleability and interoperability, are a net positive; hence, our strong support for Trade Promotion Authority and ultimately the trade deals that will emanate as a result of that.

Mr. BAINWOL. With a complex blend of membership, sometimes trade gets tricky for me. But I would say——

Mr. ISSA. Some of your members are for it, and some are against it, and you are with your members?

Mr. BAINWOL. It's more complicated than that. But the notion of harmonization is absolutely a valid one.

Harmonization has been around for 100 years as a concept, but we are building to different standards all around the globe, and that ends up upping the cost of the product for consumers all over.

And a new car is safer than an old car so we can reduce the cost of a product through harmonization. We are getting more people into newer cars and that's safer and that's good for everybody.

Mr. REED. Two quick points. Every single one of your Members of this Committee has a company in their district that is selling an app overseas. Guaranteed. We see about 20 percent of all the apps in China, are actually from U.S. companies, which is huge. If you pay attention to the China market it's hard, which brings me to the second part.

Our one concern about standards is that we are finding some countries are dipping their toe into the idea of creating quote-unquote, "domestic open standards" that are slightly tweaked from the United States, and these are strictly barriers that they are putting up to protect domestic manufacturers, domestic app developers. We have seen it in the WiFi space, around the globe. We are seeing tweaks to standards strictly to protect domestic production.

And so we would support your perspective on improving trade and improving those standards so that they are available to all.

Mr. ISSA. Thank you. And on that note, with no further questions, this will conclude today's hearing.

I want to thank all our witnesses. Without objection, Members will have 5 legislative days to submit additional written questions for the witnesses, and additional materials for the record. That also leaves our witnesses 5 days, if you could please, to provide additional material, including that which some of you promised to give to our Members. And with that, we stand adjourned.

[Whereupon, at 11:42 a.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

NATIONAL ASSOCIATION OF Manufacturers

Brian J. Raymond
Director
Technology Policy

July 29, 2015

The Honorable Darrell Issa (R-CA)
Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

The Honorable Jerrold Nadler (D-NY)
Ranking Member
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Issa and Ranking Member Nadler,

On behalf of the more than 14,000 members of the National Association of Manufacturers (NAM), the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states, I write to thank you for your attention to a transformative force in today's manufacturing environment, the Internet of Things.

Once a tool accessible only through our personal computers, the Internet has seamlessly integrated into every aspect of our daily lives. The growth of wireless networks and broadband systems capable of transmitting tremendous amounts of data keep us constantly connected. So do handheld devices whose capabilities seemed unimaginable just a decade ago.

This nexus of exciting technologies has given us the "Internet of Things" (IoT) – the interconnectivity of devices of all kinds that has resulted from secure network connectivity, wireless technology, security and cloud infrastructure. As PTC President & CEO James E. Heppelmann and renowned Harvard Business School Professor Michael E. Porter recently wrote, "Smart, connected products are changing how value is created for customers, how companies compete, and the boundaries of competition itself."

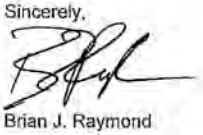
By leveraging technology, production line activities, plant security safeguards and monitoring, product performance and reliability, customer needs, inventory and raw materials management and shipping logistics can all be managed using technical tools and infrastructure.

Government and industry must work together to develop a strategy that will preserve, sustain and expand the growth generated by this game-changing technology trend.

The federal government must partner with manufacturers on a sensible strategy that encourages the growth of the IoT and investment in our telecommunications infrastructure rather than deploying rules that will chill further expansion of these enabling technologies.

The growth of the Internet of Things has translated into improved quality of life for citizens, expanded growth for businesses, and greater opportunity for all. Still, what has been achieved will be dwarfed by the possibilities which still lie ahead. The NAM looks forward to working with you on policies that ensure this opportunity is realized.

Sincerely,



Brian J. Raymond

SUBMITTED STATEMENT FOR THE RECORD OF
PUBLIC KNOWLEDGE

BEFORE THE
SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET
OF THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

HEARING ON
THE INTERNET OF THINGS

JULY 29, 2015

SUMMARY

The Internet of Things presents exciting opportunities for a technologically driven society, but it also presents challenges to the rights and interests of consumers in that same society. We urge the Subcommittee to account for the wide range of such challenges as it considers law and policy for the Internet of Things in the coming years.

Patents on consumer technologies. Reforming the patent system is already a key issue for Congress now, and the Internet of Things will bring new challenges to this law of innovation. In particular, the Internet of Things is often described as numerous devices connecting to each other, and a particularly problematic form of patent is that which merely covers obvious combinations of devices connected to each other. Patent quality and fairness in patent assertion will be key factors in the success of the Internet of Things.

Ownership of devices. A particular and discomfiting trend is toward leveraging intellectual property rights and end-user license agreements that prevent consumers from full enjoyment of the very products those consumers buy. Through technological measures like DRM and contractual provisions that purport to merely license rather than sell device-embedded software, manufacturers declare that consumers do not in fact own their own devices. This already-present problem will only be exacerbated by the world of the Internet of Things.

Freedom to tinker and innovate. Attendant to the undermining of ownership rights in devices is the loss of consumers' ability to repair, improve, and innovate upon their personal property for their personal interests. Laws like § 1201 of the Digital Millennium Copyright Act (DMCA) prevent such user-driven creativity and invention, and as such contradict the basic purpose of intellectual property to "promote the progress of science and the useful arts." Legal policy should embrace, not entangle, efforts toward consumer-level progress, especially as the Internet of Things places more devices and thus more opportunities in the hands of consumers.

Communications privacy. While the future of the Internet of Things is not yet formed, one thing is certain: there will be numerous devices using communications networks to transmit information, much of which will divulge potentially private information about those devices' users. In such a world, privacy of the platforms of communication becomes orders of magnitude more important. Communications statutes give the Federal Communications Commission authority to ensure privacy and data security on such communications systems, and such authority must be maintained, strengthened, and adapted to ensure that consumer expectations are met in the Internet of Things.

Spectrum management. Critical to the Internet of Things is connectivity, and the primary vector for Internet of Things interconnection is "open" or "license exempt" spectrum. The vast majority of wireless Internet of Things devices will rely on open spectrum technologies like Wi-Fi and Bluetooth. Success of the emerging Internet of Things thus requires expanding our increasingly strained supply of open spectrum on the same terms and conditions available today. Additionally, as economic incentives among some actors grow to block or degrade Wi-Fi and other protocols that support the Internet of Things, we must ensure that the robust and highly competitive ecosystem of open spectrum critical to the emerging Internet of Things remains intact.

TABLE OF CONTENTS

THE INTERNET OF THINGS

STATEMENT OF PUBLIC KNOWLEDGE

CHAIRMAN ISSA, RANKING MEMBER NADLER, AND MEMBERS OF THE SUBCOMMITTEE:

Thank you for providing us with the opportunity to submit the following testimony for the record of this hearing on the Internet of Things.

Public Knowledge is a non-profit organization dedicated to preserving the openness of the Internet and the public's access to knowledge, promoting creativity through balanced intellectual property rights, and upholding and protecting the rights of consumers to use innovative technology lawfully. As part of this mission, Public Knowledge advocates on behalf of the public interest for a balanced intellectual property system, particularly with respect to new and emerging technologies, and for communications policy that fosters such emerging technologies.

While much have been said about privacy and security concerns surrounding the Internet of Things, Public Knowledge wishes to bring to light many other important issues that would affect technology-using consumers as these new developments move forward. In particular, we recommend that the Subcommittee include the following considerations in its deliberations over the Internet of Things.

I. THE PROPER BALANCE OF PATENT LAW MAY MAKE OR BREAK THE INTERNET OF THINGS

This Subcommittee is no doubt aware of the ongoing issues with the patent system and efforts to reform that system. Concern over so-called patent trolls using patents in abusive ways to attack small, innovative businesses abound in the news,[1] in the Adminis-

[1] *See, e.g.*, Fabio Marino & Teri Nguyen, *Are Patent Trolls Now Zeroed In on Start-Ups?*, FORBES (Jan. 17, 2013), http://www.forbes.com/sites/ciocentral/2013/01/17/are-patent-trolls-now-zeroed-in-on-start-ups/; Charles Duan, *Taking a Page from the Patent Troll Playbook*, SLATE: FUTURE TENSE (Dec. 17, 2014), http://www.slate.com/articles/technology/future_tense/2014/12/ben_edelman_used_patent_troll_tactics_in_going_after_a_chinese_restaurant.html; Joe Mullin, *Patent Trolls Want $1,000—for Using Scanners*, ARS TECHNICA (Jan. 2, 2013), http://arstechnica.com/tech-policy/2013/01/patent-trolls-want-1000-for-using-scanners/.

tration,[2] and even in the opinions of the Supreme Court.[3] Congress has made significant progress on two major bills to reform patent litigation.[4]

The Internet of Things shines a bright light on the patent system and its effects. Obviously, patents are a strong incentive for inventing new technologies, and as such are a key part of driving the Internet of Things forward. But a system full of overbroad patents and abusive patent litigation will drive innovation backwards instead, hampering the very innovators who would create those new technologies by threatening them with protracted litigation over patents on the most basic ideas.

In particular, the Internet of Things is all about connecting multiple consumer devices: the alarm clock tells the coffee machine to turn on; the refrigerator tells the smart phone what food to buy at the grocery store, and so on.[5] These are simple, obvious ideas—any imaginative person could devise them—and the value for consumers is not in the idea itself but in the implementation and standardization among companies that bring these ideas to market.

---

[2] *See, e.g.*, Executive Office of the President, Patent Assertion and U.S. Innovation 6 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/patent_report.pdf (describing PAEs as "pursuing legal action in a way that does not increase incentives for innovation"); Fed. Trade Comm'n, The Evolving IP Marketplace: Aligning Patent Notice and Remedies with Competition 67–68 (2011), *available at* http://www.ftc.gov/os/2011/03/110307patentreport.pdf (suggesting that increased PAE activity "can be detrimental to innovation"); *U.S. Patent and Trademark Office: The America Invents Act and Beyond, Domestic and International Policy Goals: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 13 (2014), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg88922/pdf/CHRG-113hhrg88922.pdf (statement of Michelle K. Lee, Deputy Under Secretary of Commerce for Intellectual Property) ("[T]he USPTO believes that additional legislative changes to build upon the AIA are needed to further enhance patent quality and to lessen litigation abuses in the system.").

