THE INTERNET OF THINGS: EXPLORING THE NEXT TECHNOLOGY FRONTIER

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MARCH 24, 2015

Serial No. 114–26

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
21–271 PDF WASHINGTON : 2016

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 ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennesseem
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
FRED UPTON, Michigan *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
YVETTE D. CLARKE, New York
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
BOBBY L. RUSH, Illinois
G.K. BUTTERFIELD, North Carolina
PETER WELCH, Vermont
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

THE INTERNET OF THINGS: EXPLORING THE NEXT TECHNOLOGY FRONTIER

TUESDAY, MARCH 24, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:03 a.m., in room 2123 of the Rayburn House Office Building, Hon. Michael Burgess (chairman of the subcommittee) presiding.

Members present: Representatives Burgess, Lance, Blackburn, Harper, Guthrie, Olson, Kinzinger, Brooks, Mullin, Schakowsky, Cárdenas, Butterfield, and Pallone (ex officio).

Staff present: Charlotte Baker, Deputy Communications Director; James Decker, Policy Coordinator, Commerce, Manufacturing, and Trade; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Kirby Howard, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Olivia Trusty, Professional Staff, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; and Brendan Hennessey, Democratic Policy and Research Advisor.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. The Subcommittee on Commerce, Manufacturing, and Trade will now come to order. The Chair now recognizes himself for 5 minutes for the purposes of an opening statement. And again, I want to say good morning to everyone in the hearing room today and especially to our panel of witnesses as we begin to explore the emerging market in our digital ecosystem, the Internet of Things.

The Internet of Things marks a crucial juncture for the U.S. economy and for American consumers as our country looks for new economic engines and new sources for jobs. It promises a world in which digital and physical elements connect, gather information real-time, predict circumstances, prevent problems, and create opportunities.

This morning some of us attended the subcommittee's Internet of Things showcase. We saw first-hand some of the innovative ways that companies are using the Internet and networked sensors to create, enhance, and customize products to better meet consumer

preference. I thank all of the companies who participated in this morning's event.

The products and services displayed at the showcase represent how, in just a very short period of time, increased Internet connectivity, capability have led to the creation of a vast ecosystem in which machines, devices, appliances, and a whole host of other things are able to connect to the Internet.

We may be most familiar with this concept in the context of a connected refrigerator that lets us know what we need to purchase on our next trip to the grocery store or a smart watch that informs us when we have reached 10,000 steps or met our caloric intake for the day or a video monitor in our homes that can be watched remotely when traveling for work or vacation. These types of ground-breaking technologies, among many others, are providing valuable conveniences and invaluable information to users.

And yet this is just the beginning. Much of the excitement surrounding the Internet of Things lies in its immeasurable scope and potential to touch everything, to touch everyone, and every sector of the economy. We are already seeing the fulfillment of this promise as this technology expands to other areas and captures more than just objects and things.

Internet connectivity is being integrated into industrial processes, transportation routes, workforce practices, buildings, and other operational systems and entities across several different industries and environments. This is improving, this is revolutionizing the efficiency, productivity, and effectiveness of the way that individuals, businesses, and Governments are conducting various tasks and responsibilities. The Internet of Things, or the Internet of Everything, is fundamentally transforming the way we operate and participate in today's world.

The market is still very young. The potential for growth and innovation is at this point virtually limitless. As a physician, I see this potential first hand in the healthcare space. Medical professionals are able to interact with patients in revolutionary ways through connected devices, really devices that no one could have imagined just a few short years ago. This technology is offering opportunities to reduce healthcare costs, improve healthcare quality, and most importantly, to save lives.

The significance of the Internet of Things is that these types of benefits are not unique to healthcare. This technology truly has the potential to transform every sector of the economy in most profound ways. Notwithstanding the economic and societal benefits of the Internet of Things, the consumer impact of this market should be a key focus of our discussion today. While consumers are benefitting from the technologies, attention must also be given to appropriate consumer protections for privacy and security.

Today we will explore these issues, and we should recognize that not all devices are created equal. They are manufactured for different purposes. They have different capacities, and they generate varying levels and degrees of consumer information. Unlike other established markets, the Internet of Things is still developing, and quite honestly, we are trying to understand the nature and basis of the threats that face this ecosystem. In our examination of privacy and security issues, it is important that we balance these con-

cerns with the creativity and innovation that is driving this market. Too much potential for economic progress and consumer welfare is at stake to act without a full appreciation for what this market can offer.

[The prepared statement of Mr. Burgess follows:]

PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

The Internet of Things marks a crucial juncture for the U.S. economy and American consumers as our country looks for new economic engines and more jobs. It promises a world in which digital and physical elements connect and gather information in real-time to predict circumstances, prevent problems, and create opportunities.

This morning we attended the subcommittee's Internet of Things showcase. We saw first-hand the innovative ways in which companies are using the Internet and networked sensors to create, enhance and customize products to better meet consumer preferences and demand. I thank all companies that participated in this event.

The products and services displayed at this showcase represent how, in just a short period of time, increased Internet connectivity, capability, and use have led to the creation of a vast ecosystem in which machines, devices, appliances, and a whole host of other things are able to connect to the Internet.

We may be most familiar with this concept in the context of a connected refrigerator that lets us know what we need to purchase at our next trip to the grocery store; or a smart watch that informs us when we've reached 10,000 steps and met our caloric intake for the day; or a video monitor in our homes that can be watched remotely when traveling for work or on vacation. These types of ground-breaking technologies—among many others—are providing valuable conveniences and information to users.

And yet this is just the beginning. Much of the excitement surrounding the Internet of Things lies in its immeasurable scope and potential to touch everything, everyone, and every sector of the economy.

We are already seeing the fulfillment of this promise as this technology expands to other areas and captures more than just objects and things.

Internet connectivity is being integrating into industrial processes, transportation routes, workforce practices, buildings, and other operational systems and entities across several different industries and environments. This is improving and revolutionizing the efficiency, productivity, and effectiveness of the way individuals, businesses, and Governments are conducting various tasks and responsibilities. The Internet of Things—or the Internet of Everything—is fundamentally transforming the way we operate and participate in today's world.

While this market is still in its infancy, the potential for growth, innovation, and advancement is limitless. As a licensed physician, I see this potential first hand in the health care space. Medical professionals are able to interact with patients in revolutionary ways through connected devices that we only could have imagined just a few years ago. This technology is offering opportunities to reduce health care costs, improve health care quality, and most importantly, save lives.

The significance of the Internet of Things is that these types of benefits are not unique to health care. This technology truly has the potential to transform every sector of the economy in profound ways.

Notwithstanding the economic and societal benefits of the Internet of Things, the consumer impact of this market should be a key focus of our discussion today. While consumers are benefitting from these technologies, attention must also be given to appropriate consumer protections for privacy and security.

As we explore these issues, we should recognize that not all devices are created equally; they are manufactured for different purposes, have different capacities and generate varying levels and degrees of consumer information. Unlike other established markets, the Internet of Things is still developing and we are still trying to understand the nature and basis of threats facing this ecosystem. In our examination of privacy and security issues, it is important that we balance these concerns with the creativity and innovation driving this market forward. Too much potential for economic progress and consumer welfare is at stake to act without a full appreciation for what this market can offer.

Mr. BURGESS. I want to thank the witnesses again for making time to be with us here this morning. I look forward to an inform-

ative and engaged discussion on this very important topic and now would like to yield back my time and recognize the subcommittee ranking member, Ms. Schakowsky, for the purpose of an opening statement.

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Well, you don't think often of events in this building as being like really fun, and this is a day that we can say that it is because the showcase down the hall is very, very exciting. And we are going to hear about things that I think certainly can enhance and spice up and make our lives easier and better from incredible entrepreneurs. So I want to thank you all for being here today. I want to thank the chairman for holding the showcase and the hearing.

I would like to take a moment to introduce one of our witnesses, Brad Morehead, CEO of LiveWatch Security, which does have a demonstration over in the showcase. It is an innovative company from my hometown of Evanston, Illinois, that uses the Internet of Things technology to better protect, inform, and connect its customers. LiveWatch has been honored with the 2014 gold Stevie Award for Customer Service, the 2013 silver Stevie Award for E-commerce Customer Service, and was recognized as an enterprise leader by The Economist.

Mr. Morehead also participated in our showcase this morning. I welcome him and thank him for his time today as someone who often has people coming in and out of my house who don't always know the code on my security system and someone who regularly can't find her key. I want to tell you that these kinds of technologies can mean a lot in my life.

The Internet of Things is one of the fastest-growing technologies today. An estimated 25 billion products are now connected to the Internet, and that number is expected to double by 2020. Internet of Things technology brings very clear benefits to consumers, vehicles that can tell a driver if a part is in need of replacement, as the chairman mentioned, refrigerators can tell a parent to buy another gallon of milk, health gadgets that monitor a person's heart rate, running or walking speed, distance covered. All of these products and many more are made possible through the Internet of Things.

But this technology also presents some new challenges. How do we ensure that these technologies are secure? The chairman was right to raise the question of the important balance, that sensitive information doesn't get out to unintended audiences or that products connected to the Internet aren't remotely deactivated by an unauthorized user. We must ensure that as this technology continues to grow we take common-sense steps to assure that it is safe and secure.

These are issues worthy of the subcommittee's time and consideration. Again, I look forward to hearing from this distinguished panel about how they are creatively harnessing the Internet of Things, and I would yield at this time for Mr. Cárdenas.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JANICE D. SCHAKOWSKY

Thank you, Mr. Chairman, for holding today's showcase and hearing on the Internet of Things. I am eager to learn more from our distinguished panel about this technology's promise as well as the new challenges it presents.

I'd like to take a moment to introduce one of our witnesses—Brad Morehouse, CEO of LiveWatch Security. LiveWatch is an innovative company from my hometown of Evanston, Illinois, using Internet of Things technology to better protect, inform, and connect its customers. LiveWatch has been honored with the 2014 Gold Stevie Award for Customer Service, the 2013 Silver Stevie Award for eCommerce Customer Service, and was recognized as an enterprise leader by The Economist. Mr. Morehead also participated in our showcase this morning. I welcome him and I thank him for his time today.

The Internet of Things is one of the fastest-growing technologies today. An estimated 25 billion products are now connected to the Internet, and that number is expected to double by 2020.

Internet of Things technology brings very clear benefits to consumers. Vehicles that can tell a driver if a part is in need of replacement. Refrigerators that can tell a parent if they need an extra gallon of milk at the grocery store. Health gadgets that monitor a person's heart rate, running or walking speed, and distance covered. All of those products—and more—are made possible through the Internet of Things.

But this technology also presents some new challenges. How do we ensure that these technologies are secure? That sensitive information doesn't get out to unintended audiences? Or that products connected to the Internet aren't remotely deactivated by an unauthorized user? We must ensure that as this technology continues to grow, we take commonsense steps to ensure that it is safe and secure. These are issues worthy of this subcommittee's time and consideration.

Again, I look forward to hearing from our distinguished panel about how they are creatively harnessing the Internet of Things. I yield back.

Mr. CÁRDENAS. Thank you. Good afternoon. I want to thank the ranking member for yielding me some of her time. I want to introduce Brian Van Harlingen, the Chief Technology Officer at Belkin. Belkin is a local Los Angeles company, and we are proud of them. And they have been doing a great job as a driver for jobs and innovations in our great city.

Since the 1980s, Belkin has been on the forefront of innovation creating products that benefit all of our constituents in their daily lives. I look forward to watching how Belkin will use what we are calling the Internet of Things to bring new products and services to their consumers, and I look forward to their testimony today. So welcome to Washington, DC, and thank you so much for your testimony.

I yield back my time to the ranking member.

Mr. BURGESS. I thank the gentlelady. The Chair now recognizes the vice chairwoman of the full committee, the gentlelady from Tennessee, Ms. Blackburn, 5 minutes for an opening statement.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman. And I really do appreciate the attention to this issue and that my colleagues on both sides of the aisle are willing to work on this. We don't need to let this get away from us if you will. And Mr. Welch and I have put a great deal of attention on the privacy and data security issue for the past couple of years and thereby have had the opportunity with our colleagues to dig a little deeper into some of these issues.

Going back to the chairman's remarks, I think it is important that we look at size and scope when we discuss the Internet of

Things. You can look at Cisco's report, 50 billion devices, 50 billion devices connected to the Internet by the time we get to the end of this decade. And then you layer upon that what the expectations are for global economic output and contribution to the global economy from this. And right now and by the time we get to 2025, they are saying $2.7 to $6.2 trillion looking at that. So when you look at size and scope and impact, it behooves us to say, OK, how do we get our hands around this and make certain that we approach this in a light-touch way, that we encourage innovation? As Ms. Schakowsky said, we rely on a lot of these, and people like this because it does add convenience to our lives. But that accelerates the additional problem of privacy and security, whether it is B to B, or B to C, and how that is going to be filtered data and how we are going to mine it and what we are going to extrapolate and how we protect that, how we anonymize it, et cetera, et cetera. We have to realize that we are still running and hopefully always will on an open-source platform. Go back to when the Internet started, four known users, four disparate in varied locations, all known one to another, all vetted, all secure.

So we want to be here to enhance that experience for the 50 billion items that are going to be attached and still provide the underpinning and infrastructure that was there when it was the initial project of four known users.

So we welcome you all. We are going to be direct with our questions and probably a bit more conversational than some of the other hearings that you participate in.

