INTERNET OF THINGS LEGISLATION

HEARING

BEFORE THE

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MAY 22, 2018

Serial No. 115–133

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
  Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
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
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
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
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

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
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 LUJÁN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CARDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio
Chairman

GREGG HARPER, Mississippi
  Vice Chairman
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
DAVID B. McKINLEY, West Virginia
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
JEFF DUNCAN, South Carolina
GREG WALDEN, Oregon *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
  Ranking Member
BEN RAY LUJÁN, New Mexico
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
DORIS O. MATSUI, California
PETER WELCH, Vermont
JOSEPH P. KENNEDY, III, Massachusetts
GENE GREEN, Texas
FRANK PALLONE, JR., New Jersey *(ex officio)*

(II)

CONTENTS

INTERNET OF THINGS LEGISLATION

TUESDAY, MAY 22, 2018

House of Representatives,
Subcommittee on Digital Commerce and Consumer
Protection,
Committee on Energy and Commerce,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in room 2322 Rayburn House Office Building, Hon. Robert Latta (chairman of the subcommittee) presiding.

Members present: Representatives Latta, Burgess, Lance, Guthrie, McKinley, Bilirakis, Mullin, Walters, Costello, Walden (ex officio), Schakowsky, Clarke, Cárdenas, Dingell, Matsui, Welch, Kennedy, and Pallone (ex officio).

Staff present: Mike Bloomquist, Deputy Staff Director; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight & Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Austin Stonebraker, Press Assistant; Hamlin Wade, Special Advisor, External Affairs; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; Lisa Goldman, Minority Counsel; Caroline Paris-Behr, Minority Policy Analyst; Michelle Rusk, Minority FTC Detailee; and C.J. Young, Minority Press Secretary.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. Latta. Well, good morning. I'd like to call the Subcommittee on Digital Commerce and Consumer Protection to order and the chair now recognizes himself for 5 minutes for an opening statement.

And again, good morning to our witnesses and welcome to this legislative hearing on the Internet of Things. Today, we will discuss the bipartisan State of Modern Application, Research, and Trends of IoT Act, or the SMART Act IoT discussion draft.

The SMART IoT Act discussion draft is the result of work the Digital Commerce and Consumer Protection Subcommittee has done over the past 2 years. Last July, this subcommittee held an Internet of Things Showcase. At that event, members invited com-

panies from our districts and across America to demonstrate products and services in the IoT field. It was a wonderful opportunity to see this revolutionary work up close and interact with the inventors doing this important work. To accompany that Showcase, we held a hearing where participants from the Showcase discussed their companies, challenges they face with growing in this space, and what we, as policymakers, can do to help promote the continued development of the IoT solutions.

This January, we held a hearing on the state of manufacturing in the IoT space and over the following months we met with other builders, suppliers, customers, and experts to better understand IoT's enormous potential.

This technology is having a real-life impact for many of our constituents. I've personally met with manufacturers in my district that are using this cutting-edge technology to maintain their machinery and keep production on track. I also met with farmers in Defiance, Ohio, who are using IoT for better grain management, increased planting and harvesting efficiency, and improved monitoring of the temperature in their storage facilities.

The draft legislation we discuss today is the result of important bipartisan work after hearing from the experts where we noticed one lingering question: What does the universe of rules, regulations, guidelines, and best practices look like for the IoT space?

While we know there are many other topics of interest in this space, this legislation kicks off a process to give all stakeholders a base set of information to frame the other challenges without speculating or hypothesizing about what already exists.

The IoT is already revolutionizing the way that we organize factories and supply chains, transport commodities like oil and gas, make manufacturing more efficient, maximize energy efficiency, and even restock our refrigerators.

This subcommittee has engaged in historic bipartisan work with the SELF DRIVE Act this Congress and I am pleased to see that cooperation continue with the SMART IoT. When safely applied to autonomous vehicles, the Internet of Things holds the potential to significantly reduce traffic fatalities and make our roads safer while reducing costs through more efficient fuel consumption.

In these areas and more, the IoT holds the potential to greatly improve the lives of Americans.