[3] *See, e.g.*, *Commil USA, LLC v. Cisco Sys., Inc.*, 135 S. Ct. 1920, 1930 (2015) (quoting *eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 396 (2006) (Kennedy, J., concurring)); *id.* at 1932 (Scalia, J., dissenting); *Bilski v. Kappos*, 130 S. Ct. 3218, 3257 (2010) (Stevens, J., concurring) ("[P]atent holders may be able to use [patents] to threaten litigation and to bully competitors . . . . That can take a particular toll on small and upstart businesses." (footnote omitted)); *Atl. Works v. Brady*, 107 U.S. 192, 200 (1883) (expressing concern over "speculative schemers who make it their business to watch the advancing wave of improvement, and gather its foam in the form of patented monopolies, which enable them to lay a heavy tax upon the industry of the country, without contributing anything to the real advancement of the arts").

[4] *See* Innovation Act, H.R. 9, 114th Cong. (Feb. 5, 2015); Protecting American Talent and Entrepreneurship (PATENT) Act, S. 1137, 114th Cong. (Apr. 29, 2015).

[5] *See* discussion *infra* p. 13 (describing various Internet of Things devices that may be connected with each other).

But it is disappointingly common to see patents on these basic ideas of connecting one known technology to another. Consider the following examples:

- U.S. Patent No. 6,975,958: Connecting a thermostat to the Internet.[6]
- U.S. Patent No. 6,199,048: Connecting a barcode scanner to a networked computer database.[7]
- U.S. Patent No. 7,324,833: Connecting an iPod to a car.[8]
- U.S. Patent No. 7,343,165: Connecting a GPS to user directory information.[9]
- U.S. Patent No. 7,016,512: Connecting a hearing aid to an electrical plug.[10]

Such patents could easily stifle the development of new Internet of Things devices, and they could unexpectedly and undesirably deem every consumer of such devices an infringer and breaker of the law merely for connecting those devices to each other.

The Subcommittee should thus keep patents at the forefront of its thinking on the Internet of Things. Current efforts on patent litigation reform are an important step, as is encouraging and facilitating the U.S. Patent and Trademark Office's efforts toward improving patent quality,[11] to hopefully avoid such patents as those described above.

---

[6]U.S. Patent No. 6,975,958 (filed Apr. 30, 2003); *see* Mike Masnick, *Honeywell's Lawsuit Against Nest: The Perfect Example of Legacy Players Using Patents to Stifle Innovation*, TECHDIRT INNOVATION (May 8, 2012), https://www.techdirt.com/blog/innovation/articles/20120508/03354418823/honeywells-lawsuit-against-nest-perfect-example-legacy-players-using-patents-to-stifle-innovation.shtml.

[7]U.S. Patent No. 6,199,048 (filed Jan. 15, 1999); *see* Michael Barclay, *U.S. Patent Office Rejects All Ninety-Five NeoMedia Patent Claims*, ELECTRONIC FRONTIER FOUND. (July 18, 2008), https://www.eff.org/deeplinks/2008/07/u-s-patent-office-rejects-all-ninety-five-neomedia.

[8]U.S. Patent No. 7,324,833 (filed Sept. 23, 2004); *see* Samuel Howard, *Affinity Labs Hits Car Stereo Cos. With Patent Suit*, LAW360 (Sept. 2, 2008), http://www.law360.com/articles/67992/affinity-labs-hits-car-stereo-cos-with-patent-suit.

[9]U.S. Patent No. 7,343,165 (filed Apr. 11, 2001); *see* Jeff John Roberts, *Patent Troll Says It Owns GPS, Sues Foursquare*, GIGAOM (July 26, 2012), https://gigaom.com/2012/07/26/patent-troll-says-it-owns-gps-sues-foursquare/.

[10]U.S. Patent No. 7,016,512 (filed Aug. 29, 2003); *see K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1367 (Fed. Cir. 2014) (Dyk, J., dissenting) ("This should be an easy case, reversing the quite odd decision of the United States Patent and Trademark Office . . . that it could not consider whether multi-pronged electrical connections were well known in the prior art.").

[11]Charles Duan et al., Comments of the Electronic Frontier Foundation, Engine Advocacy, and Public Knowledge, *Enhancing Patent Quality*, 80 Fed. Reg. 6475 (USPTO May 6, 2015), http://www.uspto.gov/sites/default/files/documents/2015quality_a_eff_06may2015.pdf.

II. Lack of Ownership Rights over Electronic Devices Will Cause Substantial Problems for the Internet of Things

It's a basic feature of our laws that consumers have a lot of rights over their own physical and personal property. You can sell your car to whomever you like, repair it, modify it up to (and well beyond) the bounds of taste or sanity, lend it to anyone, and even rent it out or sell it to others. The same is true of pretty much anything else you have in your possession—your umbrella, your coat, and your desk. The right of ownership is the right to use and the right to dispose of physical property.[12]

Yet when it comes to equally physical, equally tangible electronic devices, those basic ownership rights have been diminished and even at times eliminated, often through use of intellectual property law.[13] Such efforts are troubling to the consumer interest and will only worsen as the Internet of Things places more electronics—and thus more opportunities to erode ownership rights—into everyday household products.

Are You Allowed to Turn Your Devices On? Every computing device, and thus every Internet of Things device, necessarily performs acts of copying of embedded software whenever it is turned on and operated. This means that, absent some sort of appropriate legal exception, it would be an act of copyright infringement merely to turn on your computer, smartphone, or FitBit. Unsurprisingly, the Copyright Act does contain such an exception: 17 U.S.C. § 117 "it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy" where the copy is made "as an essential step in the utilization of the computer program."[14]

It would seem that § 117 would resolve the issue, except that manufacturers have sought to circumvent—and successfully circumvented—this provision by declaring that a purchaser of a device with embedded software is not "the owner of a copy" of that software.

[12] *See* Denise R. Johnson, *Reflections on the Bundle of Rights*, 32 Vt. L. Rev. 247, 253 (2007) (enumerating eleven rights attendant to property ownership).

[13] *See* Christina M. Mulligan, *Personal Property Servitudes on the Internet of Things*, 49 Ga. L. Rev. (forthcoming 2015) (manuscript at 4–5), *available at* http://ssrn.com/abstract=2465651.

[14] 17 U.S.C. § 117(a) (2012).

For example, many product manufacturers write End User License Agreements (EULAs) that claim that the embedded software is never owned by the user. This allows them to assert that users can be found liable for copyright infringement for violations of the EULA despite § 117.

Courts have looked askance at such a strategy, expressing concerns that it "would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners,"[15] but have overall upheld the idea that purchasers of software may be denied status as "owners" of such software by virtue of such EULAs.[16] This Subcommittee should look equally askance at this denial of basic ownership rights by contracts of adhesion, considering the negative effects that will only multiply with the device multiplicity of the Internet of Things.

Chattel Servitudes Via Intellectual Property. The principle that physical, personal property may not be encumbered by post-sale restrictions set by a seller of that property—that chattels may not be subject to servitudes—dates back to Lord Coke's common law treatise of 1628.[17] It is now embodied in copyright's first sale doctrine[18] and patent law's doctrine of exhaustion.[19] But that right of owners to be free of easements on their things has been attacked in a number of ways using intellectual property law.

Section 1201 of the Digital Millennium Copyright Act (DMCA)[20] has been used to restrict electronic device owners' ownership rights. Although courts have at times stated that § 1201 does not "allow any company to attempt to leverage its sales into aftermarket monopolies,"[21] authorities such as the Library of Congress (who oversees administration

[15] *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 941 (9th Cir. 2010).

[16] *See, e.g., Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1111–12 (9th Cir. 2010); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 n.5 (9th Cir. 1993); *MDY Indus.*, 629 F.3d at 938.

[17] 1 Edward Coke, Institutes of the Lawes of England § 360, at 223 (1628).

[18] *See* § 109(a).

[19] *See Quanta Computer, Inc. v. LG Elecs., Inc.*, 553 U.S. 617, 625 (2008).

[20] 17 U.S.C. § 1201 (2012).

[21] *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1201 (Fed. Cir. 2004).

of portions of § 1201) have permitted such restrictions, for example by denying consumers the right to unlock their cell phones to use them with alternate mobile phone networks.[22]

Similarly, the Court of Appeals for the Federal Circuit has approved of using patent law to enforce manufacturer-imposed restrictions on consumers' ability to resell lawfully purchased goods.[23] This decision is currently being reconsidered as having potentially been overruled by later Supreme Court precedent.[24]

These efforts to erode the basic ownership right of alienation, termed "first sale" in copyright law and "exhaustion" in patent, have not gone unnoticed. As one commentator explains, "the similarities between unprotected goods and intellectual-property-embedded goods suggest that the exceptions to the first sale doctrine for conditionally-sold patented goods and software-embedded goods ought to be met with skepticism."[25] This Subcommittee should take an equally skeptical eye toward such developments in the law, in view of the Internet of Things.

LACK OF OWNERSHIP RIGHTS HARMS CONSUMERS. Such efforts to eviscerate ownership rights in their owned products directly harm consumers, who highly value freedom to use their purchase products and who despise such post-sale restrictions.

Several months ago, the coffeemaker manufacturer Keurig implemented lock-down technology into the Keurig 2.0 machine, preventing the machine from being used with single-serve coffee cups other than those authorized by Keurig. Consumers were outraged, going so far as to say, "I will never buy another Keurig product. This borders on the unethical forcing people to buy only the K-cups you make."[26]

---

[22] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 65260, 65255–66 (Library of Cong. Oct. 26, 2012) (to be codified at 37 C.F.R. § 201.40 (2014)), *repealed*, Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144, 128 STAT. 1751 (2014).

[23] *See Mallinckrodt, Inc. v. Medipart, Inc.*, 976 F.2d 700, 708 (Fed. Cir. 1992).

[24] *See Lexmark Int'l, Inc. v. Impression Prods., Inc.*, 785 F.3d 565 (Fed. Cir. 2015) (sua sponte order for rehearing en banc) (considering whether *Mallinckrodt* has been overruled by *Quanta*).

[25] Mulligan, *supra* note 13, at 30.

[26] Fred Barbash, *Keurig's K-Cup Screw-up and How It K-pitulated to Angry Consumers*, WASH. POST (May 7, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/05/07/keurigs-k-cup-screw-up-

Consumers also have objected to vehicle-implemented technological protection measures that prevent repairs, as those protection measures amount to post-sale restrictions. "Vehicle owners expect to have the freedom to repair and tinker with their vehicles, as they have done for decades," argued one organization seeking to obtain rights for consumers to overcome such technological locks.[27] And an agricultural advocacy group wrote: "We stand with a community of farmers . . . whose right to access, understand, and fully utilize their tools should be defended."[28] These civil society groups vocalized the expectations of consumers in having full, unhindered ownership rights.