Mr. Chairman, I thank you for the attention to the issue and look forward to the discussion. I yield the balance of my time for whomever would like to claim it.

Mr. BURGESS. Does any other member of the Republican side seek time? Seeing none, the gentlelady yields back her time. The Chair recognizes ranking member of the full committee Mr. Pallone, 5 minutes for an opening statement, please.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman. Today's hearing gives us an opportunity to look at a new and evolving technological development. The Internet of Things has great potential for growing the American economy and offering consumers new technology that will enrich their lives and empower them in ways never before thought possible.

Earlier today, along with my colleagues, I had an opportunity to see some of the innovation coming out of the Internet of Things at a showcase hosted by the subcommittee, and I was proud to have there IMPak Health, a New Jersey company that is building wireless technologies into products to solve practical healthcare needs. IMPak Health has taken advantage of wireless technology to help ensure patients are taking their medication and staying healthy. And the growth in these types of devices is so rapid that they soon will be as ubiquitous as electrical outlets. In fact, it is estimated that there will be 50 billion connected products by the year 2020.

But in many ways, the future is already here. Just last Friday Tesla announced that it would remotely install software updates in its Model S cars providing them with capability of autonomous driving. Cars that drive themselves were once found only in science fiction, but today it can be a reality with a quick update sent over the Internet.

Yet, along with these innovations come some new vulnerabilities, the vulnerabilities that we in Congress have a responsibility to protect consumers against. Let us take a hypothetical situation for a moment. Let us say that I wear a bracelet that monitors different aspects of my health and physical activity. It helps me keep track of how many steps I take each day. It tells me how well I sleep at night. It monitors my heart rate and along with an app in my phone, it tracks where I have gone. While, all this data is important to me, I may not want to have it released to a potential employer who requires it as part of the job application. I might not want the bracelet manufacturer selling it to an insurance company who might then utilize it for my insurance coverage, and I certainly do not want a hacker accessing the bracelet to post my information on the Internet or to monitor my location.

So without strong security and privacy protections, consumers can be at real risk. These risks can have devastating consequences when the product is accessed and controlled remotely by an unscrupulous actor. One hacker has shown that he can remotely access an insulin pump and induce a lethal overdose. Others have shown that they can remotely hijack the operations of a car, suddenly turning the wheel or cutting off the brakes.

In order to protect consumers, there has to be strong security and privacy protections built into these products. By building in security, manufacturers can more effectively prevent hackers from accessing a device or the data it produces or collects.

At last week's hearing, the FTC's witness stated that his experience in evaluating the vulnerability in Internet of Things products has led the agency to recommend that device security be added to data security and breach notification legislation. By building in privacy, consumers could have confidence in these products, and consumers need to know that their intensely personal information will not be shared with the world without their consent.

So I am confident great things will be done through the Internet of Things, but I believe that while we encourage innovation through these new technologies, we also have to be innovative in how we protect the consumer.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you, Chairman Burgess. Today's hearing gives us an opportunity to look at a new and evolving technological development. The Internet of Things has great potential for growing the American economy and offering consumers new technology that will enrich their lives and empower them in ways never before thought possible.

Earlier today, along with my colleagues, I had an opportunity to see some of the innovation coming out of the Internet of Things at a showcase hosted by the subcommittee. I was proud to have there iMPak Health, a New Jersey company that is building wireless technology into products to solve practical healthcare needs. iMPak Health is taking advantage of wireless technology to help ensure patients are taking their medication and staying healthy.

The growth in these types of devices is so rapid that they soon will be as ubiquitous as electrical outlets. In fact, it is estimated that there will be 50 billion connected products by 2020.

But in many ways, the future is already here. Just last Friday, Tesla announced that it would remotely install software updates in its Model S cars providing them with capability of autonomous driving. Cars that drive themselves were once only found in science fiction, but today it can be reality with a quick update sent over the Internet.

Yet, along with these innovations come new vulnerabilities—vulnerabilities that we in Congress have a responsibility to protect consumers against.

Let's take a hypothetical situation for a moment. Let's say that I wear a bracelet that monitors different aspects of my health and physical activity. It helps me keep track of how many steps I take each day, it tells me how well I sleep at night, it monitors my heart rate, and along with an app in my phone, it tracks where I have gone.

While all of this data is important to me, I may not want to have to release it to a potential employer who requires it as part of the job application. I may not want the bracelet manufacturer selling it to an insurance company who might then utilize it for my insurance coverage. And I certainly do not want a hacker accessing the bracelet to post my information on the Internet or to monitor my location.

Without strong security and privacy protections, consumers can be at real risk. These risks can have devastating consequences when the product is accessed and controlled remotely by an unscrupulous actor. One hacker has shown that he can remotely access an insulin pump and induce a lethal overdose. Others have shown that they can remotely hijack the operations of a car, suddenly turning the wheel or cutting off the brakes.

In order to protect consumers, there has to be strong security and privacy protections built into these products.

By "building-in" security, manufacturers can more effectively prevent hackers from accessing a device or the data it produces or collects. At last week's hearing, the Federal Trade Commission's witness stated that its experience in evaluating the vulnerability in Internet of Things products has led to the agency recommending that device security be added to data security and breach notification legislation.

By "building-in" privacy, consumers can have confidence in these products. Consumers need to know that their intensely personal information will not be shared with the world without their consent.

I am confident great things will be done through the Internet of Things. But I believe that while we encourage innovation through these new technologies, we also must be innovative in how we protect the consumer.

Mr. PALLONE. I yield back. I don't think any other member on our side wants the time. So I will yield—oh, you do? OK. I will yield my remaining time to the gentleman from California.

Mr. CÁRDENAS. Thank you very much. I would be remiss if I didn't take this opportunity to thank Intel. So Ms. Schooler, I just wanted to say thank you very much. Intel made an announcement just a few months ago that they are investing $300 million into their internal diversity initiatives over at Intel, and I hope that would be a starting point for all of the industries to follow suit as these industries are growing. They are the jobs of the future. And for Intel to make that commitment and that self-assessment is just wonderful. And many people on both sides of the aisle believe that industry does a great job when they police themselves and when they look in the mirror and they say we can do better. And I think this is a great opportunity for us to remind everyone that self-reflection and self-understanding of where we stand as individuals or organizations in the community certainly would give us an opportunity to step forward and say we can do better. And I think Intel has done a tremendous job, and thank you for that commitment.

Thank you. I yield back my time.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back.

So again, we want to welcome all of our witnesses, and thank you for agreeing to testify before the subcommittee today. Our witness panel for today's hearing will include Mr. Daniel Castro who is the Vice President of the Information Technology and Innovation Foundation; Mr. Brian Van Harlingen who is the Chief Technology Officer of Belkin International; Ms. Rose Schooler, Vice President of the Internet of Things Group and the General Manager of the Internet of Things Strategy and Technology Office at Intel Corporation; and Mr. Brad Morehead, the Chief Executive Officer at LiveWatch Security.

You each are going to be recognized in turn for 5 minutes for the purposes of an opening statement. Mr. Castro, we will begin with you. You are recognized for 5 minutes.

STATEMENTS OF DANIEL CASTRO, VICE PRESIDENT, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION; BRIAN VAN HARLINGEN, CHIEF TECHNOLOGY OFFICER, BELKIN INTERNATIONAL, INC.; ROSE SCHOOLER, VICE PRESIDENT, INTERNET OF THINGS GROUP, INTEL CORP.; AND R. BRAD MOREHEAD, CHIEF EXECUTIVE OFFICER, LIVEWATCH SECURITY, LLC

STATEMENT OF DANIEL CASTRO

Mr. CASTRO. Thank you. Thank you, Chairman Burgess, Ranking Member Schakowsky, and members of the committee. I appreciate the opportunity to discuss the Internet of Things with you today.

The Internet of Things represents the idea that ordinary objects will be imbedded with sensors and connected to the Internet. While many of these changes will be subtle, over the long term, this technology could ultimately have an enormously positive impact on individuals, businesses, and society. For example, consider healthcare. Individuals can use connected devices to prevent, screen, and diagnose a variety of medical conditions. By collecting and tracking data about their health, individuals can identify health problems sooner, get treatment faster, and save on healthcare costs.

For example, patients can use smart pill bottles to receive automated alerts when it is time to take a dose, and these types of interventions can help decrease the rate of medication non-compliance which costs the United States almost $300 billion annually.

Or look at energy. The Internet of Things is helping to provide solutions to the global energy challenge by enabling clean energy technologies. For example, in home, connected devices like smart thermostats can automate energy efficient practices and save consumers money.

Or look at public safety. The Internet of Things helps build not only smarter cities but safer cities. In homes connected sensors can improve safety by detecting fires and other emergencies quickly and reliably and alert authorities sooner.

In vehicles, the sensors can detect a crash and automatically alert emergency responders about the vehicle's location and the number of occupants. Some of these systems can even predict the injuries that might have resulted.

The availability of this real-time data is crucial in an emergency since the faster response time can mean the difference between life and death.

The Internet of Things is transforming industries like manufacturing as well. Using low-cost sensors in automation, factories can automatically turn off the lights and air-conditioning when the workers leave, shut off valves if sensors detect leaks, and shut down dangerous equipment if sensors detect a malfunction. Innovative manufacturers can use the data collected on the factory floor to gain insights about the physical fabrication process, thereby improving efficiency, increasing yields, and reducing product defects.

Manufacturers can also use sensors to collect real-time data such as temperature and moisture about their shipments to help ensure quality and optimize logistics. More information can mean the difference between a recall and a successful shipment.

As you can see, a significant amount of the data collected by the Internet of Things will not involve information about individuals but instead will be about the environment, factories, vehicles, infrastructure, and other electronic devices. And when data is collected about people, much of it will be de-identified and aggregated. But when it comes to personal privacy, Congress should tread lightly so as to avoid impeding innovation. In particular, Congress should recognize the privacy principles designed for a small-data world do not work in a big-data world. Proposals such as data minimization are based on the mistaken belief that it is always possible to predetermine what information is useful in the early stage and collect only that minimum amount. Many of the benefits from data come from exploratory analysis that finds new trends, relationships, and insights that were not obvious at the outset. Restricting data collection could severely curtail the many potential benefits of the Internet of Things.

As more devices are connected to the Internet, it will be more important than ever that they incorporate strong security features. While the private sector is moving in the right direction, Congress should further incentivize companies to adopt strong security practices by adopting policies that decrease the cost of strong security and increase the cost of weak security. For example, Congress should pass data breach notification legislation that preempts State laws and reduces the legal compliance costs companies face from abiding by multiple rules. This will allow them to focus more resources on improving the security of their products.

Congress should also pass cybersecurity information sharing legislation to help organizations respond to real-time threats.

Finally, Congress should encourage universities to integrate cybersecurity training and to technical degrees so that the next generation of coders and engineers build strong security into their products. By improving education, Congress can help raise the bar for security across the entire U.S. tech sector.

The success of the Internet of Things will depend in part on the actions of Congress. Just as the United States needed a national broadband strategy, it also needs a national strategy for the Internet of Things. Not only should Congress avoid policies that would impose costs, limit innovation, and slowed adoption, they should actively support accelerating the development and deployment of the

Internet of Things, such as by creating pilot projects for smart cities, encouraging smart infrastructure projects, and designing an efficient regulatory review process for wearable health technologies.

The Internet of Things has the potential to positively impact virtually every industry from agriculture to healthcare, and the Federal Government should be an active partner in ensuring its success.

Thank you for the opportunity to speak with you today. I look forward to your questions.

[The prepared statement of Mr. Castro follows:]

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

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

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

March 24, 2015

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

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

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

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

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

Health Care

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

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

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

Public Safety

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

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

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

Energy Use

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

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

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

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

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

The Internet of Things Is the Foundation for Smart Manufacturing

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

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

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

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

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

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

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

Privacy

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

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

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

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

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

Security

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

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

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

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

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

Conclusion

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

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

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

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

References

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

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

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back. Mr. Van Harlingen, you are recognized for 5 minutes for the purpose of an opening statement, please.

STATEMENT OF BRIAN VAN HARLINGEN

Mr. VAN HARLINGEN. Thank you, and good morning, Chairman Burgess, Ranking Member Schakowsky, and members of the committee. Thank you for holding this important hearing on the Internet of Things, otherwise known as IoT. My name is Brian Van Harlingen, and I am the Chief Technology Officer at Belkin International.

Belkin is the maker of the WeMo home automation brand, which allows users to remotely measure, monitor, and manage their homes via a software suite including applications, cloud infrastructure, and a portfolio of more than 25 connected devices. Surpassing 1 million activations, the WeMo ecosystem ranges from switches to lighting to home appliances.

After years of talk, the Internet of Things has arrived, and the pace of innovation is accelerating at a phenomenal speed. We are pleased that Congress and other policy makers have joined the conversation, as policy awareness and leadership will help to maximize the benefits of this technological revolution and ensure consumer confidence. IoT will drive economic growth, create jobs, and facilitate entrepreneurship in completely new markets.

In my testimony, I will discuss three key topics: consumer benefits, technological considerations, and privacy and security.

First, consumer benefits. WeMo has been designed as the most approachable entry point into the smart home. Affordable and easy to use, WeMo provides bite-sized solutions to make consumers' lives easier, simpler, and better. WeMo's new Echo technology uses the home's existing infrastructure to monitor, measure, and manage water, electricity, and natural gas usage. Using advanced data science and machine learning, these technologies have enormous potential to save both money and resources.