I want to thank my colleague, Representative Welch, for his willingness to continue our work together on this very important issue. As many here know, in previous Congresses Representative Welch and I started the Internet of Things Working Group. We heard from industry and other stakeholders about the importance of light-touch regulation to foster innovation and jobs here in the United States. This bipartisan draft is a result of the lessons learned in those meetings, this subcommittee's Disrupter Series hearings, and lays the groundwork for constructive conversations in the future. The SMART IoT Act will give all stakeholders, both private in industry and at the Federal level, a better sense of what guidelines and best practices exist or are in development.

As we all know, IoT issues cut across so many industries and so many Federal agencies. Ensuring that we know about overlaps or potential duplication is important for many reasons from ensuring

efficient use of government resources to understanding how stake-holders are addressing some of the important but challenging issues of privacy and data security.

From the Department of Commerce's efforts to foster the advancement of the IoT ecosystem to the Department of Transportation's focus on advancing automated vehicle, so much work is being done in this space. We want to encourage our interagency collaboration and foster an environment where transparency is key. Likewise, I would like to ensure that the environment for innovation in the United States across all of these industries remains a priority by optimizing our own efforts to promote good, consistent government. I believe the SMART IoT Act is an important step in doing just that.

And again, one of the things I always like to say is that one of the great things about serving on the Energy and Commerce Committee is that we kind of look over the horizon five to 10 years.

When we hear from our witnesses we want to hear from you to know exactly where you're going to be because we don't want to have our regulators or our laws that we were thinking about enacting looking in the rear view mirror or at the end of a car. We need to be looking far out into the future.

So, again, I want to thank our witnesses for being with us today and I look forward to your testimony today and, with that, I recognize the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes for an opening statement.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good Morning and welcome to this legislative hearing on the Internet of Things. Today we will discuss the bipartisan State of Modern Application, Research, and Trends of IoT Act or the SMART IoT Act discussion draft.

The SMART IoT Act discussion draft is the result of work the Digital Commerce and Consumer Protection Subcommittee has done over the past two years. Last July, this Subcommittee held an Internet of Things Showcase. At that event, Members invited companies from our Districts and across America to demonstrate products and services in the IoT field. It was a wonderful opportunity to see this revolutionary work up close and interact with the inventors doing this important work. To accompany that Showcase, we held a hearing where participants from the Showcase discussed their companies, challenges they face with growing in this space and what we, as policymakers, can do to help promote the continued development of IoT solutions.

This January we held a hearing on the state of manufacturing in the IoT space and over the following months we met with other builders, suppliers, customers and experts to better understand IoT's enormous potential.

This technology is having a real-life impact for many of our constituents. I've personally met with manufacturers in my district that are using this cutting- edge technology to maintain their machinery and keep production on track. I also met with farmers in Defiance, Ohio who are using IoT for better grain management, increased planting and harvesting efficiency, and improved monitoring of the temperature in their storage facilities.

The draft legislation we will discuss today is the result of important bipartisan work after hearing from the experts where we noticed one lingering question-what does the universe of rules, regulations, guidelines, and best practices look like for the IoT space?

While we know there are many other topics of interest in this space, this legislation kicks off a process to give all stakeholders a base set of information to frame the other challenges without speculating or hypothesizing about whatalready exists.

The IoT is already revolutionizing the way that we organize factories andsupply chains, transport commodities like oil and gas, make manufacturing more efficient, maximize energy efficiency, and even restock our refrigerators.

This subcommittee has engaged in historic bipartisan work with the SELF DRIVE Act this Congress and I am pleased to see that cooperation continue with the SMART IoT Act discussion draft. When safely applied to autonomous vehicles the Internet of Things holds the potential to significantly reduce traffic fatalities, and make our roads safer while also reducing costs through more efficient fuel consumption.

In these areas and more, the IoT holds the potential to greatly improve the lives of Americans.

I thank my colleague, Representative Welch, for his willingness to continue our work together on this very important issue. As many here know, in previous congresses Representative Welch and I started the Internet of Things Working Group. We heard from industry and other stakeholders about the importance of light-touch regulation to foster innovation and jobs here in the U.S. This bipartisan draft is a result of the lessons learned in those meetings, this subcommittees' Disrupter Series hearings, and lays the groundwork for constructive conversations in the future. The SMART IoT Act will give all stakeholders, both in private industry and at the Federal level, a better sense of what guidelines and best practices exist or are in development.