Full ownership rights confer numerous societal and economic benefits. They avoid unnecessary administrative costs of tracing the trail of restrictions on any given product.[29] They open the door to secondary markets like eBay.[30] They allow consumers to repair their cars and other possessions.[31]

All of these rights are necessary today, and they will only become even more necessary with the developing Internet of Things, where electronic devices will abound. This Subcommittee must ensure that in the shuffle to bring new products and services to the market, consumers' ownership rights are not lost.

A Step Forward: The You Own Devices Act Fortunately, there are simple and straightforward solutions to protecting this consumer interest in ownership rights. The

---

and-how-it-k-pitulated-wednesday-to-angry-consumers/; *see also* Mat Smith, *Surprise! People Don't Like Keurig's DRM-Protected Coffeemakers*, Engadget (Feb. 6, 2015), http://www.engadget.com/2015/02/06/unsurprisingly-people-didn-t-like-keurigs-drm-protected-coffee/ (noting "consumers complaining everywhere online" about Keurig's plan).

[27] Comments of Electronic Frontier Foundation 16, *Exemption to Prohibition on Circumvention of Copyright Protection Systems*, 79 Fed. Reg. 73856 (Copyright Office Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class21.pdf.

[28] Comments of Farm Hack, *Exemption to Prohibition on Circumvention of Copyright Protection Systems*, 79 Fed. Reg. 73856 (Copyright Office Feb. 4, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_FarmHack_class21.pdf.

[29] *See, e.g., Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013); Mulligan, *supra* note 13, at 32 ("As software is incorporated more frequently into personal property, the information costs associated with using and transferring personal property will increase.").

[30] *See* Zachariah Chafee, *The Music Goes Round and Round: Equitable Servitudes and Chattels*, 69 Harv. L. Rev. 1250, 1261 (1956) (describing "policy in favor of mobility" long embraced by personal property law).

[31] *See Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 497 (1961).

You Own Devices Act, introduced this February, provides that a consumer is allowed to sell a device containing operating software, regardless of any contractual provision on the right to resell such software.[32] Such a bill would be a substantial step toward restoring the rights of consumers to use and sell their personal property.

As this Subcommittee continues to look at the legal implications of the Internet of Things, it should consider solutions such as the You Own Devices Act to ensure that consumers are adequately protected in their purchases of Internet of Things devices.

III. Laws Regulating the Internet of Things Must Enhance, Not Hamper, User-Driven Innovation

The ownership interests in Internet of Things devices are particularly important because they are the prerequisite to the "freedom to tinker": the ability of consumers to use, repair, modify, and improve upon their devices, in ways not contemplated by or even contrary to the interests of the original manufacturers.

The law would never prevent a consumer from shortening the legs of a chair to better fit his table, or a driver from replacing the stock tires on her car with ones that better suited her driving conditions. Parents might disable the camera on their children's laptops to protect their privacy. The addition of networked computers into everyday devices doesn't change the impulses to modify them. Whether a homeowner wants to alter his smart thermostat to work better with his existing air conditioner, or an abuse victim who wants to alter her car's location reporting so as not to expose it to her stalker, consumers enmeshed in the Internet of Things will still want and need to make their own adjustments to their property.

Yet the presence of embedded software can change the legal status of consumers' rights to repair, adapt, and tinker with their own goods. As explained above, the mere act of turning on an Internet of Things device can be a copyright infringement based on end-user license agreements, thus opening an avenue for manufacturers to prevent consumers

[32] *See* You Own Devices Act, H.R. 862, 114th Cong. sec. 2(a) (Feb. 11, 2015).

from modifying their devices, for fear of intellectual property litigation. Such a result ought to be avoided, either through application of 17 U.S.C. § 117 as discussed above or, to the extent that a license agreement purports to divest consumers of ownership of their own property,[33] through the doctrine of fair use.[34]

The anticircumvention provisions of the DMCA[35] provide a second avenue for extinguishing the freedom to tinker. By placing digital locks on consumer products and then using § 1201 to prevent consumers from opening those locks, manufacturers can dictate what consumers are allowed to do with their property. Some of the most celebrated cases on § 1201 feature precisely the type of behavior: a printer manufacturer denying consumers the right to refill their toner cartridges,[36] and a garage door opener manufacturer disallowing its customers from using aftermarket clicker transmitters.[37] These attempts at control have not lessened over the past decade, as filings and testimony at this year's triennial proceedings have demonstrated the interest of a number of manufacturers to continue using embedded software and access controls upon it to prevent users from adapting their products.[38] The Subcommittee should take notice of the demonstrated overreach of § 1201 and make efforts to provide necessary exceptions, exemptions, and limitations to the anticircumvention provisions, so as to grant consumers their deserved freedoms.

The freedom to tinker is particularly important because it is frequently the wellspring of productive innovation. As one multinational survey found, "millions of citizens

[33]Such an assertion, which would put the ownership of the product at odds with the ownership of software necessary to grant the owner full and fair use of it, should be scrutinized for potential violations of antitrust law or as potentially unfair or deceptive trade practices.

[34]*See* 17 U.S.C. § 107 (2012). Patent law has long recognized a right to repair, *see* discussion *supra* note 31, and copyright law has recognized one as well, *see* Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. Rev. 889, 912–19 (2011) (detailing cases of rights to repair and modify under copyright law analogous to the patent doctrine). These doctrines should operate today, whether independently or through the mechanisms of fair use and first sale.

[35]17 U.S.C. § 1201 (2012).

[36]*See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).

[37]*See Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

[38]*See Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Second Round of Comments*, U.S. Copyright Off. (Mar. 27, 2015), http://copyright.gov/1201/2015/comments-032715/.

innovate to create and modify consumer products to better fit their needs."[39] The resulting user-driven innovations became an "unexpected 'front end' of free innovation designs to serve as an important feedstock to commercial innovation processes in a wide variety of fields."[40] Freedom to tinker does not merely benefit the tinkerers; it in fact benefits manufacturers and the public as a whole.

But many manufacturers prefer instead to curtail consumers' rights to tinker with goods. A manufacturer may try to prevent consumers from modifying products to better suit their lives and households, preferring instead that they go back to the manufacturer for repairs—or to buy a new suite of products entirely.

Consumers should therefore be protected against attempts to use copyright law to prevent these traditional rights in the emerging Internet of Things—in the interests of them exercising their full property rights, protecting their privacy, and even building their and their children's skills in working with technology. The value of the freedom to tinker is not only the pocketbook value of fixing and customizing one's own belongings; it also provides an educational value in showing the user how devices—and the increasingly scientific, technological, and engineered world—works.

IV. Communications Privacy Takes On an Increasingly Important Role in the Internet of Things

The Internet of Things raises numerous privacy and data security concerns due to the quantity and granularity of data opened up by software-enabled devices. The Subcommittee should carefully consider one particular such concern, namely privacy and security of communications data sent over broadband Internet and other communications networks.

[39] Eric von Hippel et al., *The Age of the Consumer-Innovator*, MIT Sloan Mgmt. Rev., Fall 2011, at 28, *available at* https://evhippel.files.wordpress.com/2013/08/smr-art-as-pub.pdf.

[40] *Id.* at 29.

A Mass of Private Information, Open to Communications Carriers. The Internet of Things puts a wealth of information into the hands of carriers such as broadband Internet providers. First, the average consumer in an Internet of Things connected home now generates more data than ever before. Second, the data produced by the Internet of Things has grown both vaster and more detailed. And third, the potential for abuse by private interests has grown exponentially.

The fundamental idea underlying the Internet of Things is one of externalization—that is, to take the tasks once managed by an individual, and delegate their coordination to a series of outside devices. A typical example may go something like this: Sarah Consumer programs her LED smart lighting system[41] to wake her at a certain time by simulating a sunrise. The program controlling the lights,[42] having identified this as the time of day when Sarah rises and goes to eat breakfast, prepares the household for the day by performing various tasks, such as adjusting the thermostat,[43] dispensing diet food for the cat,[44] brewing a pot of coffee,[45] checking to make sure there is fruit and yogurt in the fridge,[46] and compiling a grocery list if any items were missing.[47]

The amount of data that passes between devices is substantial, and extremely detailed. In the example above, at various times, connected devices are swapping information including Sarah's sleep patterns, her dietary preferences, how warm she likes her

[41]Lee Hutchinson, *In Living Color: Ars Reviews the Hacker-Approved Philips Hue LEDs*, Ars Technica (Nov. 19, 2012), http://arstechnica.com/gadgets/2012/11/in-living-color-ars-reviews-the-hacker-approved-philips-hue-leds/.

[42]Tim Bajarin, *Amazon's Echo Is Showing Us the Future*, PCMag (July 27, 2015), http://www.pcmag.com/article2/0,2817,2488071,00.asp.

[43]Tom Simonite, *How Nest's Control Freaks Reinvented the Thermostat*, MIT Tech. Rev., Feb. 15, 2013, at 28, http://www.technologyreview.com/featuredstory/511086/how-nests-control-freaks-reinvented-the-thermostat/.

[44]Colin Jeffrey, *Bistro Cat Feeder and Health Monitor Identifies Cats Using Facial Recognition*, Gizmag (July 21, 2014), http://www.gizmag.com/facial-recognition-bistro-cat-feeder-health-monitor/33032/.

[45]Philip Palermo, *IRL: I Spent a Month Controlling My Coffeemaker over WiFi*, Engadget (Feb. 3, 2015), http://www.engadget.com/2015/02/03/irl-a-month-controlling-my-coffeemaker-over-wifi/.

[46]AJ Dellinger, *The New GE ChillHub Fridge Is So Smart, It Thinks It's a Computer*, Digital Trends (Feb. 5, 2015), http://www.digitaltrends.com/home/ge-firstbuild-chillihub-smart-fridge/.

[47]Bajarin, *supra* note 42.

apartment, her preferred brand of coffee, whether she lives alone or with others, and the fact that her cat is overweight.

Much of this data is passed over broadband providers or other communications carriers. An Internet of Things device may collect usage data and send it over the Internet to the manufacturer or third parties for various purposes, such as providing services to the consumer, collecting and aggregating data, or assessing quality of service. The Internet carrier potentially sees all of this communication, and likely can deduce from the traffic the nature of the device and potentially even usage patterns.

Others have raised privacy concerns about the capability of individual Internet of Things devices to collect and track information.[48] But communications carriers raise privacy concerns an order of magnitude larger, because they have a purview over *all devices* used by a consumer. While the manufacturer of Sarah's smart refrigerator may learn much about Sarah's eating habits, Sarah's broadband provider could potentially learn of her cat feeding preferences, coffee schedule, and daily routine as well, aggregating the many pieces of information flowing across Sarah's Internet channel.