As a connected solution, WeMo gains insight into how consumers use WeMo devices in order to provide better experiences and design future products. For example, through data analytics, we learned that consumers were finding ways to turn on their devices at sunrise and sunset, so we built that functionality directly into our WeMo app. We also learned that most WeMo Switch users were using them for lighting purposes. So we developed and marketed the WeMo Light Switch as our next product. These are examples of how we use the data from the WeMo cloud to drive better experiences for our consumers.

Second, technological considerations. IoT for the home and business cannot exist without two primary technologies: Wi-Fi and smart devices. As the maker of both WeMo and Linksys Wi-Fi routers, Belkin understands both markets. Wi-Fi has been widely adopted with a 61 percent penetration rate in U.S. homes. WeMo products use familiar Wi-Fi technology. They do not rely on hubs for connectivity or intelligence. WeMo can integrate directly into partner products and serve as an on-ramp to the Internet of Things for everyday products like Crock-Pot slow cookers, Mr. Coffee coffeemakers, and Osram Sylvania light bulbs.

From a policy perspective, the Government and Congress can help promote and grow the Internet of Things by making sure these devices can talk to each other. Wireless spectrum, already an important technology policy issue, becomes even more important as IoT adoption accelerates and billions of new devices come on line. Congress and the FCC should continue to free up new spectrum, particularly on an unlicensed basis. Failure to expand spectrum will stifle IoT innovation and growth.

Last but not least, privacy and security. At WeMo, we believe the nascent IoT market will benefits when consumers know privacy and security are our top priorities. We believe the Federal Government can take a light-touch regulatory approach and work with the industry to ensure consumer confidence.

We applaud this committee's efforts to pass data breach legislation that would address the patchwork of State data breach laws. WeMo has a very transparent data policy and strictly controls all PII. The data collected from WeMo devices is aggregated and anonymized. Non-personal information is used to identify trends, to improve network performance, and to provide additional benefits to consumers. We understand the importance of data security and employ a combination of industry-led security standards, procedures, and organizational measures.

We have safeguards in place to prevent security breaches and work closely with outside security researchers to identify and address potential security vulnerabilities. We support the latest security applications and continuously improve and push consumer device firmware and application updates. Security will always be a top priority, and as the technology evolves, so will our efforts to provide safe and secure products for consumers.

In conclusion, at WeMo, we are focused on delivering the most user-friendly, innovative, and secure products. I appreciate the opportunity to testify today and to share our vision of the Internet of Things and answer any questions the committee might have.

[The prepared statement of Mr. Van Harlingen follows:]

Statement of
Brian Van Harlingen, Chief Technology Officer, Belkin International
Before the
House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade
Hearing on
"The Internet of Things: Exploring the Next Technology Frontier"
March 24, 2015

Good morning, Chairman Burgess, Ranking Member Schakowsky and Members of the Committee. Thank you for holding this important hearing on the Internet of Things. My name is Brian Van Harlingen and I'm the Chief Technology Officer at Belkin International.

Belkin International is the maker of the WeMo home automation brand, which is at the forefront of the Internet of Things. WeMo technology allows users to remotely measure, monitor and manage their home electronics via a software suite including an application, cloud infrastructure and portfolio of more than 25 connected devices. The WeMo ecosystem includes everything from switches and lighting to home appliances and DIY maker solutions, and is available in more than 130 countries around the world. Surpassing one million activations, WeMo is a market leader in delivering exceptional experiences for the Internet of Things. Our products can save energy, help reduce water use, and generally make our lives easier to manage.

After years of talk, the Internet of Things (IoT) has arrived and the pace of innovation is accelerating at a phenomenal speed. We are pleased Congress and other policy makers have joined the conversation, as policy awareness and leadership will help to maximize the benefits of this technological revolution and ensure consumer confidence. IoT will drive economic growth and create jobs through creative consumer use of smart devices, improving productivity using advanced manufacturing capabilities, and facilitating entrepreneurship in completely new areas that rely on connected smart technology.

The Internet of Things will reinvent the way people live around the world as more everyday physical objects connect to the Internet and become intelligent. Consumers are still acclimating to the digital world controlling the physical, but platforms like WeMo will help spur the transition by helping consumers realize real and tangible benefits. Because of this, WeMo is confident in our role in IoT and will remain focused on being the most approachable entry point to the smart home, driving unparalleled user experience, and bringing value to consumers by making everyday life simpler, easier and better.

In my testimony, I will discuss three key areas in the development of IoT: consumer benefits, technological considerations, and privacy and security.

Consumer Benefits

WeMo, as a part of Belkin International, has more than 30 years of experience in the consumer electronics industry. We have seen the lifecycle of devices and technology time and time again

– from portable stereos to MP3 players, VCRs to DVD players, flip phones to smart phones. As a company, we have lived through this evolution and know how both technology and consumer adoption changes over time. This understanding, coupled with a commitment to innovation and putting the consumer first, has enabled us to develop strong consumer trust and confidence.

From the beginning, WeMo was designed as the most approachable entry point to the smart home. Affordable, easy to use, scalable and infinitely customizable, the goal of WeMo has always been to help people tailor their daily functions one solution at a time to make life easier, simpler and better. This allows consumers to scale their smart home at their own pace in an affordable, easy way.

Though the IoT has grown immensely, the reality is that the technology still does not live up to the promise of full, anticipatory automation, or automation without consumer input. WeMo is actively driving towards a more intelligent home with its new WeMo Water and Power with Echo technology that uses the home's existing infrastructure to accurately monitor, measure and manage systems such as water, electricity and natural gas. Using advanced data science and machine learning technologies, WeMo Water and Power push the boundaries of what is currently possible in IoT and have enormous potential to save both money and natural resources across a variety of industries.

As a connected solution, WeMo offers insight into how consumers are using their WeMo devices and which app features they use most often. We can then use that to provide better app experiences, as well as roadmap future products tailored directly to consumer preferences. For example, when WeMo launched an "If This Then That" or IFTTT channel, we were able to see that Sunrise/Sunset rules were especially popular and were then able to go back and build that functionality directly into the WeMo app. Additionally, we were able to see that most WeMo Switch users were using it for lighting purposes, so we changed direction and brought to market the WeMo Light Switch as our next product, directly in line with consumer desire. These are examples of how we use the data from the WeMo cloud to drive better experiences for our consumers.

Technological Considerations

IoT for the home and business cannot exist without two primary technologies: Wi-Fi and smart devices. As a company, Belkin has a deep history and understanding of both. Belkin has been making accessories for smart devices since the first iPod launched back in 2001. We also have a deep history in wireless networking, with more than a decade of experience on the Belkin side, and more than 30 years on the Linksys side. Linksys will soon ship its 100 millionth router, so it is safe to say we have significant experience in building wireless networking products. We understand the complexities of both the smart device and networking markets, and know what goes into building products that consumers want and need. IoT is at the crossroads of our two largest businesses, which places us in a unique and beneficial position among players in the industry.

WeMo is focused on the consumer experience and the delivery of a future-proof architecture, which is why all WeMo products use Wi-Fi as the core connection standard. Wi-Fi has become ubiquitous in homes and businesses across the globe, with about a 70 percent penetration rate in US homes. Relying on Wi-Fi makes it easier for consumers and businesses to adopt new smart devices and technologies because they are already familiar with that core technology. WeMo products do not rely on hubs to connect to the network; rather they can operate in either an independent or connected manner. For example, WeMo technology can integrate directly into partner products and serve as an on-ramp to the Internet of Things for legacy products like Crock-Pot and Mr. Coffee. We can also work with existing smart devices through back-end technologies and standards to create a compatible product platform, such as our work with lighting manufacturer Osram Sylvania. Current partners and products include household and kitchen appliances like Crock-Pot Smart Slow Cooker with WeMo, Mr. Coffee Smart Coffee Maker with WeMo, Holmes Smart Air Purifier with WeMo, Holmes Smart Air Purifier with WeMo and Holmes Smart Console Heater with WeMo, as well as a variety of different lighting options from Osram Sylvania's Lightify brand. By combining our partners' user insights and market efficiencies, we are able to bring WeMo's simple, approachable platform and user experience to additional products and devices throughout the home, which helps expand the WeMo ecosystem to a new audience.

Although WeMo uses Wi-Fi as the primary method to directly connect users to the network, some industry players like Wink, Iris, and SmartThings are focusing their strategy on connecting multiple products to the network through aggregator hubs. These hubs work to integrate multiple devices that may use different standards into one control system. Hubs can be valuable for very sophisticated early adopters who own multiple IoT or home automation devices like ZigBee, Z-Wave, Bluetooth and Lutron devices. However, every wireless radio included in the hub increases the cost and complexity of the technology. Further, sophisticated hub systems require an educated sales force and technical assistance for consumers. WeMo strongly believes that our efforts are better spent on delivering delightful and uncomplicated experiences for our users that do not rely on complicated integration services. Rather, integration will happen where and when there is a clear and lasting value for consumers. Bringing together multiple systems and functions is a clear direction for the future, but we do not want to alienate the mass market with costly and complicated technology that diminishes user experience and functionality.

From a policy perspective, the government and Congress can help promote and grow the Internet of Things by making sure all the "things" can talk to each other. The evolution of IoT will add billions of new devices to our wireless networks. In other words, our airwaves will soon be very crowded and noisy. At WeMo, we are working with our corporate subsidiary Linksys to ensure the most efficient and consumer friendly use of spectrum in our products.

Wireless spectrum, already an important technology policy issue, becomes even more important as IoT adoption accelerates. Congress and the Federal Communication Commission are continually working to free up new spectrum, particularly on an unlicensed basis. Unfortunately,

the progress is slow, which is at odds with the rapid growth of IoT devices. Failure to expand available spectrum for these uses has the potential to stifle important growth in this area.

Also important to the future of IoT is research and development. WeMo recently received a grant from the Department of Defense's Environmental Security Technology Certification Program (ESTCP) to reduce facility energy costs at two test sites in the western United States using the sensor and machine learning algorithms developed by WeMo Power. We also have a close relationship with the University of Washington's Computer Science & Engineering School and its Ubicom Research Lab through our Chief Scientist and UW professor, Dr. Shwetak Patel. Through this relationship, we are able to keep WeMo on the forefront of the latest advancements in IoT technology.

Privacy and Security

One of the top policy issues in both Washington and in our industry is privacy and security. At WeMo, we share this priority. The Internet of Things in general will benefit when consumers know the whole industry is working hard to build privacy and security into IoT devices. At WeMo, we aim for the highest standard, and believe the federal government should continue with its light touch approach that will be helpful in allowing the industry to innovate while keeping consumers safe.

We applaud this Committee's effort to pass data breach legislation that would address the patchwork of state data breach laws. WeMo complies with privacy laws on the collection of personally identifiable information (PII) and has a very transparent privacy policy. The data collected from WeMo devices is aggregated and anonymized, and only non-personal information is used to identify trends, devices, network health; to improve network performance; and to provide additional benefits to consumers such as better overall experiences. We understand the importance of data security and have taken steps to protect PII from unauthorized access, use or disclosure by a combination of industry-standard security technologies, procedures and organizational measures.

In light of the recent FTC report and your efforts on data breach legislation, WeMo agrees wholeheartedly that consumer trust is an essential step in enabling IoT to reach its full potential. Like all technology systems, security for IoT devices and WeMo's own IT system is an arms race. While no system will ever be 100 percent secure, we have safeguards in place to prevent security breaches and work closely with outside security researchers to identify and address potential security vulnerabilities before they become a reality. We support the latest security applications and continuously update consumer firmware and device apps to address any vulnerabilities that may arise. We push the updates to our customers and urge them to use the latest versions to promote the best security. Security will always be a huge priority and, as the technology evolves, so will our efforts change to provide as safe and secure a network as we can for consumers.

Conclusion

As the CTO for WeMo, I spend every day thinking about delivering the best products and making sure we meet our customers' expectations. I appreciate the opportunity to testify today to share our vision of the Internet of Things and answer any questions you might have about our products or the industry.

While some innovators ignore Washington and shy away from policy questions like providing more spectrum and protecting consumer privacy, at WeMo, we believe Congress and the government can help the IoT market evolve by educating the public and continuing its light-touch regulatory approach. The Internet of Things has the potential to create jobs and drive true transformation within homes and businesses. We look forward to working with policymakers both in Congress and the Administration as partners in the future of the Internet of Things.

Mr. BURGESS. The Chair thanks the gentleman. The Chair now recognizes Ms. Schooler 5 minutes for the purpose of an opening statement, please.

STATEMENT OF ROSE SCHOOLER

Ms. SCHOOLER. Good morning, Chairman Burgess, Ranking Member Schakowsky, and members of the subcommittee. Thank you for the opportunity to provide testimony on the importance of the United States' establishing a global leadership role in the Internet of Things or the IoT.

As head of Intel's IoT's Strategy and Technology Office, own the IoT strategy for the company. Intel's 30 years of investment, innovations, and standards leadership in the evolution of computing provide the foundational elements of the strategy. Intel believes the IoT presents a transformational opportunity for the United States and for the world. It will enable innovation, increase productivity, and deliver efficiencies across the public and private sector. While some think of the IoT as smart thermostats and wearables, these consumer devices are only a few of the many applications. The primary economic driver will be non-consumer areas such as industrial and commercial applications. I will address three topics that are important to consider as you chart your policy. One: Why is the IoT important? Two: What are the barriers to a successful IoT ecosystem? And three: How can policymakers accelerate deployments to ensure U.S. leadership?

First: Why is the IoT important? It will drive unprecedented benefits for Government, businesses, consumers, and communities. It is estimated that 50 billion devices will connect to the Internet by 2020 generating 44 zettabytes of data. Consider that in 2009, the World Wide Web was estimated at just a half a zettabyte. The IoT presents the opportunity to connect these devices, efficiently analyze the data, and use the information to improve our decision-making. In doing so, the IoT is expected to have a multitrillion-dollar global economic impact. What should most excite U.S. policymakers is that America and other developed economies are expected to capture 20 percent of this impact if we lead.

Let us consider one IoT application. Saia Trucking is located in Georgia and has a nationwide fleet of 3,000 trucks. They recently deployed an Intel-based IT solution which alters routes and guides drivers' performance real-time. Saia increased fuel efficiency by 6 percent translating into $15 million of annual savings. The U.S. trucking industry consumes 54 billion gallons of fuel per year. Extrapolating that success, our Nation could save over 3 billion gallons of fuel yearly while reducing our CO2 emissions.

What are potential barriers to a successful IoT ecosystem? One barrier as noted could be security. It is not implemented from the outset. For this reason, Intel prioritizes security as the foundational element of our IoT strategy. We will integrate security at the outset building cryptography into our chips to enable strong identity and data protection. In addition to the compute device itself, our solutions will employ advanced software security to prevent harmful applications from being activated on the device or taking down the network. Integrating multiple layers of security at

the outset enables trusted data transmission necessary for successful IoT deployments.

Other potential barriers include connecting to legacy infrastructure, interoperability between devices, and developing global standards. To address these barriers, Intel collaborated with industry leaders to define five tenants of successful IoT solutions. They are security, ease of connectivity, interoperability, data analytics, and ease of deploying new applications and services. Based on these tenants, we recently launched the Intel IoT platform.

Finally, how can policymakers accelerate IoT deployments to ensure U.S. leadership? Candidly, the United States is behind. Other countries are aggressively investing and deploying IoT implementations to transform their economies, address societal problems, and spur innovation. China, Brazil, Germany have all adopted national IoT plans with time-bound goals and are investing heavily in IoT R&D and infrastructure. The United States must leverage our vast resources and capabilities, promoting industry alignment around these large-scale IoT deployments based on secure, open, and interoperable solutions will showcase U.S. leadership.

Congress can advance our Nation's IoT momentum by collaborating with industry to establish a national IoT strategy, encourage public/private partnerships, and invest in IoT research. Intel is confidence that the United States can lead the IoT transformation with a continued open dialogue as you are doing here today and by implementing some of these recommendations.

Thank you for your time, and I look forward to your questions.

[The prepared statement of Ms. Schooler follows:]

PREPARED STATEMENT FOR THE RECORD OF

INTEL CORPORATION

For the

UNITED STATES HOUSE OF REPRESENTATIVES

ENERGY AND COMMERCE SUBCOMMITTEE ON

COMMERCE, MANUFACTURING, AND TRADE

On

THE INTERNET OF THINGS:

EXPLORING THE NEXT TECHNOLOGY FRONTIER

MARCH 24, 2015

Intel Corporation ("Intel") respectfully submits this statement for the record in conjunction with the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade's hearing on "The Internet of Things: Exploring the Next Technology Frontier." Our statement focuses on the opportunity to unleash the vast potential of the Internet of Things (IoT) through public-private partnerships and to create a leadership opportunity for the U.S. in this multi-industry transformation.

Witness: Rose Schooler is a Vice President within Intel's worldwide IoT Group (IOTG) and general manager of Intel's IoT Strategy and Technology Office. Rose has been an Intel employee for nearly three decades, beginning her Intel career as a graduate rotation engineer, followed by positions in process engineering in wafer manufacturing, corporate quality and reliability, and marketing. For more than a decade, Rose has run Intel's worldwide networking business and now leads Intel's IoT Strategy and Technology Office. Her organization is responsible for the company's IoT strategy – consisting of hardware, software, security and services across a wide range of IoT market segments, including transportation, manufacturing, healthcare, retail, smart home, smart buildings and smart cities. For the past 30 years, Intel has made significant investments, driven exciting innovations, led standards activities, and supported what has evolved to become the Internet of Things. At Intel, we like to say IoT is an overnight transformation thirty years in the making.

INTEL AND THE INTERNET OF THINGS

Intel's Role

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

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

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

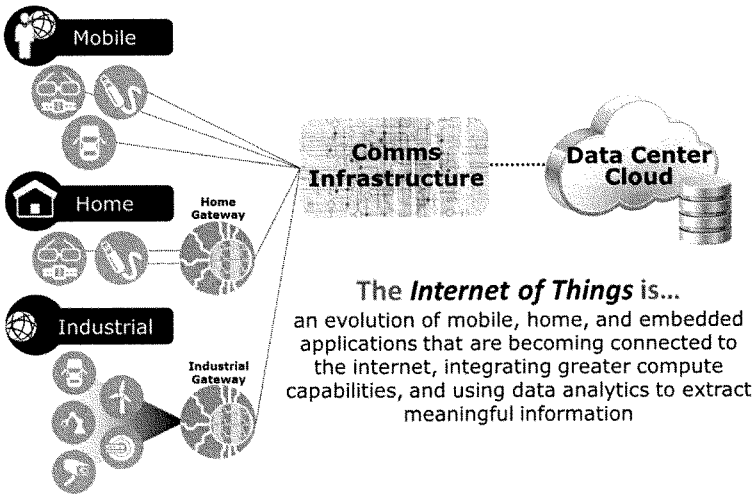
In the late 2000s, "Machine to Machine" (M2M) emerged. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. Before M2M, people had to be physically located at the machine to analyze the data to make decisions for managing each machine.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

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

IOT DEFINITION

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

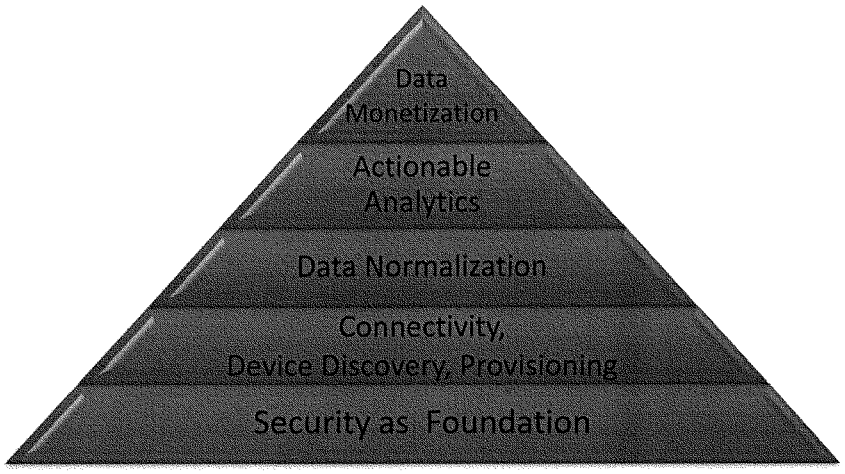
[1] A gateway is a node on a network that serves as an entrance to another network.



THE FIVE CRITICAL TENETS OF IOT

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

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



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

IOT: A TRANSFORMATIONAL OPPORTUNITY BUILT ON A FOUNDATION OF SECURITY

With respect to the critical element of security, Intel values this first and foremost. We believe that security is the foundation of IOT and it is fundamental to Intel's roadmap planning. We have dedicated security products and security features embedded into both our hardware and software products. Our hardware and software are being designed from the beginning to be secure. This is important for trusted data exchange in the IoT, as data generated by devices and

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

existing infrastructure must be able to be shared among the cloud, the network, and intelligent devices for analysis. This enables users to aggregate, filter and share data from the edge of the network all the way to the cloud with robust protection. Moreover, data must be accurate to be beneficial. Intel prioritizes the security, accuracy, privacy and integrity of data in all market sectors, and especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. Intel understands that we must deliver and evoke consumer and industry trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

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

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

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

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

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

IOT PRIORITIES – ENABLERS OF SCALE

Security

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

Interoperability

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

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

---

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

Open Standards

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

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

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

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

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

[5] http://openinterconnect.org/

MARKET TRENDS DRIVING THE EMERGENCE OF IOT

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

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

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

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

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

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

---

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

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

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

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

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

Smart Cities: Intel has partnered with the city of San José, California in a public-private partnership to further the city's 'Green Vision' goals. This Smart Cities Project, announced as part of the Smart America Challenge in 2014,[10] is expected to help drive San José's economic growth, foster 25,000 clean-tech jobs, create environmental sustainability and enhance the quality of life for residents. Together, Intel and San José City Management are deploying a network of sensors to create a "sustainability lens" that uses Intel IoT technology to measure characteristics such as particulates in the air, noise pollution and traffic flow. This real-time city data will produce meaningful insights that enable the City to make better management decisions, and lead to improvements in air quality, transportation efficiency, environmental sustainability,

[8] *Id.*

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

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

health, and energy efficiency. Consider the U.S. potential opportunity: The ten largest U.S. cities alone have an aggregated population of 25,292,500 people.[11] What if we initially focused on 10 cities, 10 counties, and 10 rural towns from across the nation and implemented IoT "smart city" solutions into those communities?

IOT: EXTRAORDINARY POSITIVE IMPACT ON U.S. GDP

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

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

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

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

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

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

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

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

[17] *Id.*

could boost average incomes in the U.S. by an exceptional 25 to 40 percent over the next twenty years.[18]

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

RECOMMENDATIONS FOR POLICYMAKERS

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

1. **Continue an open dialogue with industry, experts and stakeholders as you are doing today.** This IoT hearing is a promising start and the right first step. Intel believes that an open, multi-stakeholder process can best enable a secure and vibrant IoT ecosystem. Also, legislators may want to consider encouraging the Department of Commerce to create a non-partisan National IoT Advisory Board of policymakers, agency representatives, industry leaders, think tanks, academia, and leaders of IoT-focused consortia like IIC and OIC.

2. **Encourage focus on security and interoperability as critical foundational elements of IoT.** While industry is in the best position to develop and determine security and interoperability solutions, government can encourage industry alignment around large-scale IoT deployments based on secure, open and interoperable IoT solutions. This will enable deployments to scale quickly and provide both short-term and long-term economic and social benefits to consumers, government, and businesses.

---

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

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

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

3. **Encourage open standards and open architectures** to maintain the long term viability of IoT, based on an approach that is scalable, interoperable and reusable across a variety of use case deployments, vendors and sectors. While industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, government should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards. Specifically, government should encourage the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

4. **Collaborate with the industry to develop a U.S. National IoT Strategy** with time-bound goals for sector-specific IoT deployments over the next 3 to 5 years. These deployments will not only address critical societal issues and save tax payer dollars, but also will demonstrate U.S. leadership. A National IoT Strategy will help align IoT stakeholders and incentivize innovation, ultimately creating value for society by increasing efficiencies and productivity, creating jobs, sustaining our environment, and improving quality of life in our cities and towns.

5. **As part of our National IoT Strategy, encourage Public-Private Partnerships (PPPs)** to address societal problems and accelerate more rapid deployment of IoT solutions. Government and industry collaboration can be one of our nation's best assets to accelerate the adoption of a world-class IoT ecosystem. Viable PPPs will make IoT deployments an appealing investment for both government and industry, while ensuring scalability and sustainability of infrastructure and technological innovation over the long term. Notably, countries like China,[21] the UAE,[22] Malaysia,[23] Germany[24], Brazil[25] and others are moving

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

[22] The Telecommunications Regulatory Authority, in collaboration with the Prime Minister's Office, is working to announce The National Plan for UAE Smart Government Goals: http://www.tra.gov.ae/news_The_TRA_to_announce_The_National_Plan_for_UAE_Smart_Government_Goals-636-1.php.

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

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

aggressively ahead on IoT deployments – establishing national IoT plans and blueprints establishing time-bound measurable goals, investing substantial funding in IoT research and deployments, and launching PPPs to jumpstart these opportunities and quickly enable IoT scale. As these other countries have recognized, a vibrant and state-of-the-art IoT ecosystem is critical to a nation's global competitiveness and economic stability in the 21st century. By adopting and implementing a National IoT Strategy, the U.S. can seize the leadership position in this next evolution of computing.

PUBLIC-PRIVATE PARTNERSHIPS – MARKET SEGMENT FOCUS

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

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

Impact – Logistics and Transportation was a $1.3 trillion industry in the U.S. in 2012, and represented 8.5 percent of GDP. With almost 9 percent of the U.S. labor force employed in the transportation sector and the U.S. spending roughly $160 billion annually on highway infrastructure (about ¼ funded by the federal government), a more efficient and effective trucking industry has the potential to yield significant savings to the U.S. economy. For

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

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

[27] *Federal Motor Vehicle Fleet Report FY 2012*, http://www.gsa.gov/portal/mediaId/181179/fileName/FY_2012_Federal_Fleet_Report.action.

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

example, the commercial trucking industry in the U.S. uses about 50 billion gallons of fuel each year. A 7 percent increase in fuel efficiency results in more than 3.5 billion gallons of fuel saved. Imagine if we set a national goal for 25 percent of the Federal Fleet in 3 years, and 50 percent in 5 years, be retrofitted with IoT transportation solutions, not just for telematics but to increase fuel economy by a minimum of 5 percent, with incentives for higher efficiency.