The panoptic possibilities that the Internet of Things opens up to communications services thus demands strict oversight, if consumer privacy and data security are to be maintained.

The FCC's Communications Privacy Authority Is Critical Here. The Internet of Things highlights just how sensitive communications data can be, and thus it should come as no surprise that Congress has created specific, strong privacy protections against communications carriers misusing such data. These protections are found in Sections 201 and 222 of the Communications Act, which protect so-called "customer proprietary network information," or "CPNI."[49]

[48] *See, e.g.*, Federal Trade Commission Staff, Internet of Things: Privacy & Security in a Connected World 15 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[49] 47 U.S.C. §§ 201, 222 (2012).

Current FCC regulations put tight restrictions on the collection and use of CPNI, which is defined to include administrative network data about a user's communications, including its point of origin, destination, time, and duration.[50] Those regulations prevent communications services from utilizing CPNI for reasons other than providing "the telecommunications service from which such information is derived, or . . . services necessary to, or used in, the provision of such telecommunications service."[51] In other words, broadband providers cannot use the data gleaned from routing a customer's broadband traffic for any purpose that is not essential to providing service. This includes marketing—even when conducted by the broadband provider itself.[52]

The FCC has expressed its intent and dedication to applying these strong privacy protections to broadband Internet services in view of the agency's recent decision to reclassify broadband Internet as a telecommunications service under Title II of the Communications Act.[53] In that decision, the FCC noted that Sections 201 and 222 will apply to broadband providers,[54] because "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth."[55]

Through its CPNI authority, the FCC has proven to be a champion of consumer privacy, taking on massive data breaches by phone companies and rapidly adapting regulations to meet the needs of the times.[56] But there have been concerning efforts to strip this effective agency of this consumer-protective mandate.[57] This Subcommittee should make

[50] 47 U.S.C. § 222(h)(1)(A).

[51] 47 U.S.C. § 222(c)(1).

[52] 47 U.S.C. § 222(b).

[53] *See* Protecting and Promoting the Open Internet, 30 F.C.C. Rcd. 5601 (Fed. Commc'ns Comm'n Mar. 12, 2015) (Report and Order on Remand, Declaratory Ruling, and Order), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

[54] *Id.* ¶ 462.

[55] *Id.* ¶ 54.

[56] *See* Letter from Pub. Knowledge & 11 other organizations, to Michael C. Burgess & Jan Schakowsky, *Data Security and Breach Notification Act of 2015* 2 (Mar. 18, 2015), *available at* https://www.publicknowledge.org/assets/uploads/documents/letter-data-breach-3.pdf.

[57] *See id.* at 1.

efforts to enhance, not impair, consumer privacy in the Internet of Things by protecting the FCC's abilities in this arena.

Clear, direct protections must be applied to CPNI generated by Internet of Things devices. The Subcommittee must remain aware of these and other privacy challenges going forward, as the Internet of Things becomes more ubiquitous, and the expectations of privacy evolve.

V. A Dynamic Internet of Things Requires Spectrum Management That Favors Innovation, Not Incumbents

It is an obvious truism that any device considered part of the Internet of Things must connect "things" to the "Internet." Discussion of the Internet of Things and its evolution all too often elides over this truism without any concern for precisely how this will occur. We must not, however, take this condition for granted. If we neglect this first fundamental precondition—a way for devices to connect cheaply and seamlessly to the Internet and each other—then the Internet of Things will ultimately become stunted and strangled as it chokes on its own success.

By far, the preferred means of connecting devices to the Internet of Things has become wireless. Wireless provides mobility and limits the need for clunky physical connections. Improvement in wireless technologies has facilitated faster and more reliable connections.

A. A Brief Overview of Spectrum Policy In the United States

Access to wireless spectrum capacity (generally referred to simply as "spectrum") is managed in the United States by the Federal Communications Commission (FCC). Until the 1980s, every use of wireless spectrum required a dedicated band of frequencies for a specific purpose and no other. For example, one band for television broadcasting, one band for radio controlled cars, one band for police radios, and so forth.

Changes in technology and the rising demand for spectrum access prompted

Congress and the FCC to rethink the traditional model. By the mid-1990s, the U.S. shifted to making spectrum available primarily in 2 different ways:

- *Exclusive use "licensed" spectrum*, where the FCC auctioned off a limited number of geographic area licenses for general and exclusive use by the winner of the licenses at auction.
- *Unlicensed or "license exempt" spectrum*, where any person could operate a device that conformed to a set of fixed rules, and on the understanding that the device must (a) Not interfere with licensed services; and (b) must accept interference from any source, including other license exempt devices.[58]

The chief benefits of licensed spectrum are (a) protection from interference from other man-made transmitters (there are always sources of natural interference, such as sunspots or lightning, and networks must adjust accordingly); (b) relative high power use; and (c) exclusivity, allowing a relatively few wireless licensees to recoup the high cost of licenses and deployment by excluding other users. Licensed spectrum has become the basis for the cell phone industry. Licenses for spectrum suitable for mobile broadband cost billions of dollars,[59] and the cost of deployment of national wireless networks also runs into the billions. As a result, the United States has only 4 national wireless carriers offering mobile broadband services. Anyone seeking to use these frequencies, whether to connect with the Internet or with other local devices, must lease spectrum from one of these carriers and often must use the carrier's network—which is designed primarily for the over 300 million mobile phone customers in the country.

By contrast, unlicensed spectrum has become the home of practically all other devices using wireless access. Wi-Fi and Bluetooth have become the chief drivers of this enormous expansion of unlicensed devices, although the unlicensed spectrum supports

[58]For history, see generally Harold Feld, *From Third Class Citizen to First Among Equals: Rethinking the Place of Unlicensed Spectrum in the FCC Hierarchy*, 15 CommLaw Conspectus: J. Comm. L. & Tech. Pol'y 53 (2006), *available at* http://commlaw.cua.edu/articles/v15/feld.pdf.

[59]The most recent auction of mobile broadband wireless spectrum, Auction 97, yielded a total of approximately $45 billion in winning bids. *See* Federal Communications Commission, *Auction 97: Advanced Wireless Services (AWS-3)* (last updated Oct. 1, 2014), http://wireless.fcc.gov/auctions/default.htm?job auction_summary&id=97.

any number of proprietary or open standards for communications and support billions of non-Internet connected devices such as cordless phones, home security systems, and garage door openers.

B. Unlicensed Spectrum Continues to Be Necessary for Connectivity of the Internet of Things

Despite the advantages of interference protection offered by licensed spectrum, unlicensed spectrum has become the overwhelming source for connectivity for the Internet of Things.[60] Indeed, one may argue that the Internet of Things would be impossible without the ubiquity of cheap license exempt spectrum.

The open nature of license exempt spectrum reduces costs. Today, the number of unlicensed devices far exceeds the number of licensed devices, an inevitable result since nearly all "smart" devices operating on licensed frequencies also include Wi-Fi and Bluetooth capability.[61] This creates fantastic economies of scale, driving down the cost of standard Wi-Fi and Bluetooth chips to almost nothing per device.

The open nature of license exempt spectrum encourages innovation. Because wireless carriers invest billions in their networks, they exercise tight control over what devices may attach to the network, how much data subscribers may use, and other factors relating to the nature and type of traffic. By contrast, no one controls access to license exempt spectrum. This allows for innovation on an unprecedented scale.[62] When

[60] *See Wi-Fi Alliance "Fifteen for 2015" predictions*, Wi-Fi Alliance (Jan. 13, 2015), http://www.wi-fi.org/beacon/wi-fi-alliance/wi-fi-alliance-fifteen-for-2015-predictions ("Wi-Fi leads in smart home, industrial IoT, and connected car."); Richard Katz, Telecom Advisory Servs., LLC, Assessment of the Future Economic Value of Unlicensed Spectrum In the United States (2014), http://www.wififorward.org/wp-content/uploads/2014/01/Katz-Future-Value-Unlicensed-Spectrum-final-version-1.pdf; Richard Thanki, The Economic Significance of License Exempt Spectrum To the Future of the Internet (2012), http://download.microsoft.com/download/A/6/1/A61A8BE8-FD55-480B-A06F-F8AC65479C58/Economic%20Impact%20of%20License%20Exempt%20Spectrum%20-%20Richard%20Thanki.pdf.

[61] *See* Reply Comments of Open Technology Institute at New America, Public Knowledge, Free Press, and Common Cause 8–11, *Office of Engineering and Technology and Wireless Telecommunications Bureau Seek Information on Current Trends in LTE-U and LAA*, 80 Fed. Reg. 26561 (Fed. Commc'ns Comm'n June 26, 2015) [hereinafter LTE-U Comments], *available at* http://apps.fcc.gov/ecfs/document/view?id=60001105564.

[62] *See id.* at 8.

companies in the United States initially began to deploy "smart meters," they opted to deploy in unlicensed spectrum rather than in licensed spectrum because they could do so without either acquiring licenses or partnering with a licensed carrier. As a result, over 75% of the connections using smart meters rely on unlicensed spectrum.[63]

Internet of Things Traffic Is Better Suited to License Exempt Spectrum. Licensed networks have become highly congested with downloads of video traffic and other high-bandwidth latency-sensitive traffic. Wireless carriers have turned to unlicensed spectrum to meet their increasing need for capacity through "Wi-Fi offload" and LTE over unlicensed. As a result, experts predict that Wi-Fi networks will carry as much as 60% of all traffic originating on smartphones by 2019.[64]

Most IP traffic from Internet of Things devices is relatively low-bandwidth and tolerant of the environment of license exempt spectrum. A great deal of Internet of Things traffic involves local area networks, where devices communicate directly to one another rather than routing through a cell tower, traveling through a wireless carrier's network, and being rerouted to a device within the same building, or even the same room. The nature of this Internet traffic from devices is ideally suited to networks using unlicensed spectrum. By contrast, attempted to load this expanding Internet of Things traffic load onto licensed spectrum would result in an unmanageable spectrum crunch for everyone.

All of This Created a Virtuous Cycle that Makes Wi-Fi Ubiquitous. All these factors have combined to create a "virtuous cycle" that has expanded the availability of Wi-Fi and other technologies using shared spectrum rather than exclusively licensed spectrum. The ubiquity of Wi-Fi access points, drives down costs and encourages more innovation. This, in turn, creates more demand, driving costs down further.

[63]Yochai Benkler, *Open Wireless v. Licensed Spectrum: Evidence From Market Adoption*, 26 Harv. J.L. & Tech. 69 (2012), *available at* http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech69.pdf.

[64]Andrew Burger, *Juniper: Wi-Fi Offload Will Reach Nearly 60 Percent of Mobile Traffic*, Telecompetitor (June 18, 2015), http://www.telecompetitor.com/juniper-wi-fi-offload-growth-will-reach-nearly-60-percent-of-mobile-data-traffic/.

C. Threats to the Availability of Open Spectrum Threaten the Growth of the Internet of Things

While the availability of license exempt spectrum has driven the dramatic expansion and deployment of the Internet of Things, we cannot assume this happy state will continue forever. To the contrary, two major threats loom on the horizon. First, we are rapidly exhausting our supply of open spectrum available for the Internet of Things, creating a "spectrum crisis" for open spectrum similar to the "spectrum crisis" for exclusive use spectrum that has driven most spectrum policy for the last 5 years. Second, we are seeing the emergence of actors with the technical capability and financial incentive to either block or degrade Wi-Fi and unlicensed spectrum generally. Federal policy must address both these concerns to assure a robust and healthy future for the expanding Internet of Things.

We Need More License Exempt Spectrum Access. In 2010, the National Broadband Plan published by the FCC declared that the supply of available licensed spectrum could not keep pace with the increasing demand. Declaring a national "spectrum crisis" or "spectrum crunch," the FCC called for allocation of 500 MHz of wireless capacity for mobile broadband use, either from federal users or from broadcasters and other commercial users.[65] The FCC gave scarcely a nod to the need to enhance the availability of unlicensed spectrum for Internet of Things or other uses.[66]

In the 5 years since then, federal policy has gradually come to recognize the need to expand access to license exempt spectrum as well as exclusive use spectrum sold at auction. In 2012, the President's Council of Advisors for Science and Technology (PCAST) issued a report proposing that the future of federal spectrum reallocation required a mixed use "sharing model" that would permit federal users to retain adequate access to spectrum to

[65] Fed. Commc'ns Comm'n, Connecting America: The National Broadband Plan ch. 5 (2010), *available at* https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[66] *See id.*

perform vital national security and public safety functions, while providing greater opportunity for non-federal users to access spectrum on both an exclusive and non-exclusive basis.[67] Additionally, the FCC has commenced several proceedings designed to expand the availability and utility of spectrum in the 5 GHz band,[68] promote sharing with federal users as recommended in the PCAST Report,[69] and maximize the utility of license exempt operation in unassigned channels in the broadcast band—the so-called "TV white spaces"—for next generation Wi-Fi.[70]

Unfortunately, the FCC has met with considerable resistance from the automobile industry in the 5 GHz band,[71] and from wireless carriers worried that expanding license exempt access will introduce new competitors to the mobile wireless space. In addition, Qualcomm, which derives the majority of its revenues from patents in the licensed space, has consistently fought to limit expansion of license exempt and shared spectrum where its patent portfolio is weak, and where patenting policies adopted by the relevant standards bodies would prevent Qualcomm from using its patents to exclude rival chipmakers.[72]

Even if all the pending proceedings were completed, however, it would not suffice

[67]President's Council of Advisors on Sci. & Tecil., Executive Office of the President, Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth (2012), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast spectrum_report_final_july_20_2012.pdf.

[68]Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, 28 F.C.C. Rcd. 1769 (Fed. Commc'ns Comm'n Apr. 10, 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-22A1.pdf.

[69]Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550–3650 MHz Band, 27 F.C.C. Rcd. 15594 (Fed. Commc'ns Comm'n Dec. 12, 2012), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-12-148A1.pdf.

[70]Robert M. McDowell, *The FCC Should Fight for Our Right to TV White Space*, Wired (Apr. 17, 2015), http://www.wired.com/2015/04/fcc-white-spaces-database/.

[71]A portion of the Unlicensed National Information Infrastructure (U-NII) Band was assigned to the auto industry in 1999 for development of collision avoidance systems. This assignment was intended to be shared with unlicensed operations already designated for the band. *See* 28 F.C.C. Rcd. 1769, ¶¶ 92–93. Since 1999, the auto industry has failed to develop any standards or technology suitable for deployment. Since the FCC announced its intent in 2012 to expand the availability of this portion of the U-NII Band for advanced Wi-Fi capabilities, the auto industry has fiercely resisted any rule change that would facilitate deployment of Next Generation Wi-Fi.

[72]*See* LTE-U Comments, *supra* note 61, at 24–26.

to meet the expanding needs of the Internet of Things for the long term. Just as the FCC proposed developing a "spectrum pipeline" for licensed spectrum in 2010, Congress and the FCC should supplement this with a spectrum pipeline for license exempt spectrum. This will require significant rethinking by both the Office of Management and Budget (OMB) and the Congressional Budget Office (CBO) in how to assess the value of opening federal spectrum to sharing. At present, because spectrum auction provide an immediate injection of revenue, OMB and CBO do not assign a positive value to opening federal spectrum for sharing. Given the enormous value of the Internet of Things to the national economy, Public Knowledge recommends that CBO and OMB adopt "dynamic scoring" models to capture the macro-economic benefits of expanding license exempt spectrum access.

Public Knowledge therefore makes the following policy recommendations:

1. The FCC should move expeditiously to complete its proceedings to expand shared access of the 5 GHz band. Auto manufacturers should be required to either demonstrate interference with proposed use of their assigned spectrum, and to propose suitable mitigation measures that will permit enhanced shared access for the Internet of Things.[73]
2. The FCC should move expeditiously to finalize the rules for sharing the federal 3.5 GHz band consistent with the Order adopted in April 2015.[74]
3. Congress should amend Section 922 of the Telecommunications Act[75] to require the Administrator of the National Telecommunications Information Administration (NTIA) and the Chairman of the FCC to identify federal bands suitable for license exempt or otherwise shared operation with non-federal users as part of the National Spectrum Allocation Planning.
4. Congress should direct the Congressional Budget Office to develop and implement a dynamic scoring methodology to reflect the macro-economic benefits of existing

[73]Automobiles already use licensed and unlicensed spectrum as part of the Internet of Things, including anti-collision radar and rear-view cameras, without any deployment by auto manufacturers on the 5 GHz spectrum assigned to them in 1999.

[74]*See* Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550–3650 MHz Band, 30 F.C.C. Rcd. 3959 (Fed. Commc'ns Comm'n Apr. 21, 2015) (Report and Order and Second Further Notice of Proposed Rulemaking), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-47A1.pdf.

[75]47 U.S.C. § 922 (2012).

license exempt access to spectrum, and of expanding license exempt access to spectrum. Congress should further require CBO to use this methodology when assessing all proposals for allocation of spectrum.

We Must Protect the Ecosystem from Those with Incentive to Abuse It. In the last year, several incidents have come to light that indicate that some actors may have particular incentives to degrade the availability of Wi-Fi or the capacity to use unlicensed spectrum. Because devices using license exempt spectrum are not entitled to any interference protection, there is considerable concern that actors with the incentive to degrade operation of competing services using license exempt spectrum will either deliberately chose to do so, or will deploy technologies indifferent to their overall impact on the ecology of the license exempt space.

Two incidents are particularly noteworthy. First, the FCC brought an enforcement action against Marriott Corporation for deliberately jamming mobile Wi-Fi "hot spots" used by guests to force these guests to pay Marriot for use of Marriott's own Wi-Fi network.[76] Marriott took the position that the FCC lacked the authority to prohibit jamming of devices and networks using license exempt networks.[77] Ultimately, in the face of customer backlash, Marriott withdrew its legal Petition, leaving the question of the FCC's authority unresolved.

More recently, a number of stakeholders (including Public Knowledge) have raised concerns over the planned deployment of LTE over unlicensed spectrum (LTEU) by wireless carriers to supplement their existing LTE deployments on licensed spectrum.[78] Although proponents of LTEU, and of a proposed standard to utilize licensed and unlicensed spectrum simultaneously ("Licensed Assisted Access" or "LAA") insist that LTEU/LAA will not degrade Wi-Fi, stakeholders note that the LTEU/LAA protocols have the capacity

[76] *See* Press Release, Federal Communications Commission, *Marriott to Pay $600,000 to Resolve WiFi-Blocking Investigation* (Oct. 3, 2014), https://apps.fcc.gov/edocs public/attachmatch/DOC-329743A1.pdf.

[77] *See* Petition for a Declaratory Ruling to Interpret 47 U.S.C. § 333 or, in the Alternative, for Rulemaking, *In re Petition of Am. Hotel & Lodging Ass'n, Marriott Int'l, Inc., & Ryman Hospitality Props.*, No. RM-11737 (Aug. 25, 2014), *available at* http://apps.fcc.gov/ecfs/document/view?id=60000986872.

[78] *See* LTE-U Comments, *supra* note 61.

to degrade Wi-Fi, and that wireless carriers have the financial incentive to do so in the face of competition from cable offering mobile services on their Wi-Fi footprints. Additionally, Qualcomm—the primary chip vendor for LTEU/LAA—has the incentive to shift the standard development process away from the Wi-Fi standards bodies because the Wi-Fi standards bodies have adopted polices that would limit Qualcomm's ability to deny rival chipmakers patents on fair, reasonable and non-discriminatory terms.[79]

The Internet of Things relies on expanding access to license-exempt spectrum, particularly to ubiquitously available technologies such as Wi-Fi, and so this potential for abuse this a matter of grave concern for the future of the Internet of Things. At the same time, regulation of the "unlicensed space" may have unintended consequences with regard to the future of innovation.

Don't Regulate Technology, Police Bad Actors. A straightforward first step would be to clarify that the FCC's existing statutory authority will allow it to sanction actors who either deliberately attempt to degrade traffic using license-exempt frequencies, or who deploy technologies with callous indifference to their detrimental impact on the ecosystem as a whole. Arguably the Communications Act already provides mechanisms for the FCC to do this,[80] but the full Commission has never definitively determined whether the existing statutes provide the necessary authority to police the improper behaviors described above.

This Subcommittee should consider amending the law to clarify that no one may "willfully or maliciously" degrade or block the operation of devices using license exempt or otherwise non-exclusive/shared frequencies. Alternately, the Subcommittee should otherwise prohibit willful or malicious interference with devices operating on license exempt spectrum. In all events, the FCC should be authorized to order remedial steps where

[79] *See id.*

[80] *See* 47 U.S.C. § 333 (prohibiting anyone from "willfully or maliciously" interfering with any signal "licensed or authorized" by the FCC); § 324 (requiring all users of radio frequencies to use the minimum power necessary to complete the desired communication).

it finds that operation of a licensed or unlicensed service would constitute a threat to the unlicensed ecosystem and the Internet of Things.