Approach – Consistent with existing national goals to improve the fuel efficiency of American trucks – thereby bolstering energy security, cutting carbon pollution, saving money, and spurring manufacturing innovation[29] – this proposed PPP would leverage private sector and academia IoT expertise in "Intelligent Transportation" solutions. The PPP would accelerate efforts by Congress, DOT, DOC, DOE, EPA, and U.S. commercial fleet managers to increase engine efficiency and fuel economy of large fleets traveling our nation's roads and highways. It would realize direct economic savings including increased fuel efficiency, reduction in carbon dioxide emissions, labor savings, improved driver safety, accident savings, productivity and distribution proficiency, and logistics tracking effectiveness. The PPP also would provide insights into improvements and new business models for the U.S. transportation sector at large, leading to more satisfied employees and customers. Notably, this PPP would be an early step toward the ultimate goal of an autonomous trucking industry; the estimated savings to the U.S. freight transportation industry from autonomous vehicles is $168 billion per year, with savings from labor ($70 billion), fuel efficiency ($35 billion), productivity ($27 billion), and accident savings ($36 billion).[30] Funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One possibility could be for public and private partners to share in the transportation fuel savings. For example, if the PPP were to reduce a department', or commercial end user operator's fleet, fuel expenses by 7 percent, the department (operator) could allot 2 percent of that savings to the (other) private partners over a specified period of time until the (other) private partners recoup their upfront investment plus some incremental percent of return. The department operator would retain the remaining percentage of the savings, after which time, the department and U.S. taxpayers (operator) would retain 100 percent of the fuel savings benefit in perpetuity.

---

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

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

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

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

Approach – Consistent with the goals of NIST's Smart America and Global Cities Team Challenges[33] – to use IoT solutions to improve services, promote economic growth, and enhance quality of life – this proposed PPP would leverage private sector IoT expertise in deploying "Smart Community" solutions. These IoT solutions would accelerate local government and municipality efforts to improve urban management and planning in a variety of ways. For example, the PPP could provide a model to improve operational efficiencies and safety across existing and new city infrastructure by utilizing air quality and traffic flow data to enable sustainable traffic management and planning, and create an innovative tool for urban growth management and planning. The funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One opportunity may include public and private partners to share in new revenue streams by leveraging the IoT sensor network infrastructure to deliver new services to city residents. For example, if the PPP were to deliver new services to city residents (i) via the city sensor network or (ii) by sharing the real-time data generated by the city sensor network, the city could share the new revenue stream with the private partners. The city (and its taxpayers) would enjoy the benefits of improved traffic flow, air quality, and safety, and avoiding the hefty cost to rebuild city infrastructure.

---

[31] *World Urbanization Prospects The 2011 Revision*, United Nations Department of Economic and Social Affairs (March 2012), http://esa.un.org/unpd/wpp/ppt/CSIS/WUP_2011_CSIS_4.pdf.

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

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

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

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

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

[34] Frost & Sullivan.

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

remaining 10 percent of the savings. After which time, the U.S. government would retain 100 percent of the energy and utility savings benefit.

CONCLUSION

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

Mr. BURGESS. Thank you. The Chair recognizes Mr. Morehead for 5 minutes for the purpose of an opening statement, please.

STATEMENT OF R. BRAD MOREHEAD

Mr. MOREHEAD. Thank you, Chairman Burgess, Ranking Member Schakowsky, and members of the committee. We use the IoT every day when we check traffic or look at the weather forecast. We also see it in the wide variety of smart devices that are popping up everywhere, like smart refrigerators, smart coffee makers, or smart watches. But rather than talking about smart coffeemakers and refrigerators, I would prefer to illustrate the potential benefits of a robust Internet of Things by sharing a brief story about how the security alarm industry works.

Imagine an emergency at your home or at your school or at your work, a burglary or violent crime in progress with multiple potential victims on the scene where the intruder or the victim has triggered an alarm. Speed and information are critically important to the first responders. However, when that security alarm goes off at that home, business, or public location, that signal is delayed for over a minute to reduce false alarms. Furthermore, the process of notifying the alarm monitoring center is surprisingly manual, as the alarm is transmitted after the delay to a person in the alarm center who must then be connected to another person at a 911 public safety answering point, or PSAP, for emergency dispatch.

After an average 1- to 3-minute phone conversation between that security station and the PSAP safety agency, emergency responders are contacted and dispatched to the site of the alarm—again, where time is of the essence. But the first responders are given nothing more than basic information about the type of alarm and location of the incident. This average dispatch total can take 5 to 10 minutes, and that is valuable time and information that is lost in a true emergency. By some estimates from the DOJ, each year more than 1 million police hours are wasted due to these human errors and communication issues in this transmission process.

Adding to that frustration is the fact that there may be additional security cameras, motion sensors, door sensors, or other sensors at the site of the emergency capturing valuable information. Unfortunately, in most cases, those additional sensors and cameras have no way of communicating to the monitoring station, 911 PSAP, or the first responders.

In other words, there is potential lifesaving data available that no one sees. This can cause first responders to arrive at the wrong place at the wrong time and without important information to save lives.

With the IoT, these processes could be seamlessly automated and integrated to prevent and mitigate crimes in a more efficient way. In the future, the transmission of emergency alarms and sensor data could occur instantly from machine to machine, or M–2-M, instead of manually. Automated applications could be used to gather and interpret the alarm information from various IoT devices to determine the probability of a false alarm or help first responders use their time more efficiently and arrive at the right place. Smart sensors and cameras could be used to automatically transmit images and data from the scene of the crime directly to the officers.

Using IoT, two companies and centers were able to cut alarm transmission times down to 5 seconds and reduce the volume of calls going between these centers by 10 percent. Now imagine if that was implemented nationwide, how much more

productive our police, fire, and EMT responders could be with fewer false alarms and better, faster information from IoT connected systems and devices. Internet of Things can help deliver first responders to the scene faster, more efficiently and with more information on the current emergency, if we invest now in the IoT infrastructure that we need so that we go beyond smart coffeemakers and refrigerators.

Unfortunately, there are still a few technological barriers that are preventing us from implementing an ideal system. The IoT consists of a few key components: a power source, a communication protocol and data processing.

Let us begin with power, since this is a subcommittee of the Energy and Commerce Committee. These connected sensors in the Internet of Things must have a power source, and while wired is preferred in some cases, it is typically too expensive to implement. Therefore battery power offers the widest array of uses, but the currently short battery life must be improved to lower the cost of ongoing maintenance and fully tap the potential of IoT.

As an example of this, recently a tech startup called Quirky developed a smart egg holder that would tell you when you were out of eggs in your refrigerator. This sounds like an interesting and useful, but due to current battery technology, it unfortunately it needed its batteries replaced more often than it ran out of eggs to replace. So when lives are on the line instead of omelets, we need to make sure that these smart devices don't lose power. This will require investment in more powerful batteries with longer lifespans.

Secondly, we need to insure the availability of open wireless spectrum for IoT and specifically IoT for public safety agencies. A Government program called FirstNet is developing new wireless applications to aid first responders instead of existing radio-dispatch technology first used in the 1960s. We need more funding for projects that involve improving our Nation's infrastructure for wireless integration and emergency dispatch.

As an example of our outdated emergency infrastructure, currently only about 200 out of 5,900 911 PSAP centers can handle text messages. Text messaging has been around for 20 years, but approximately 3 percent of 911 centers can receive texts. And when you consider that 96 percent of young people text regularly but only 67 percent make phone calls regularly, you can see how much emergency information we may be missing.

Also in our way looms the threat of multiple connection standards for smart devices. Computers generally connect to the Internet using one of two methods, Ethernet or Wi-Fi. However, smart devices connect using a plethora of standards including Wi-Fi, Bluetooth, Ethernet, z-wave, ZigBee, and Thread, in addition to numerous proprietary protocols. So currently a Nest thermostat may know the temperature in a home is increasing due to a fire but it is unable to contact the 911 PSAP through the security system if

the homeowner is asleep or unavailable. IoT standards and interconnectivity would solve this.

As an example, my company, LiveWatch Security, developed As Soon As Possible Emergency Response, or ASAPer, which is an application that is a step in that direction. It combines the speed of machine-to-machine communication with the latest group chat communication technology to allow people to process this information from the IoT and sensors. This IoT-enabled system has reduced false alarms by up to 30 percent while also improving response times, in some cases, by 80 percent. We must continue to invest in the entrepreneurs that will develop these new applications and improve the way we process data from the IoT to turn it into useful information for our first responders.

These are all issues that can be solved with additional smart investment in the smart things that make up the Internet of Things. We can obtain the most progress towards eliminating these obstacles by focusing on engineering advances in battery efficacy and low-power radio range, finding better ways to utilize wireless spectrum for first responders and creating standards for communication between the IoT ecosystems, and finally, investing in better first-responder infrastructure that can handle new types of communication to, and from, IoT devices and users.

We are at the beginning of the next big shift in technology where machines and devices can talk to each other and instantly share data in ways that change lives.

We can use IoT to enhance the security of Americans and the safety of our first responders. To me, these are compelling reasons to invest in this new frontier of technology. Thank you.

[The prepared statement of Mr. Morehead follows:]

R. Brad Morehead

LiveWatch Security, LLC

"The Internet of Things: Exploring the Next Technology Frontier." Tuesday, March 24, 2015, at 11AM

Subcommittee on Commerce, Manufacturing, and Trade

The Internet of Things, or I-O-T, is the technical term we use to describe direct communication between electronic devices. This phenomenon has blossomed into existence over the past several decades. We use the IoT every day when we check traffic or look at the weather forecast. We also see it in the wide variety of smart devices that are popping up everywhere, like "smart" refrigerators, "smart" coffee makers, or "smart" watches that help inform our eating, sleeping, and exercise habits.

But rather than talking about smart coffeemakers and refrigerators, I would prefer to illustrate the potential benefits of a robust internet of things by sharing a brief anecdote about how the security alarm industry works now, and then show you how it could work better with a more developed IoT.

Imagine an emergency at a home or school or work. A burglary or violent crime-in-progress with multiple potential victims on the scene where the intruder or the victim has triggered an alarm. Speed and information are critically important to the first responders. However, when a security alarm goes off at a home, business, or public location, that signal is delayed for over a minute typically to reduce false alarms. Furthermore, the process of notifying the alarm monitoring center is surprisingly manual, as the alarm is transmitted (after the delay) to a person in the alarm center who must then be connected to another person at a 9-1-1 public safety answering point, or PSAP, for emergency dispatch.

Then, after an average 1-3 minute phone conversation between the security station and the safety agency (assuming there was no connection delay because of overwhelmed PSAPs and budget cuts), emergency responders are contacted and dispatched to the site of the alarm with nothing more than basic information about the type of alarm and location of this incident. Furthermore, there are numerous opportunities for additional human error through miscommunication. The average dispatch can take 5-10 minutes. That is valuable time and information that is lost in a true emergency. By some estimates from the Department of Justice, each year more than one million police hours and over $1.5 billion dollars are wasted due to these human error and communication issues.

Adding to the frustration is the fact that there may be additional security cameras or motion sensors and door sensors at the site of the emergency capturing valuable information. Unfortunately, in most cases, those additional sensors and cameras have no way of communicating to the monitoring station, the 9-1-1 PSAP, or the first responders. In other words, there's potential lifesaving data available that no one sees until it's too late. This can cause the first responder to arrive to the wrong place at the wrong time without important information to save lives.

With the Internet of Things, these processes could be seamlessly automated to prevent and mitigate crimes in a more efficient way. In the future, the transmission of emergency alarms and sensor data could occur instantly from machine to machine (or M-2-M), instead of manually. Automated applications could be used to gather and interpret alarm information from various IoT devices to determine the probability of false alarms and help first responders use their time more efficiently. Smart sensors and cameras could be used to automatically transmit images and data from the scene of the crime directly to officers to help them perform their duties in a safer and more efficient manner.

There have already been several successful small-scale implementations of this concept. Several alarm companies and 9-1-1 centers in Richmond and Houston have implemented a system called ASAP,

or the Automated Secure Alarm Protocol. Using ASAP, participating companies and centers were able to cut alarm transmission times down to five seconds, and reduce the volume of calls going between centers by 10 percent. Now imagine how much more productive our police, fire and EMT responders can be with fewer false alarms and better, faster information from IoT connected systems and devices. IoT can help deliver first responders to the scene faster, more efficiently and with more information on the current emergency, if we invest now in the IoT infrastructure that we need so that we go beyond smart coffeemakers and refrigerators.

Unfortunately, there are still a few technological barriers that are currently preventing us from implementing an ideal system.

The IoT consists of several key components. The:

1. Power source
2. Communication method (typically hardwired or radio)
3. Communication protocol and ecosystem
4. Data processing
5. Data security

Let's begin with power, since this is the Energy and Commerce Committee. These connected sensors in the Internet of Things must have a power source. While wired is preferred in some cases, it is typically too expensive to implement for strapped budgets for most new types of devices and sensors. Therefore battery power offers the widest array of uses, but the currently short battery life must be improved to lower the cost of ongoing maintenance and fully tap the potential of IoT.

As an example, recently, a tech startup called Quirky developed an "smart" egg holder that would tell you when you were out of eggs in your refrigerator. This sounds like an interesting and useful

smart device, but due to current battery technology, it unfortunately it needed its batteries replaced more often than it ran out of eggs to replace. When lives are on the line, instead of omelets, we need to make sure that these smart devices don't lose power. This will require investment in better, smaller, and more powerful batteries with longer lifespans.