It is important to understand that the "willful and malicious standard" does not include the standard "harmful interference" which all devices operating on unlicensed spectrum must accept. Nor would it in any way create superior rights of unlicensed devices to licensed devices. "Willful and malicious" are terms directed at *actors*, not at technology. "Maliciously" refers to a deliberate effort to degrade operation for personal gain, such as occurred when Marriott deliberate jammed Wi-Fi hot spots to drive traffic to its own network. "Willfully" refers to actions taken with the clear understanding that deployment creates hazards to the broader ecosystem, but where the individual nevertheless acts with callous indifference and choses to deploy the technology anyway.

Under such a standard, wireless carriers would be free to deploy LTEU/LAA, but with the understanding that deliberate efforts to degrade competing services would result in enforcement actions and sanctions. Additionally, if the deployment of LTEU created widespread interference with Wi-Fi services critical to the Internet of Things, even if carriers did not intend to cause such widespread interference, the Commission would retain the authority to order mitigation measures to protect the unlicensed ecosystem.

VI. Conclusion

As the chairman of this Subcommittee has said, Internet of Things devices "raise both opportunities and questions about regulatory policy, spectrum space, privacy and more."[81] We hope that the considerations outlined in this statement highlight the breadth of those opportunities and questions as policymakers such as the members of this Subcommittee face a fast-changing technological space. We thank the Subcommittee for offering us the opportunity to provide this statement.

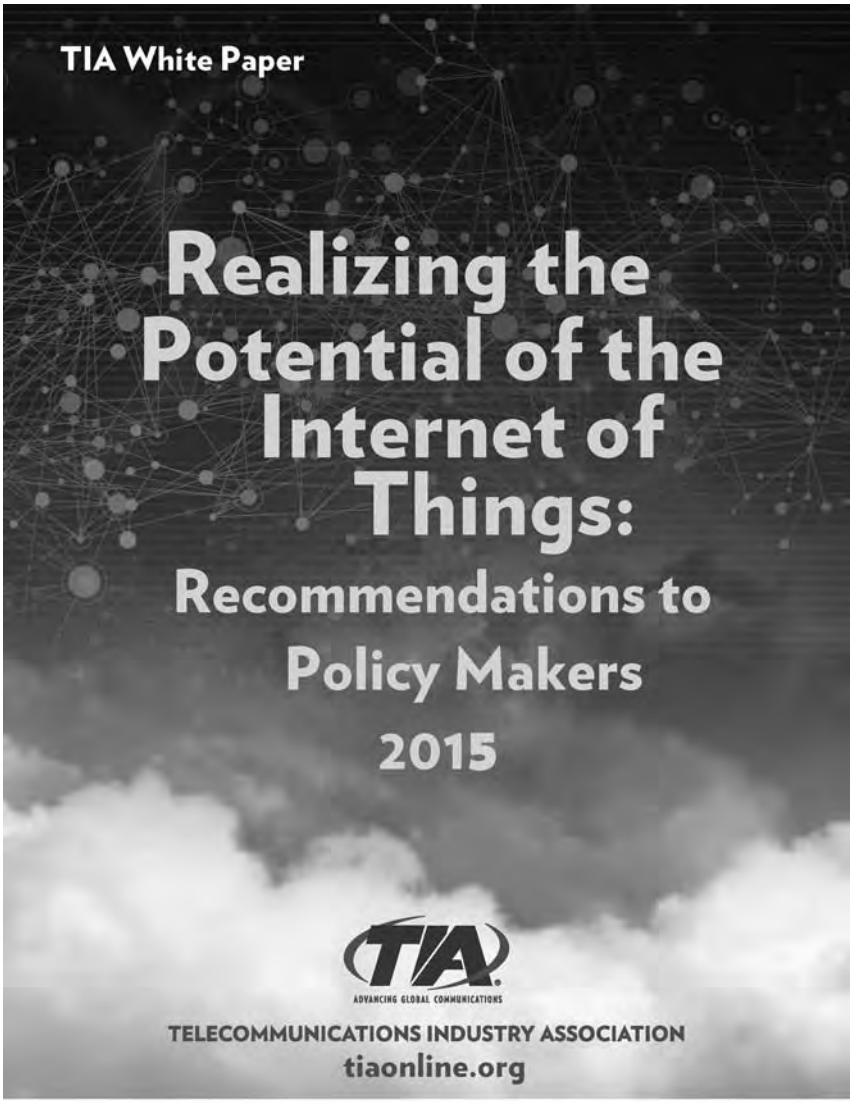
Respectfully submitted,

Charles Duan
Harold Feld
Meredith Filak Rose
Sherwin Siy

On behalf of
Public Knowledge

July 29, 2015

[81] Erin Kelly, *Congress Sees Security Risk in 'Internet of Things'*, USA Today, Feb. 9, 2015, http://www.usatoday.com/story/news/politics/2015/02/09/internet-of-things-house-caucus-senate-hearing/22927075/.


TIA White Paper
Realizing the Potential of the Internet of Things:
Recommendations to Policy Makers
2015
TIA
ADVANCING GLOBAL COMMUNICATIONS
TELECOMMUNICATIONS INDUSTRY ASSOCIATION
tiaonline.org

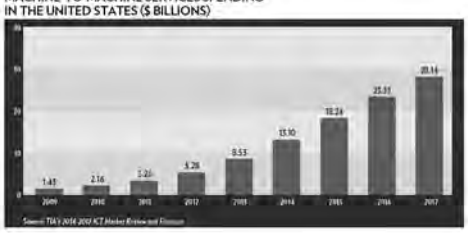
Realizing the Potential of The Internet of Things: Recommendations to Policy Makers

The future for telecommunications and the world economy lies with the Internet of Things (IoT). At its most basic, the "Internet of Things" is a label for an increasingly connected future in which regular, everyday items – from household appliances to cars to medical devices – are outfitted with sensors and connected to the Internet to share their data. Viewed more broadly, the Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. In this new world, most communications will be machine-to-machine (M2M), and there will be a continuous exchange of information between devices, sensors, computers, and networks.

The rapid rise of the Internet of Things has been driven by several factors, including the widespread penetration of broadband Internet, faster mobile connections, and the use of advanced computing capability, which allows for the development of smaller and cheaper devices. In recent years, a key element driving growth has been the ability to install inexpensive sensors in machines and devices. This has been made possible by advances in sensor technology that have dramatically reduced costs, while also capitalizing on geo-location or other technology advancements. Once these devices are connected to a network, consumers and businesses will have the ability to collect and analyze significant amounts of machine-generated data in real-time, allowing people to make decisions that maximize efficiencies in time and cost.

Aside from driving transformative societal effects, the economic potential of the IoT is enormous. In 2012, an estimated 8.7 billion "things" were connected worldwide, and projections show that this could grow to 50 billion

MACHINE-TO-MACHINE SERVICES SPENDING IN THE UNITED STATES ($ BILLIONS)



by the year 2020[1] – generating global revenues of $8.9 *trillion* in the process[2]. In direct terms, this represents an enormous market for information and communications technology (ICT) manufacturers, vendors, and suppliers. Ultimately, however, there will be enormous secondary economic effects as the Internet of Things emerges and gradually transforms daily life worldwide.

The Internet of Things holds the potential for major disruptive effects across a wide variety of market sectors... [m]eanwhile, there are a number of important horizontal policy issues that affect the Internet of Things across markets and use cases.

Not surprisingly, policymakers are taking a much greater interest in the Internet of Things, and are attempting to craft forward-looking laws and regulations that keep pace with innovation – or at least do not hinder it. This white paper begins by offering a general framework for such policy discussions. The recommendations that follow are applicable across market sectors, and will help ensure that the full economic, societal, and technological potential of the Internet of Things is ultimately realized.

A Horizontal Framework for IoT Policy

The Internet of Things holds the potential for major disruptive effects across a wide variety of market sectors. Vertical markets that will be affected include, for example:

- ***Health Care.*** Health care applications include the potential for remote patient monitoring using smart electronic devices, allowing patients and their doctors to obtain real-time access to health data. This is expected to lead to vast improvements in the quality of care, better health outcomes, and significantly lower costs.
- ***Transportation.*** Transportation applications will include not just the rapidly emerging self-driving and connected vehicles, but also the ability to develop "intelligent" transportation infrastructure from roads to airports to parking garages.
- ***Energy.*** Applications include smart metering, other "smart grid" technologies, and the ability to drive greater efficiencies in both energy production and consumption.
- ***Manufacturing.*** Sensor networks and smart devices will drive major improvements throughout the manufacturing process based on process improvements such as increased visibility into manufacturing processes that better inform decision-making, improved automation, augmented energy management, increased ability for proactive maintenance, and a better-connected supply chain.
- ***Government.*** The Internet of Things will have a major impact in the public sector, from defense and emergency service applications to driving improvements in service delivery and responsiveness to constituent needs.

With the Internet of Things holding the potential to achieve the real-world advances described above, much of the initial policy interest has developed vertically, i.e., with respect to a specific market. Market-specific regulators have started considering IoT-related policy actions for several of the markets above, although often never actually using the term "Internet of Things."

Meanwhile, there are a number of important horizontal policy issues that affect the Internet of Things across markets and use cases. These include, for example:

[1] http://share.cisco.com/internet-of-things2.html

[2] http://www.idc.com/getdoc.jsp?containerId=prUS24566813

- ***Interoperability.*** Enabling devices and systems to connect with each other on a technical level, typically through reliance on common standards or protocols.
- ***Privacy.*** The ability of consumers and businesses to safeguard their own personal or business data in a world of machine-to-machine transmissions.
- ***Security.*** Ensuring that devices, networks, and applications are secured from threats by malicious actors.
- ***Data Storage.*** Where, how, and when the vast amounts of data generated from individual sensors and devices will be stored.
- ***Spectrum and Bandwidth.*** Ensuring that sensor-enabled and network-aware devices are able to transmit their data in a manner that uses constrained resources efficiently.

IoT policy discussions should begin with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications only as necessary.

With these common threads running across IoT applications and use cases, a significant danger exists that vertical regulations imposed in one market will be inappropriate for another. This could lead to a balkanized regulatory approach that stifles innovation and delays or degrades the economic and social potential of the IoT.

To avoid this scenario, ***IoT policy discussions should begin with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications only as necessary***. Of course, achieving complete regulatory uniformity across different vertical markets may be both difficult and inadvisable. However, maximizing commonalities across sectors holds the potential for achieving both greater efficiencies as well as synergies across markets, increasing the potential for innovation. The IoT will effectively impact all aspects of society, and will grow existing – and create new – circular interdependencies among networks and devices used in the commercial enterprise, commercial consumer, public utility, and public safety segments, among many others. For example, the need for adequate consideration and management of risks to ensure the security and integrity of data (addressed later in this white paper) rests across all IoT applications.

The recommendations that follow in this white paper address many of the cross-cutting horizontal issues described above. As such, they are generally applicable across applications, use cases, and market sectors.

Recommendation: Policymakers' Approach to the Internet of Things Should Adhere to Competition- and Technology-Neutrality Principles

As ICT manufacturers and vendors work to meet the needs of their customers, competition will ultimately determine which products and services succeed or fail in the market, thereby fueling further innovation. As businesses increasingly make investments in the IoT, an utmost concern for policymakers should be to take a competition- and technology-neutral approach that respects the need for specific sectors to utilize creative solutions, and for innovators to address the needs of market segments. Policy makers should be wary of taking any action that locks the market to a limited set of solutions when new innovations, some of which cannot be predicted, are constantly being rolled out. No industry illustrates the need for flexibility and technology neutrality more than the dynamic ICT industry.

Policymakers should also avoid any situation that would put a government actor in a position to determine the future design and development of technology. To do otherwise would set a precedent of interference with the core innovation engine of the ICT sector, negatively impacting the interoperability and standards needed for IoT proliferation. Should a well-developed public policy case based on the consensus of stakeholders find that regulatory action is needed, we strongly encourage policymakers to promote the competitive dynamic by adopting regulations that are outcome-based, allowing innovation to thrive while still achieving the regulatory requirement.

Recommendation: Policymakers Should Encourage and Leverage Voluntary, Open, and Consensus-Based Standards

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards.

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards. Ongoing and future standardization efforts that enable the success of the IoT will cut across market segments, and will range from overarching guidelines to specific technical criteria, ensuring increasing interoperability as well as backwards-compatibility. Importantly, these standards are able to dynamically adapt to needed changes based on the expertise of their stakeholders. These standards also reduce costs, because manufacturers and software developers can produce for multiple applications and multiple end uses, allowing the benefits of economies of scale. TIA expects the development of IoT to be driven by a global – not regional – approach based on the development of open, voluntary, and consensus-driven standards.

Numerous existing standardization efforts, as well as future efforts, to address industry-consensus needs will define and contribute to the development of an interoperable IoT. TIA broadly supports the "multiple paths" approach to the development of international standards whereby healthy competition among the different efforts will result in market-driven solutions that provide customers with the best options. TIA houses this type of standardization efforts, such as in its Engineering Committee TR-50 M2M (Smart Device Communications).[3] Other examples of such standardization activities include:

- oneM2M, an international partnership working to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software.[4]
- Open Interconnect Consortium (OIC), a group of industry leaders working together to deliver a specification and to promote an open source implementation to improve interoperability among the billions of devices making up the IoT.[5]

[3] Engineering Committee TR-50 M2M (Smart Device Communications) is responsible for the development and maintenance of access-agnostic interface standards for the monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications or networks. These standards development efforts pertain to but are not limited to the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.

[4] http://www.onem2m.org/

[5] http://openinterconnect.org/

Standardization is a form of economic self-regulation that can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways. TIA urges policymakers to defer to these standards as they are developed and come to define the IoT. By taking this approach, policymakers can use these standards as valuable sources of scientific and technical information developed with the assistance of private sector experts, allowing agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area.

Standardization is a form of economic self-regulation that can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways.

At the same time, Government can help encourage the development of industry standards by funding research in cross-cutting areas such as cybersecurity and M2M interoperability for advanced communications technologies. Continued research is needed to prevent systemic attacks on IoT systems. This may provide an opportunity to create university-based cybersecurity "centers of excellence" or Federal lab-based research such as the National Cybersecurity Center of Excellence (NCCoE) at NIST. Interoperable mobility enables public safety and law enforcement officials to use the various public safety and cellular mobile networks while avoiding the necessity of carrying multiple mobile devices. It promotes coordinated communications among various public service agencies and allows higher-priority use of scarce spectrum services market and is critical for the common good. Also, bringing commercial technologies and emergency services technologies closer together will result in lower costs and more advanced features for critical emergency services.[6]

Policymakers should avoid any approach that would redefine "open standards" in a way that equates patented technology with "free" (as in without payment) or "free to use freely" (as in without payment and without any restrictions). This kind of redefinition would undermine the rights of those who have invested in the development of standardized technologies that enable the functioning of countless sectors of the economy. Technological capabilities and innovations most often result from substantial investments in research and development. Thus, if patent holders in standards-setting activities are expected to give away or waive their patent rights, there are likely to be significant adverse results, including that technology leaders will reduce or cease participation in voluntary standards-related activities; or that individuals and organizations will not invest in the development of next-generation technology in the technical areas subject to standardization, creating innovation "dead zones" in those areas.

Recommendation: Policymakers Should Employ Regulatory Approval Approaches that are Globally Harmonized, Transparent, and Streamlined

The ICT industry is one of the most far-reaching and competitive segments of the global economy. Across jurisdictions, the varying requirements of ICT present unique challenges to ensuring that governments, consumers, and other stakeholders in a diverse marketplace have the ability to determine readily whether a device has been properly certified, and to obtain additional information about a device as efficiently as possible. With the drastic increase in the number of connected things in the IoT, it will be very important for policymakers to ensure that regula-

[6] http://www.tiaonline.org/gov_affairs/fcc_filings/documents/TIA%20U.S.%20ICT%20R&D%20Policy%20Report.pdf

tory approval processes are transparent and efficient. We urge policymakers to examine their regulatory device approval mechanisms methodically to ensure that these systems are as globally-harmonized, predictable, transparent, and reliable as possible. This will promote the "build once, sell anywhere" principle, which drastically reduces regulatory costs, time-to-market, and cost to end users throughout the business and consumer markets.

The IoT will rely significantly upon maximizing continuity of connectivity. With the world rapidly becoming wireless, establishing an appropriate spectrum policy is essential to ensure that the IoT will be successful.

For example, to streamline the process ICT manufacturers must go through to get products to market, policymakers are strongly urged to consider permitting the use of Supplier Declarations of Conformity (SDoCs) for trusted classes of products as an alternative means by which an ICT manufacturer may demonstrate compliance with regulatory rules. The benefits of such an allowance include flexibility and objective treatment for manufacturers in where to have their products tested, high compliance levels, and lower administrative costs. The appropriate allowance of SDoCs would also support mutual recognition agreements (MRAs) among trading partners and widespread recognition of another country's conformity assessments, further reducing associated costs. Based on a long-standing record of compliance, many technologies have proven that very low risk exists for violating the technical rules, primarily because they are built to meet consensus technical standards, allowing policymakers to be assured that they can take this step to allow for more rapid availability of products into the marketplace at reduced cost to stakeholders, including consumers.

As a further example, the use of physical markings or labels has played a key role in providing important information about devices, but the continuous evolution of industrial design and multiple regulatory environments has led to increased costs and difficulty in ensuring that all relevant markings or labels are affixed in an efficient and convenient manner for the user of the device. An effective solution to this problem is the non-exclusive use of electronic labeling, which allows consumers and other users access to easily readable and prominently displayed information about each device. This information should include required regulatory markings and other important information, including proper device care, electronic recycling programs, and warranties. Already, through closely working with TIA, several key jurisdictions have allowed this approach.

Recommendation: Utilize a Spectrum Policy that Maximizes a Continuity of Connectivity

The IoT will rely significantly upon maximizing *continuity of connectivity*. With the world rapidly becoming wireless, establishing an appropriate spectrum policy is essential to ensure that the IoT will be successful. In commercial communications networks, mobile data use is exploding as consumers embrace smartphones, tablets and other devices. Wireless connectivity is becoming the way in which consumers access the Internet through technologies such as LTE, Wi-Fi, and satellite. Governments worldwide also have a significant dependency on spectrum for both communications and non-communications purposes.

Meanwhile, radio technologies themselves are changing, placing new demands on spectrum allocations and raising new operational and regulatory challenges. There are currently several new or emerging technologies that are competing in the marketplace to serve the Internet of Things. These include Near Field Communication (NFC), a standards-based short-range wireless technology widely linked with mobile payments. More recently, Bluetooth Low Energy (Blue-

tooth LE or BLE) has been built specifically to consume small amounts of energy; it is also viewed as a good candidate for small data packets sent from wearable computing devices such as smart watches and fitness trackers. Traditional Wi-Fi is also expected to play a key role, due to its low cost and ubiquity in the marketplace. Indeed, the future Internet of Things will likely be based on *heterogeneous networks* whereby devices can sequentially or simultaneously use different network technologies.

As a result of these dynamic changes, spectrum allocations and uses that may have sufficed during the 20th century are increasingly under stress. Unfortunately, policymakers are no longer writing spectrum policy on a blank sheet of paper, and virtually all spectrum suitable for mobile service has been allocated. For that reason, TIA believes that any spectrum policy must reflect the following principles to allow the use of radio spectrum to evolve to meet changing demand and promote innovation:

- ***Predictability.*** Spectrum allocations need to be predictable. Identifying demand and changes in demand, understanding the pace of radio technology development by platform, and long term planning are all essential parts of a spectrum policy that can provide predictability for both commercial and government users.
- ***Flexibility.*** For commercial allocations, flexible use policies consistent with baseline technical rules that are technology-neutral have proven to be the best approach. Any government allocations of spectrum should be managed to ensure better usage of scarce spectrum resources for all users.
- ***Efficiency.*** Policies should encourage more efficient use of spectrum where technically and economically feasible. In particular, policies should prioritize *global harmonization* and coordination of spectrum allocations;[7] protection from harmful interference for licensed uses; adjacency to similar services; and allocations of wide, contiguous blocks of spectrum. Cleared, exclusively-licensed spectrum allows the most efficient and dependable use of spectrum for commercial mobile broadband deployment.
- ***Priority.*** In cases where spectrum sharing is technically and economically possible, policies must advance good engineering practice to best support an environment that protects those with superior spectrum rights from harmful interference.

Furthermore, spectrum sharing represents a means of increasing the efficient use of spectrum and of helping to alleviate challenges in spectrum scarcity. It could eventually prove critical in enabling the *continuity of connectivity* that is so critical for the Internet of Things. In addition to ongoing efforts underway to realize successful sharing regimes, other promising efforts include the deployment of Licensed Shared Access (LSA) approaches, a "third way" spectrum management system that combines elements of traditional "command and control" spectrum management with geolocation technology, e.g., by providing users with a "token" to use spectrum at certain times/places. LSA approaches show great promise, as they provide a means of ensuring the ongoing viability of incumbent uses by creating a policy environment that enables compatible operations with new uses while also providing secondary users a means of gaining access to spectrum that is already licensed to one or more primary users, but may be underutilized or capable of supporting multiple uses.