Research suggests that Moore's law—the theory that explains why the number of transistors in circuits has increased exponentially—does not apply to batteries. To physically power our Internet of Things, we will need additional breakthroughs in the chemistry of batteries to make long-term device life possible.

Secondly, we need to ensure the availability of open wireless spectrum for IoT and specifically IoT for public safety agencies. FirstNet is a government program that is developing new wireless applications to aid first responders, instead of existing radio-dispatch technology first used in the 1960s. We need more funding for projects that involve improving our nation's infrastructure for wireless integration and emergency dispatch. Automated security will be impossible without sufficient wireless spectrum for devices and continued investment in faster wireless networks.

As an example of our outdated emergency infrastructure, currently, only about 200 out of 5,900 9-1-1 PSAP centers can handle text messages. Text messaging has been around for more than 20 years, but approximately 3% of 9-1-1 centers can receive texts. When you consider that 96% of young people text regularly, but only 67% make phone calls regularly, you can see how much emergency information we may be missing from people and devices already on our networks. Only when all emergency call centers can handle texts, tweets, IoT data and other new types of communication will we be fully utilizing IoT to save lives.

Also in our way looms the threat of multiple connection standards for smart devices. Computers generally connect to the Internet using one of two methods: Ethernet or Wi-Fi. However, smart devices

connect using a plethora of standards including Wi-Fi, Bluetooth, Ethernet, z-wave, ZigBee, and Thread, in addition to numerous proprietary protocols.

Currently a Nest thermostat may know the temperature in a home is increasing due to a fire, but it is unable to contact the 911 PSAP through the security system if the homeowner is asleep or unavailable. IoT Standards and interconnectivity would solve this. We must invest resources to develop a reliable system of cross-compatibility so devices from different manufacturers and ecosystems can talk to one another without errors.

Additionally, we must synthesize all of the data made accessible by IoT. Once we understand all the information we're collecting, we must invest in infrastructure for first responders that handle new types of communication.

As an example, my company, LiveWatch Security developed As Soon As Possible Emergency Response, or ASAPer, which is an application that is a step in that direction. It combines the speed of machine-to-machine communication with the latest group chat communication technology to allow people to process information from multiple sensors and other users. This IoT-enabled system has reduced false alarms by up to 30% while also improving response times, in some cases, by 80%. We must continue to invest in entrepreneurs that will develop these new applications that will improve the way we process data from the IoT and turn it into useful information for our first responders.

Lastly, the Internet of Things presents us with issues of privacy and security. We need to continue to develop a better understanding of exactly where our data goes, and make sure that smart devices remain hard to hack. Unfortunately, un-hackable will be impossible to achieve. This is a moving target. While systems like ours use 256-bit encryption, which is typically found in online bank security, we need to continue to push the envelope of information security.

These are all issues that can be solved with additional "smart" investment in the Internet of Things.

We can obtain the most progress towards eliminating these obstacles and automating and improving security of Americans by investing time and money in three major areas:

1. First, we should focus on engineering advances in Battery efficacy and low-power Radio range.
2. Second, we must find ways to better utilize wireless spectrum for first responders and create standards for communication between IoT ecosystems, so that IoT devices can communicate across platforms.
3. And finally, we should invest in better first responder infrastructure that can handle new types of communication to, and from, IoT devices and users.

We are at the beginning of the next big shift in technology, where machines and devices can "talk" to each other and instantly share data in ways that change lives. Clearly, the internet of things is a growing trend, but if we invest in the right places now, we can make it more than "smart" coffee makers and "smart" refrigerators that re-order eggs...We can use IoT to enhance the security of Americans and the safety of our first responders. To me, these are compelling reasons to invest in this new frontier of technology.

Mr. BURGESS. The Chair thanks the gentleman for his remarks. We will now move into the question-and-answer portion of the hearing. I will begin by recognizing myself 5 minutes for the purpose of questions.

I want to ask a couple of general questions just on the general theme of the governance of the Internet of Things, and I would like to ask each panelist to respond briefly in turn. And Mr. Castro, we will start with you. It is an open-ended question, and I will acknowledge that. And many of you have already addressed this partially in your testimony, but what do you see is the appropriate role of Congress right now relative to the Internet of Things, bearing in mind we are marking up data breach notification tomorrow and probably before the spring is over, we will have a mark-up on patent demand letters. But irrespective of that, I welcome your thoughts.

Mr. CASTRO. Sure. Absolutely. I think the number one issue right now, just because it is growing in attention, is data breach. We saw, you know, so many data breaches over the past year, high profile. This is something that Americans are worried about, and it is something where I think Congress could take an immediate and important step. But long-term, as I think you have heard from at least two panelists up here, we are really thinking about national strategy for the Internet of Things. This is something that Congress can get behind, that the Federal Government can get behind, and you really create a new vision for the future of commerce, the future of houses that interact with technology and how we can have an impact in so many different areas.

Mr. BURGESS. Thank you. Mr. Van Harlingen?

Mr. VAN HARLINGEN. As has been mentioned, I think data breach management and rules around that and consistency around that nationwide would be very helpful to both the industry and consumers.

As I mentioned in my opening statement, I think spectrum management, both for the unlicensed spectrum and as Mr. Morehead mentioned, for emergency first responders in a more licensed fashion would be very good investments of time for the committee and for the Federal Government.

I would advocate a light-touch approach. This is a very new and emerging space where we have a lot to learn about what is possible and what value we can create.

Mr. BURGESS. Thank you. Ms. Schooler, your thoughts on the appropriate role of Congress.

Ms. SCHOOLER. Yes, absolutely. I think it is starting today, an open dialogue between industry and Government, consumer groups to get the needs and the interests of the consumers on the table as we chart policy moving forward as well as people from industry environments.

I think we need, as I mentioned in my statement, to encourage a focus on security and interoperability. I think the opportunity to leverage public and private partnerships will be key, and I think even if you look at the infrastructure and the capabilities within transportation's $351 billion opportunity in that segment over I think it is 650,000 fleets and tires and trucks within the Postal

Service in the U.S. Government, excellent opportunity to try out some of this technology with public and private partnerships.

We talked about a national IoT strategy. I think that is critical moving forward. And again, open standards, open architecture, open source, interoperability, allow for the continuation of innovation.

Mr. BURGESS. Very good. Mr. Morehead?

Mr. MOREHEAD. I agree on the points about open standards and interconnectivity. For most of the sensors, I think that investment in battery power and improved performance for batteries will be incredibly important as we develop new sensors. But finally I do think investing in the infrastructure of our Nation's PSAPs and emergency first responders is incredibly important.

There was an article in the Journal recently about a company called Smart Things, and the journal reviewed the technology of smart things. And at the end of the article, what they found is that the most compelling use of the technology was turning on the coffeemaker in the morning, which frankly wasn't compelling, was the summary of the article.

When you talk about investing the types of time and money that you would be investing, I think you could look to the Nation's infrastructure and truly save lives which has an immeasurable benefit of both the first responders and potential victims by investing in the public infrastructure and the PSAPs to get the right information distributed to emergency first responders faster. And that has a faster payback than potentially some other projects.

Mr. BURGESS. Great. I thank all the panelists for their thoughts on that. Just being mindful that I want to stay within the constraints of 5 minutes because I am going to insist that everyone else do that on the dais, Mr. Morehead, you referenced the fact that, well, the Journal article about the coffeemaker, well, that is really not that important. But what some days seems trivial to one person may down the road actually be very significant, and I guess the overarching theme here is a regulatory touch. You heard Ms. Blackburn mention it, the light regulatory touch. Could each of you speak in one word or two words to the regulatory touch that you would like to see on the side of the agencies?

Mr. CASTRO. I think we want to embrace innovation and let, you know, let these companies—you saw the showcases out there today. Imagine what it will look like 10 years from now. You want to see that innovation flourish.

Mr. BURGESS. Mr. Van Harlingen?

Mr. VAN HARLINGEN. Agreed, a light touch that fosters innovation and creativity and exploration in this space.

Mr. BURGESS. Great. Ms. Schooler?

Ms. SCHOOLER. Light touch to spur innovation.

Mr. MOREHEAD. The coffee from the smart coffeemaker is good dark, but regulatory touch I think would be better light.

Mr. BURGESS. Very good. You have all allowed me to fit within the constrains. I will now recognize the ranking member of the subcommittee, Ms. Schakowsky, 5 minutes for questions, please.

Ms. SCHAKOWSKY. Thank you very much for all your testimony. I wanted to give a little bit of opportunity to Mr. Morehead to tell us a little bit more about LiveWatch. Mr. Morehead, home security

systems have been in existence long before 2002 when LiveWatch was created. So as we increase our technologies, et cetera, what motivated you and your business partners to enter this space? And how do you think that what you are doing improves consumer experience?

Mr. MOREHEAD. Thank you, Ranking Member Schakowsky. When we entered the space, we saw an opportunity with a business model in the home security industry that was relatively unchanged for decades, predominantly ADT where customers were paying significant amounts of money and not getting the value that they needed. And we saw an opportunity to bring a technology focus, a disruptive technology focus to a relatively nascent industry.

And the nice thing about home security is it is formed upon a foundation of security, right? We talk about security and privacy here, home security is by definition focused on security. So we use that as a foundation to disrupt the business by going direct to consumers and lower their prices by about 30 to 50 percent, by eliminating the middlemen of sales and delivery and having customers self-install their wireless systems.

So all of our infrastructure is wireless. It is formed on a basis of security, and then from that point, we added layers of additional technology, received multiple patents for that to determine how customers could use the information that was flowing from those systems. Specifically the opportunity we saw there is a home security system was really Internet of Things before there was an Internet of Things. We have sensors in homes and businesses throughout the country, throughout the world. Those produce data. That data is then transmitted to a central station where it looks for alarms.

But the fact of the matter is, we can do additional things with that information, and that is where we have taken the next step with our product, ASAPer, to allow customers to process the information, the data coming from those devices, in a more effective way.

Ms. SCHAKOWSKY. Are you concerned at all? Because a number of people will be contacted that there is some sort of breach of security in the home, right? How do you protect against unwanted invasions of that information that is circulated to a certain population of people, family members for example?

Mr. MOREHEAD. The main thing that we try to do is we limit the information to the people that the homeowner or the business owner specifically selects to receive that information. So we keep it in a tight-knit group that is selected by that person to receive the information.

The challenge is that there is power in numbers, and so we want to get the information to as many people as we can in an emergency because we are looking for the one person that knows what is actually happening and that can help resolve it.

So we need to get it ideally just to the one person that knows, but to do that we have to get the information to multiple people. So we allow the homeowner to put those people on the list, and then we bring them into a group chat to help facilitate the resolution of that alarm signal. And we found that thus far, implementing the right technology and security on the back end, it has

been a productive way to do it. And instead of having two to three fixed members on an alarm distribution list, we have tested it with up to in a school setting, up to 170 people simultaneously on one group chat to see what would happen if there was an emergency at a school and there is no other system that can facilitate that communication.

Ms. SCHAKOWSKY. Have you seen any particular problems that result from having a universe as large as 170?

Mr. MOREHEAD. At this point we have not. Overall it has been pretty positive. I think that there is some learning curve for consumers and users as they get up to speed and say, oh, I am chatting and trying to have a conversation with 170 other people. But in the end, what you tend to find is that only one or two people actually step up in that conversation because they are the ones with the relevant information. So of that 170, we are really just looking for the one or two people that can help resolve the situation.

Ms. SCHAKOWSKY. Thank you. Mr. Castro, you said something interesting at the end of your written testimony about education and building cybersecurity education. I am going to read it. Congress should encourage universities to integrate cybersecurity training into technical degrees so that the next generation of coders, engineers, build strong security into products at the outset.

Do we not do that now as we are training people?

Mr. CASTRO. Yes, it is a great question. I mean, the field of information security has evolved over time. So originally many of the problems that we saw in computer systems were because the coders weren't thinking about the security issues, and you had people fixing that afterwards. As we are moving into the Internet of Things, we want people to be thinking about the big issues that exist today and how they can fix them at the outset rather than doing it later on.

Ms. SCHAKOWSKY. Thank you. I think universities and educational systems have a role, too, to play, and I thank you for pointing that out.

Mr. BURGESS. The Chair thanks the gentlelady. The gentlelady yields back. The Chair recognizes the gentlelady from Tennessee 5 minutes for questions, please.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I have got three questions, and I want to hear from each of you on them. So I appreciate brevity. And if you want to expand to anything further, please do it in writing within the next week or so.

First of all, let us talk about privacy because that is always top of mind. What is this going to do to me if I use this thing? And when you talk about big data and the explosion of data that is out there, first of all, let us look at it like this. What do you think the trend is for growth of data on the Internet? Are we going to continue to see this explosion? And secondly, what should Congress' role be in protecting that data? And let us just start. Very quickly, Mr. Castro, I am going to start with you. Let us work down so we can move to question two.

Mr. CASTRO. Sure. So in terms of the trend, it is increasing.

Mrs. BLACKBURN. OK.

Mr. CASTRO. Do you want me to address the second part?

Mrs. BLACKBURN. Sure.

Mr. CASTRO. Yes, and so the second part about this is, you know, Congress should be really looking at how consumers are hurt or not hurt by the use of the data.

Mrs. BLACKBURN. So define harm?

Mr. CASTRO. Define harm and not regulate the collection. We want data to be collected and shared.

Mrs. BLACKBURN. OK. Yes, sir?