[7] **Globally harmonized spectrum is essential to ensure the economies of scale that will facilitate the large-scale deployments necessary** to utilize the promise of new technologies fully. Global harmonization also facilitates roaming, an important part of creating the "continuity of connectivity" required for the Internet of Things.

Recommendation: Promote Efforts to Modernize Wired Media for IoT Applications

IoT applications will continue to depend heavily on wired media for various industrial applications (the deployment of parking space sensors in a garage is a basic example). High-capacity, low-cost cabling solutions that allow the connection of a multitude of increasingly sophisticated individual sensors to the network will often be essential for quality-of-service or security reasons where wireless options do not make sense. For example, excessive errors in motion control systems could cause machinery shut-downs and a break in the manufacturing process and require a manual re-set of equipment, increasing manufacturers' costs.

IoT applications will continue to depend heavily on wired media for various industrial applications.

Moreover, wired solutions generally also avoid the spectrum bandwidth constraints associated with widespread deployment of individual sensors or devices. In addition, cabling can also potentially be used to provide electrical power to the individual sensors or devices, making it essential for applications where the use of individual device batteries may be difficult.

Ultimately, as the experience with conventional Ethernet has demonstrated, the use of cost competitive and high performance cabling can lead to economies of scale in network designs and deployments.

For these reasons, standards-making bodies are making progress toward the development of next-generation cabling standards for IoT applications. The IEEE 802.3 working group is looking at channel models, cable, and connectivity for Reduced Twisted Pair Gigabit Ethernet (RTGPE).[8] In particular, there are two efforts to devise performance models for supporting 100 Mbps and 1 Gbps data rates on a single twisted pair copper cable (as opposed to the four pairs normally required), as well as providing electrical power (Power over Ethernet – PoE). Products based on these and other wired standards represent potentially smarter and cheaper alternatives to today's low-voltage wiring applications, allowing network functionalities and intelligence to move closer to the edges of a network (e.g., smarter individual sensors) rather than in a centralized device controller.

Recommendation: Utilize a Voluntary, Flexible, and Collaborative Approach to Data Security Based on International Standards

With the IoT naturally involving an ever-increasing number of "things" connected throughout society, new and evolving security issues will emerge as challenges. The ICT industry already considers security issues throughout the design process, and this approach will continue to be employed to mitigate threats in the IoT. TIA urges policymakers to regard the IoT as an opportunity for greater security, since by using a network approach paired with proper risk management techniques, IoT devices can be made to work together to produce comprehensive, actionable security intelligence in near real time. These approaches and risk management techniques are by and large driven by market demand, typically manifested through industry-driven best practices and standards developed in open, voluntary, and consensus-based fora.

[8] IEEE has also recently formed the P2413 group for the purpose of aggregating technical standards from existing IEEE efforts (such as 802.3) that may be relevant for IoT applications. *See* http://standards.ieee.org/develop/project/2413.html

To support high levels of security and resilience in the IoT, TIA urges policymakers to be guided by the following principles:

- *Respect competitive differentiation and business continuity.* As ICT manufacturers and vendors work to meet the needs of their customers, less secure products that are more vulnerable to cyber attacks will naturally be less attractive in the market. Today, this drives ICT manufacturers and vendors to strive to make their products and services less susceptible to cyber attacks, and these efforts are expected to increase dramatically.[9] The degree to which an organization's performance goals are used to ensure its ability to provide essential services while managing cybersecurity risk will depend on the specific needs of its sector and organization. However, in the ICT sector, manufacturers work with the range of organizations they supply to ensure that performance goals of those organizations are reflected in the ICT they purchase. The flexibility to innovate and the use of voluntary, consensus-based standards are both key enablers of this capability. There is no "one size fits all" solution to securing the IoT. The reach of the IoT across segments of the economy with varied levels of risk illustrates this. Government does have a legitimate role in requiring technology providers to disclose cyber risks to users (for example, the FTC has adequate authority under Section 5 of the FTC Act,[10] to stop unfair or deceptive acts or practices on a case-by-case basis using a flexible standard of reasonable security).

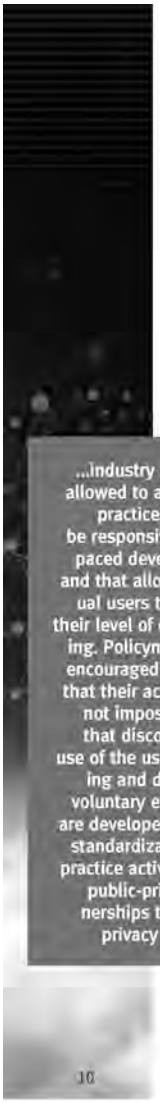
There is no "one size fits all" solution to securing the IoT.

- *Rely on international standards.* Numerous standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners and operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels. TIA urges policymakers to ensure that their approach to the IoT reflects the priority of the development of internationally-used standards and best practices. The global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and a global supply chain can be secured only through an industry-driven adoption of best practices and global standards. Country-specific standards should be avoided, as they would ignore the benefits of global harmonization, restricting trade in telecommunications equipment imported to or exported from other countries that are part of the global trading system. While there are legitimate public safety or security concerns, Government's role should be limited to setting performance requirements that can be flexibly addressed in standards and technical specifications – not to pick or mandate specific technologies or process methodologies. Such an approach is consistent with the United States' Department of Commerce National Institute of Standards and Technology's (NIST) *Cybersecurity Framework*,[11] which is voluntary, risk-based, and technology neutral, and relies on a variety of existing standards and other best practices to enable critical infrastructure providers to achieve resilience to cyber-based threats.
- *Utilize the successful public-private partnership model.* Public-private partnerships are an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive encouraging businesses to make investments in cybersecurity that are appropriate for the risks they face. The voluntary, public-private model is also able to evolve in response to changes in threats and the risk environment. As both the complexity and number of attacks grow, it will be critical that policymakers leverage and augment, or create where necessary, public-private partnerships. Where industry collaboration is lacking or is not mov-

[9] http://www.gartner.com/newsroom/id/2629722

[10] *See* 15 U.S.C. § 45

[11] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.



ing forward at a pace able to address significant national needs, the Government can use its convening power to bring stakeholders together and encourage cross-sector development. Such an approach is reflected in the President's National Security Telecommunications Advisory Committee (NSTAC) report on the IoT and its impact tonational security and emergency preparedness,[12] which recommends the close collaboration of Government and industry to "coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks."

- *Increase end-user education*. This is a crucial aspect of improving cybersecurity in the IoT, as many cyber vulnerabilities are already known, and related attacks are relatively easy to prevent. Policymakers should lend focus to the common use of key terms and definitions related to the IoT, as well as to efforts that inform end users across the business and consumer communities of proper steps to take to ensure that proper cyber "hygiene" is impressed.

Recommendation: Ensure Flexibility and Feasibility in Addressing Data Privacy

While the IoT will bring significant societal benefits, increased connectivity also gives rise to new risks and vulnerabilities. The ICT industry recognizes privacy as a priority in the success of the IoT and understands the wide range of related concerns held by policymakers. Industry believes that IoT services must adopt principles similar to those that have worked successfully on the Internet to enable informed consumer choice: transparency about what data will be collected, how it will be used, and who will have access. We urge regulators not to adopt privacy regulations that would make it impossible for IoT systems to flourish, as full consumer benefits will require that data be retained and used in ways not currently contemplated, even by IoT innovators themselves. Instead, industry should be allowed to adopt best practices that can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing. Policymakers are encouraged to ensure that their activities do not impose barriers that discourage the use of existing and developing voluntary efforts that are developed through standardization, best practice activities, and public-private partnerships to address privacy concerns. Internationally, policymakers should work towards interoperable privacy systems to avoid unnecessary impediments to the cross-border flow of information, which will be critical to the growth and functionality of the IoT.

...industry should be allowed to adopt best practices that can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing. Policymakers are encouraged to ensure that their activities do not impose barriers that discourage the use of the use of existing and developing voluntary efforts that are developed through standardization, best practice activities, and public-private partnerships to address privacy concerns.

Policymakers should avoid implementing privacy obligations that are ambiguous, overly burdensome, or technically infeasible. The effect of adopting such policies would be to decrease industry's incentive to invest in IoT opportunities due to resulting regulatory uncertainty and unnecessarily higher risk. Industry members exploring IoT opportunities should have certainty and the ability to determine the most appropriate method to meet any regulatory requirements. This approach would best promote the development of the IoT, as it is a fluid and quickly evolving market opportunity. TIA believes that any Government actions should be focused in areas where the circumstances in fact raise significant privacy and security issues. For example, if data is de-identified or aggregated it does not present the same level of security or privacy concerns as other types of data.

12 See NSTAC, NSTAC Report to the President on the Internet of Things (Feb. 19, 2014), available at https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf.

Further, Government guidance about the collection, use, and processing of data should be flexible to enable a range of possible technological means.

In addition, policymakers may serve an important role in ensuring IoT data privacy through public awareness efforts. Through "cyber hygiene" education efforts, many breaches that would result in a loss of data privacy can be avoided. In addition, a more informed end-user is less likely to make voluntary decisions with IoT devices and services that allow data usage beyond their individual comfort.

Conclusion

The IoT represents an immense opportunity for the improvement of the lives of citizens around the globe, across use cases. By ensuring that the path taken forward is collaborative and pro-innovation, consistent with the above recommendations, TIA believes policymakers can help these benefits materialize rapidly.

ABOUT TIA

The Telecommunications Industry Association (TIA) represents manufacturers and suppliers of global communications networks through standards development, policy and advocacy, business opportunities, market intelligence, and events and networking. TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment. Visit tiaonline.org for more details.

TIA is accredited by the American National Standards Institute (ANSI) and is a proud sponsor of ANSI's Standards Boost Business campaign. Visit www.standardsboostbusiness.org for details.

TIA Policy Committees & Divisions

TIA conducts its policy and government affairs Innovation Agenda through membership committees. A TIA Board Member serves as TIA's Policy Chair and represents TIA's Government Affairs activities on the TIA Board of Directors.

TIA's Communications Research Division, User Premises Equipment Division, and Wireless Communications Division are also represented on the TIA Board of Directors. The Chairs and TIA Staff for each committee, working group and division can be found at http://www.tiaonline.org/policy/tia-policy-committees-divisions.

For more information on TIA's Government Affairs activities, please contact Danielle Coffey, VP of Government Affairs, at dcoffey@tiaonline.org.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Headquarters
1320 N. Courthouse Rd.
Suite 200
Arlington, VA 22201
USA
Phone: +1.703.907.7700
Fax: +1.703.907.7727

tiaonline.org

○