Mr. VAN HARLINGEN. So I agree the trend is huge. The amount of data that we have is directly proportional to the value we can create, and I think the way to deal with it as in the FTC's recommendations is pay very attention to providing notice and choice to the consumers.

Mrs. BLACKBURN. OK.

Ms. SCHOOLER. I saw data recently where 90 percent of the data today was created in the last 2 years.

Mrs. BLACKBURN. That is right.

Ms. SCHOOLER. I think that is indicative of the pace of innovation and the creation of data, and I think whatever we say in terms of data growth, we will be grossly wrong.

Mrs. BLACKBURN. OK.

Ms. SCHOOLER. We will under-call it. What do we need to do from a policy perspective? Again, I think we need to bring multiple parties to the table. I think we need to bring the Government, industry, consumer groups to understand what some of the use cases are and create policy around use case versus a broad, blanket policy to try to manage every scenario. And two, I think we need to build security in from the onset as I mentioned in my testimony from the device to the network to the cloud.

Mrs. BLACKBURN. OK.

Ms. SCHOOLER. And when we often say we want to create redundancy in that transmission, it means you don't always secure it at one point. You secure it throughout the transmission and the manipulation of the data. So those are my two comments.

Mrs. BLACKBURN. OK. Mr. Morehead?

Mr. MOREHEAD. I think there will obviously be substantial growth in the data. I think you will see multiple models emerge because this is not a winner-take-all market, and for lack of better terms, I will call it an Apple model and a Google model, an Apple model where the data is more private and a Google model where the data is used publically. The customer, the consumer, may get less expensive hardware, less expensive or free services, but the data will be used to provide other options. So I think multiple models will emerge for the data.

Mrs. BLACKBURN. OK. Second question, I want to look at education for consumers and some of the consent agreements that companies have when you are talking about the Internet of Things and the utilization of this data.

Do you think that companies in these agreements for a particular service, did they adequately inform consumers and the consumers understand how this data is going to be utilized and what can be done to improve those privacy policies if you will so that consumers are offering true informed consent when they agree to utilization of some of the services that are there? And you know, one we dis-

cussed yesterday was insurance companies wanting you to utilize some type of component, and it gives you the number of hard breaks and fast stops and speeds driven, things of that nature. And we have got only 45 seconds left. So let me do this. I will ask for that response. I want to move onto the third question just to lay it out since we are going to run out of time, the economic impact. And Accenture had a great report on the economic impact of the Internet of Things. And I would like to get your take on that statement. We have it for you. And I want to know if you agree with it, and then I would like for you to speak specifically when you respond in writing to the challenges that exist in the United States to realizing this type of economic growth. What are the barriers to entry? What are the hurdles that are going to be there? What are we doing wrong from a regulatory side that are disenfranchising innovators? And I yield back my time.

Mr. BURGESS. The Chair thanks the gentlelady. The gentlelady yields back, and those responses will be anticipated as written responses. Mr. Cárdenas of California, you are recognized for 5 minutes for questions, please.

Mr. CÁRDENAS. Thank you, Mr. Chairman. The first question that I have is to Ms. Schooler. The City of Los Angeles is still a pretty big economic juggernaut for manufacturing in this country. When it comes to the Internet of Things and that type of innovation, what do we anticipate for manufacturing and production of products, et cetera, and the streamlining? And what is in the back of my mind is jobs, the opportunity to have successful businesses and therefore, a good, robust economy. So what can we expect going forward? Is this something that is going to be utilized more and more when it comes to manufacturing or something that we plateaued on where are we at, do you think?

Ms. SCHOOLER. Excellent question. We very much believe manufacturing will be smart manufacturing, in particular will be an excellent opportunity for the Internet of Things. At Intel we actually deployed a smart manufacturing pilot within one of our manufacturing facilities, and as you know, we make millions of things every year. So I think we are a pretty good test case. In that implementation we found that we collected data that allowed us to do predictive maintenance, and with predictive maintenance you increase up-time, you improve yields. And in that pilot, we realized a $9 million return on that single opportunity for that pilot in that single factory.

Accenture published a report recently that they said 87 percent of the CEOs in the country see a long-term job growth opportunity, and I think to put that into practical terms, if you think about lowering the cost of goods sold, that is a great way to attract jobs back to the United States. So number one, let us optimize our manufacturing facilities from a product-cost perspective, use the technology to use predictive maintenance as a capability to increase up-times, again bringing down the total cost of goods, and to improve the utilization and the effective utilization rates of the equipment, again, improving output.

So I think all of these things will result in job creation and bringing jobs back on shore.

Mr. CÁRDENAS. Thank you. And I like your example that you gave, and it reminds me that efficiency is a win, win, win, win, win, not only for the manufacturer but also for the consumer and for the community.

Which leads me to my next question. Brian, if you could please. Hopefully it is a great answer for Los Angeles. California is going through a drought. We have yet to see the worst of it. So what do you see in the consumer space or even in the industrial space when it comes to efficiency, opportunities for energy, water, things of that nature with this technology?

Mr. MOREHEAD. So one of the technologies that we are working on in particular is a technology that we call Echo that allows the consumer's home or a business to monitor their energy use, their water use, in great detail through a single point using the existing infrastructure in the home. It is a very cost-competitive technology or cost-effective technology. We think we will educate people about how water and power are being used in their house and lead to improved behavior around that consumption.

Mr. CÁRDENAS. So you see a lot of advancements there and a lot more usage?

Mr. MOREHEAD. Absolutely. It is a place that we are putting a lot of our research efforts.

Mr. CÁRDENAS. Yes. Hopefully it is a lot more efficient than pounding on the door when I tell my kids they have to take shorter showers.

Mr. MOREHEAD. Agreed. It is also very good at detecting leaks which are a huge source of water waste in the city.

Mr. CÁRDENAS. Absolutely. Well, thank you. And the last question to whoever would like to help enlighten us, what can we learn from the rest of the world? We are very spoiled in this country. We are still the economic juggernaut of the planet. We are looked to by many places around the planet for leadership. But once in a while we see ourselves looking and jog our head back and go wow. They got it right over there. They did something really cool or they did something that is advanced or something that we probably should have thought of but we didn't. What examples can you enlighten us about what is going on maybe around the world that we could learn from and then take their leadership?

Mr. CASTRO. Well, following up on your question about the water, if you look at India, I mean, so many countries have these big economic and social problems. They don't have any alternative but to go to the best technology and really look for an innovative solution. So in India, you know, they have decaying water infrastructure. Using smart technology, they are able to actually you know, cut significant waste at less cost than it would have been to replace the infrastructure. So really the United States should be looking at the same thing. We have decaying infrastructure. We just have a lot more money. So how can we do it really efficiently?

Mr. CÁRDENAS. Thank you. Real quick?

Ms. SCHOOLER. I would be happy to go next. I think I noted in my testimony that we see national IoT plans in other countries, Germany, Brazil, China. I definitely think as we had a broadband plan, we should have an IoT strategy and plan for the country. I

think that would help us accelerate our learnings and accelerate our deployments which is critical.

And just interestingly enough, a little tidbit from the demo room, I was talking to the SteadyServ beer keg optimizer which I think is a fascinating IoT use case. And in that deployment, one of the things that he was discussing and we were talking about was the adoption between the United States and Europe. Well, in Europe, they are looking at the opportunity, looking at the return on the investment in adopting the technology much more aggressively. And in the United States, there is still some hesitancy because it is not how we are used to doing it. And I think collectively between Government and industry, large business and small business, we have to start embracing technology in a much more aggressive fashion than we have in the past.

Mr. CÁRDENAS. Thank you, Mr. Chairman. I yield.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back. The Chair recognizes the gentleman from New Jersey, vice chairman of the committee, Mr. Lance, for 5 minutes for your questions, please.

Mr. LANCE. Thank you, Mr. Chairman. And good morning to the panel. I was very pleased to see Alcatel-Lucent, Bell Labs, and Qualcomm representing the district I serve at the showcase today, and I thought it was a wonderful showcase. And I commend the chairman for his hard work in making sure that it occurred.

Bell Labs demonstrated truly remarkable 5G wireless technology that will enable a variety of Internet of Things applications such as high-quality videos, smart meters, and connected cars. One thing is clear. Spectrum is one of the engines that will drive the Internet of Things revolution.

To the panel in its entirety, what would you suggest that Congress do to provide the spectrum resources needed to support next generation networks in the Internet of Things? Mr. Castro?

Mr. CASTRO. Thank you. As we can see in these demos and just looking around the market, there are going to be a growing number of devices, a huge number of devices everywhere. So I think just in general, we are looking for commercial spectrum to be available, both licensed and unlicensed, and that is something that I think we are just going to have—Congress will have to continue to monitor and promote.

Mr. LANCE. Thank you.

Mr. VAN HARLINGEN. I agree. I think that there are requirements for both licensed and unlicensed spectrum for a variety of different applications. I would encourage Congress to collaborate in detail with the industry on what those needs are and provide that spectrum as available.

Mr. LANCE. Thank you.

Ms. SCHOOLER. I agree with the previous comments. I think we need to leverage both the licensed and unlicensed spectrum, utilize the technologies that exist today to get the economies of scale that will enable us to drive and growth and accelerate deployments. That in lieu of looking at a specific use case and a specific spectrum band for IoT, I think we should leverage what we have today.

Mr. LANCE. Thank you. Mr. Morehead?

Mr. MOREHEAD. As we look forward, it is important to understand where we are going with the spectrum. I think that there are some lessons we can learn from the past. One of the challenges for those of us that have been doing IoT for the last decade or so is backward compatibility and sunset of existing wireless connectivity, 2G, 2 ½G and the sunset that is happening with the wireless providers there is creating a big issue for us where we already have Internet of Things systems in the field and we are having to replace those. It is a large expense.

So as you think about moving forward what you want to do with the spectrum, I think it is important to consider backward compatibility and when and how those wireless systems sunset.

Mr. LANCE. OK. Thank you very much to the entire panel. Mr. Castro, privacy oftentimes means different things to different people. Do you think the market is capable of addressing concerns related to privacy in the Internet of Things market over time?

Mr. CASTRO. Yes. I think, you know, consistently what we see is when there is new technologies—and this goes back, you know, decades, centuries even—when new technologies come out, there are fears and doubt and uncertainty about the technology. But what we see is over time many of those issues are resolved just by the market, that you have this, you know, convergence between what business wants to do, what consumers want to have, and what Government regulates. And a lot of these issues are worked out which is why in general I think we want this light touch approach. Especially it is important with the Internet of Things because so much of the innovation is around the data, and if you can't have companies sharing or reusing this data for lots of innovative purposes, this kind of long tail of innovation, you are not going to get this magnitude of benefits that we want to see.

Mr. LANCE. Thank you. Belkin has a close connection to consumers and access to very personal data. How has Belkin approached the privacy and security of consumer data in its product offerings?

Mr. VAN HARLINGEN. So Belkin takes privacy very seriously. Some of our products, you know, are very close to consumers, as you mentioned, including cameras and things like that. We work very closely on security, stay standard and ahead of the curve with industry standards. We have an application security team that is very active in the industry working with the Black Hat Community and other security researchers, and they are very thorough at reviewing our products, both before launch as well as after launch.

Mr. LANCE. Thank you. Mr. Chairman, I yield back 28 seconds.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman does yield back. The Chair recognizes the gentleman from Houston, Mr. Olson, 5 minutes for your questions, please.

Mr. OLSON. I thank the Chair, and welcome to our witnesses. I want to follow up on my colleague's comments from California about manufacturing. As you all know, in the last decade, loss of good manufacturing jobs have left America and gone overseas. Many reasons, excessive taxes, excess regulations, but this appears to be the opportunity to bring things back to America with the IoT. So my question to you, Ms. Schooler, as one who has manufacturing as part of your business, you mentioned Germany, Brazil,

and China. What are they doing that we are not doing? What can we learn from them and how can we make sure we have U.S. leadership to quote you in the future on the IoT?

Ms. SCHOOLER. Thank you. So one of the things that I noted was some of the advancements in the manufacturing capabilities in the IoT standards and national policy in other countries. If you look in areas like Germany, you will see some of the most highly automated, highly advanced connected factories in the world. I think there is a lot we can learn by going into some of these other geographies and understanding and levering some of the advancements that they have put into place up until now.

If you look at places like China, they are highly adopting and supporting things like smart cities where they are using the technology, not only for manufacturing capability but also for societal positive impact by looking at the air quality as an example. We can look at use cases such as monitoring the health of an oil pipeline, all of these things, and a lot of it is around predictive maintenance. I think as we journey as industry over into these other geographies, understand the deployment capabilities that are in place. We need to bring that back into the dialogue that we are having on a regular basis, both with our other industry partners as well as Government to continue to progress our policy to support some of the implementations of these technologies moving forward.

Mr. OLSON. I know there are at least two domestic groups that are looking at interoperability here in America and open standards. Is that enough? Should there be more? Who else should be involved in this? Because let us bring those jobs back.

Ms. SCHOOLER. Standards is an excellent point. We have the OIC and the IIC which I believe are the two——

Mr. OLSON. Yes.

Ms. SCHOOLER [continuing]. Consortiums that you are inferring. One is the Industrial Internet Consortium and the other is the Open Internet Consortium. In both of those cases, you are taking very large members of industry, bringing them together to really set whether it be an architectural framework or series of test beds that allow for the understanding of the deployment. It is one thing to set standards. It is another thing to architect and build solutions based on those standards.

So in both of those bodies you have not only the definition of the architecture but the deployment and the testing of the implementation of that architecture.

So I think those are a good start. I think if you look from a connectivity perspective, you have efforts in 3GPP around 5G that are looking at IoT-specific use cases. We need to continue to put wood behind the arrow on the connectivity solutions as well. So I think we have a good start. I think as we continue through the commercial deployment phase, it remains to be seen as if it is enough or if we need to extend those standards' efforts further as we learn more through our initial commercialization efforts.

Mr. OLSON. Thank you. Mr. Castro, any comments, sir, on the issue of manufacturing, bringing it back to America? And Mr. Van Harlingen? Anybody before I get my time run out here?

Mr. CASTRO. I think you are absolutely right. When we look at, you know, the opportunity here, the United States leads in this

technology area, and we want to, you know, regain these manufacturing jobs. The way to do it is by investing and having the most innovative factories. And when we look—you know, the examples that I have in my testimony I submitted for the record, you know, we see U.S. companies leading in this space on the Intel, Harley Davidson, Raytheon, you know, these companies that are able to track to the turn of the screw what is going on in the factory and use that data to operate more efficiently than anyone else. That is our competitive advantage. We have to make sure we are investing in that opportunity. We have to make sure that our schools that are leading the development of this have the funding to do that, and that is one opportunity that Congress might be able to help support further.

Mr. OLSON. Mr. Harlingen?

Mr. VAN HARLINGEN. As a consumer electronics company, most of our focus is on consumer products. A lot of our manufacturing is done off shore, but we are constantly evaluating opportunities to bring manufacturing back on shore. There have been a couple of instances in some of our business areas where we have done so, and we are enthusiastic about doing so. We look forward to IoT technologies brought by other companies into the manufacturing sector to make that more possible and more practical for companies like ourselves.

Mr. OLSON. Well, come back to Texas. Mr. Morehead, your final thoughts, sir?

Mr. MOREHEAD. I am not as involved in the manufacturing side, but most of our vendors unfortunately do use off-shore partners. Where I see the opportunity, though, here is the fact that we are talking about 25 billion devices being implemented in the United States or some portion of that. You can't outsource the installation, activation, servicing, and redeployment of those devices here in the United States. So potentially retraining that workforce to get them intelligent and smart on how to maintain and install the devices could be another way to engage the workforce in the United States as opposed to just being dependent on the manufacturing.

Mr. OLSON. Thank you. Yield back. Out of time.

Mr. BURGESS. The gentleman's time has expired. The gentleman yields back. The Chair recognizes the gentleman Mr. Mullin from Oklahoma for questions, 5 minutes, please.

Mr. MULLIN. Thank you, Mr. Chairman, and first off, I would like to thank the CMT staff for organizing the showcase earlier this morning and of course, all the participants. I was kind of blown away.

One technology that was out there is brought to you by Al Sutherland from my State who shared the amazing technology that has already proven extremely useful to people like myself in the farming and ranching business. Mr. Sutherland has a product called the Mesonet where basically—and I hope I said that right—but basically it has a monitoring station in all 77 counties throughout the State. One of them is just located a couple miles from our place. It gives us real up-to-date information. He was demonstrating the app on the phone. I had that app downloaded real shortly, considering that this time of the year we begin to start burning off fields and then we enter hay season. It is very useful. In fact, I was very

upset that I didn't already have it on my phone. It would have helped a few times laying that hay down. You can predict weather only so well. Well, it gives us some great technology.

So it shows itself very useful out there. But there is been some fear around technology. There is this group of people out there that says, you know, it is going to eliminate jobs. And so for our panel, whoever wants to answer this, how do we combat that fear? You know, people automatically fear things that they don't understand. We see that all the time. But there is an argument being said that, look. If we go so far and we start continuing getting smart machines, our unemployment is going to rise. Go ahead, ma'am.

Ms. SCHOOLER. Yes, I think we need to continue to communicate the positive impacts that we see by doing things like the smart manufacturing use case that we talked about earlier. As I noted Intel implemented a smart capability within our own factory, and it provided a $9 million savings in just one factory. And what was that savings based on? Equipment utilization rates, predictive and preventative maintenance, and for every time you institutionalize one of those learnings, you bring down product cost. You bring down product costs, you get more competitive on a world-wide basis, and you have the opportunity to bring jobs back to the United States.

In those cases, I think we need to get much more aggressive in sharing those stories and sharing those learnings to balance out some of the fear and uncertainty that are put into the press around the other use cases where the news is very negative around job destruction.

Mr. MULLIN. All right.

Ms. SCHOOLER. I noted the data point earlier that in the January Accenture survey, 87 percent of the CEOs believe it is going to create new jobs. Mr. Morehead noted that, even in some cases if it is a consumer device and it is being manufactured off shore, these still need installed. There are still services. There are still new information-type positions that are going to be created. It may not be in all cases the types of jobs that we are used to today, but it will result in job creation moving forward. I am very passionate about that.

Mr. MULLIN. So how do we educate the people? Do we start putting these in trade schools? Do we start in high school? How do we implement it? And that is for anybody on the panel that wants to try answering this.

Mr. CASTRO. I will jump in. I mean so, you know, there is myth that robots or automation kill jobs. I think part of that is an education problem that, you know, better economics lessons will teach people that, you know, if you look at the history—you know, I mean, if we want full employment, yes, we can get rid of John Deere and all the tractors on farms and, you know, problem solved. That is not what we want to do. We want to lower prices for consumers. We want more efficiency. And most of the Internet things examples that we are talking about, they are addressing these issues. They are addressing, you know, productivity on farms. You look at safety issues, you know, automation with grain bins, you know, making workers safer. That is not eliminating jobs. That is actually improving quality of life.

So I think once people start to see how this actually helps them, they are going to realize it is not technology to be feared but that technology improves their life.

Mr. MULLIN. Anybody else?

Mr. VAN HARLINGEN. So agreed. You know, this technology promises, like any new technology, it is going to bring change. Hopefully it will bring manufacturing opportunities back to the United States, and that will create jobs. But it is also going to create different types of jobs. As we mentioned in the service industry and things like that, I think it is going to be important to invest in education to prepare people for those new types of roles.

Mr. MULLIN. Thank you. I appreciate your time and once again appreciate the CMT putting this hearing together. Thank you. I will yield back.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back. The Chair recognizes Mr. Harper from Mississippi 5 minutes for questions, please.

Mr. HARPER. Thank you, Mr. Chairman, and thanks to each of you for being here today and really exciting to see the stuff on display this morning at the showcase, and I was obviously very happy to see Camgian Microsystems there which had a display on their new product, Egburt, so Gary Butler who started that. It is pretty remarkable what it does and can be used for a broad range of remote monitoring including the infrastructure help for say bridges and dams, and the future looks great for our country and to make sure that we have the innovation that we need and how we handle that, how we do it from Congress. So thank you for adding your insight to that.

Mr. Castro, I know we discussed the governance aspect of this already, but within that Internet of Things, would there be a difference on that governance based upon the specific product or machines in that variance there? How would you comment on that?

Mr. CASTRO. Absolutely. I think, you know, the traditional way that Congress has looked at a lot of data issues is industry specific. I think that is a very useful framework. And it, you know, differentiates us from Europe which has these broad-based privacy rules. And I think that is one of the reasons we were so much more successful I this space.

But going forward, we should continue to do that. We should look. Are there areas where people have particular sensitivities? Maybe it is in education. Maybe it is in healthcare. We have different rules there, but we allow that same flexibility of sharing data throughout all of those sectors.

Mr. HARPER. And so should that governance even different within itself be different than other industries, let us say? Give me a little bit more meat on the bones for that.

Mr. CASTRO. Yes. So you know, it really depends I think on what the consumer harm is that we are trying to protect against. So for example, you know, a really good example that we have historically is discrimination against pregnant women when they go to apply for a job. You know, that is something that we don't want to have happen. So we restrict that use. It doesn't matter how you found that information out. It doesn't matter if it is accurate or not. It doesn't matter if you guessed it from, you know, using some kind

of in-home smart system or you, you know, just saw someone walking down the street. The point is we regulate the use. And that is what we want to do. We want to look very clearly at what it is we don't want to have happen and make that illegal. And that provides consumers with confidence no matter where their data goes, or if there is a data breach, they are still safe.

Mr. HARPER. Well, what we want to make sure of from our end is we don't issue some regulation or enable some regulation that stifles innovation within the creative industry. And so that sometimes is a tough balancing act. But it seems to allow for more innovation if we get out of the way sometimes and don't create that roadblock at the beginning.

Ms. Schooler, if I could ask you, do you see an overlap between consumer uses and enterprise or industry use of the Internet of Things?

Ms. SCHOOLER. I will respond to that in two factions.

Mr. HARPER. OK.

Ms. SCHOOLER. I think from a privacy concern the use cases are very different. As Mr. Castro noted, I think the consumer privacy issues are going to need to have a specific type of set of considerations around how you share information, what personal information you share, versus in an enterprise implementation, you are really collecting, analyzing data within the confines of your own enterprise yourself. So I think those use cases will be very different.

The area that I do think that we can leverage learnings is in security. I think if we look at security as a foundational element built in from the onset of implementation, there is a couple different vectors that we have to consider. One, you need to secure the device, the network, and the cloud because all are critical on-ramps into the Internet of Things. And if you only secure one of those assets and not the entire pipeline, if you will, I think that is an insufficient way to look at the architecture from a device to a cloud perspective. So that is one.

Number two, I think we not only need to build in intellectual property into our silicon architectures and we are doing much of that at Intel, we also need to also build upon that software that monitors and manages those security concerns. The unique position that we are in at Intel is that we have both assets. So we are looking at how do we not only secure the device to the network to the cloud, how do we do it in silicon and how do we do it in software, such that we can create the most robust, secure, IoT implementation possible across consumer, industrial, and commercial implementations.

Mr. HARPER. Thanks to each of you, and I yield back the balance of my time.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman from Mississippi. Seeing no other members wishing to ask questions, I do want to thank the witnesses and the members for participating in today's hearing. Before we conclude, I would like to include the following document to be submitted for the record by unanimous consent: A letter on behalf of the Consumer Electronics Association.

[The information appears at the conclusion of the hearing.]

Mr. BURGESS. Pursuant to committee rules, I remind members they have 10 business days to submit additional questions for the record. I ask that the witnesses submit their response within 10 business days upon receipt of those written questions. I also want to take just a moment and thank the subcommittee staff for their hard work on the showcase this morning. I thought it was very informative and instructive, and without objection, the subcommittee is adjourned.

[Whereupon, at 12:28 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Consumer Electronics Association
1919 South Eads Street
Arlington, VA
22202 USA
866-858-1555 toll free
703-907-7600 main
703-907-7601 fax
CE.org

March 24, 2015

Chairman Michael C. Burgess and Ranking Member Jan Schakowsky
House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky;

On behalf of the Consumer Electronics Association (CEA)® please accept our views on the role of government and industry in the next shift in innovation, the Internet of a Things (IoT).

CEA is the trade association representing the $223 billion U.S. consumer technology industry. Every day, our more than 2,000 member companies are busy innovating; introducing extraordinary products and services and creating American jobs. At CEA, we work to advance government policies that encourage innovation and job and business creation.

CEA members are driving the growth of the IoT. Over 900 exhibitors displayed IoT devices at the 2015 International CES. The convergence of connected devices, cloud computing services, and powerful data analytics will help drive near to mid- term economic growth.

While businesses have been using connected devices, the IoT is new to the consumer market. Consumers are realizing its benefits, and our interactions with these devices will become so routine that they will go almost unnoticed. The IoT has profound potential to improve the lives of our citizens. Within a few years, Americans will be able to connect with their doctors remotely, share their health data and information and better manage their diseases. Home automation systems will enable consumers to manage their security systems, turn on appliances, and maximize their home's energy efficiency, all from a smart phone. Connected cars will eventually avoid collisions, but before then will notify first responders of an accident immediately, saving time and lives.

As this transition takes place, manufacturers and service providers will be focused on making good decisions about the privacy and security of information that devices collect and share. It is not only important to their customers; it is vital for them as well, because consumer adoption hinges on building trust. Devices that do not meet consumer privacy and security expectations will fail.

Along with the new capabilities that emerging technologies create also come questions about how to best protect users and promote consumer practices. CEA and others are exploring these issues and how best to ensure consumer privacy and security while enabling

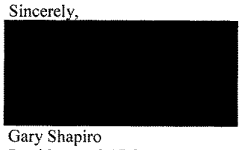
new technologies to develop. We believe that industry-driven solutions are the best way to promote innovation while protecting consumers.

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 or technologically biased standards will stymie growth and become outdated. If governments must act, such actions should be narrowly tailored to address tangible harms without creating roadblocks for future innovation.

Please recognize that the evolution of *things* comprise only part of the value of the entire IoT ecosystem. Analytics software extracts value and finds useful patterns in data collected by IoT devices. Data analytics are a vital tool in understanding consumers' needs and uses for products and allow companies to both improve current products and create new ones that meet consumers' needs and desires. The Internet runs on data. Restrictions on data collection may hurt new services which provide personal and societal benefits. We ask policymakers to tread carefully as they explore the potential and growth of the IoT.

The connected world of tomorrow will improve people's lives. CEA is proud to represent the companies whose products and services largely comprise the Internet of Things, and we look forward to working with the Committee to ensure the government supports growth and innovation through thoughtful policies.

Sincerely,



Gary Shapiro
President and CEO