As we all know, IoT issues cut across so many industries and so many Federal agencies. Ensuring that we know about overlaps or potential duplication is important for many reasons from ensuring efficient use of government resources to understanding how stakeholders are addressing some of the important but challenging issues of privacy and data security.

From the Department of Commerce's efforts to foster the advancement of the IoT ecosystem to the Department of Transportation's focus on advancing automated vehicle, so much work is going on in this space. We want to encourage interagency collaboration and foster an environment where transparency is key. Likewise, I would like to ensure that the environment for innovation in the U.S. across all of these industries remains a priority by optimizing our own efforts to promote good, consistent government. I believe the SMART IoT Act is an important step in doing just that.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

This subcommittee frequently discusses the Internet of Things. We have hearings on IoT in manufacturing and wearable devices, not to mention our IoT showcase last summer.

Today, we transition from general discussion to discussion of actual legislation. The SMART IoT Act is a first step. It would require the Commerce Department to survey the use of connected devices and examine the Federal role in this space.

As the bill acknowledged, internet-connected devices provide an opportunity for economic growth. But we want to ensure that those devices are developed securely. My hope is that the report generated by the SMART IoT Act provides the foundation for further legislative efforts.

Our hearings on the Internet of Things have raised important issues. What privacy and cybersecurity protections are going to be baked into these devices? Normal household items can now collect very personal data that must be stored and used appropriately. Connected devices present new safety concerns. The Consumer Product Safety Commission just held a public hearing on IoT and safety last week with stakeholders on that very subject.

We need the infrastructure to support the rise of connected devices including affordable broadband. The Internet of Things could also disrupt the current labor market. We must ensure workers are prepared for a changing economy.

Finally, we must make the strategic investments in research to promote future innovation. Last week's hearing on quantum computing made clear that the United States is not providing the consistent support necessary to keep groundbreaking research moving forward. Standing on the sidelines is simply not an option. These are big issues for Congress to tackle and we must rise to the challenge. We know what happens if we rely on industry self-regulation. Consumer privacy goes unprotected and safety is put at risk. The SMART IoT Act should provide a resource for us to better understand the variety of devices on the market.

I plan to use this information as I continue my push for comprehensive consumer privacy and data security legislation. We have had bipartisan furor over misuses of consumer data. It's time now for bipartisan solutions to the problem. The bill before us is a natural extension of the work that members of the subcommittee have been doing for the last couple of sessions.

In 2016, Congressmen Latta and Welch convened stakeholders for several forums under their IoT Working Group to discuss the Internet of Things and the issues that new technology raise.

In many ways, the study and the SMART IoT Act is a formalization of that very survey. In the coming weeks, I look forward to working on a bipartisan basis to move this legislation forward, and then I am ready to take the next step of updating consumer protections and funding key investments.

The Internet of Things has tremendous potential. We must work together to make sure that America benefits from that opportunity.

I thank you, Chairman Latta. I yield back, unless anybody wants the remaining time.

I yield back.

Mr. LATTA. Thank you. The gentlelady yields back.

The chair now recognizes the gentleman from Oregon, the chairman of the full committee for 5 minutes.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Good morning, Mr. Chairman, and other members on the committee and to our witnesses on the panel. Thank you for being here.

Today, we will hear testimony about the draft bill, the SMART IoT Act, to support the development of the Internet of Things here in the United States. This bipartisan effort underscores one of the key goals of the Energy and Commerce Committee, and that is helping American entrepreneurs and established businesses expand to create jobs for American workers and help improve the lives of American consumers.

So I would like to thank Chairman Latta and Representative Welch for working on this issue and finding a bipartisan path forward. This is what we do at the Energy and Commerce Committee, particularly on this subcommittee when faced with new technology policy questions. We have done that on the Self Drive Act. I would commend my colleagues on both sides of the aisle for the good work there. Now we just need to get the Senate to move forward, as we are won't to do in many cases.

The Internet of Things, or IoT, does hold great promise to connect workers, suppliers, products, consumers throughout efficient networks that can save time, money, and bring about new innovation and resources.

Building this network won't be easy. We know that. It requires engineers, entrepreneurs, and visionaries. It also requires public policies that foresee a world designed for the next-century policies that foresee a world designed for the next century policies that are forward looking and that reflect a world to come of self-driving cars, self-organizing materials, and innovations we have yet to even think of. These must replace many of our still-existing rules and policies that reflect the old technologies of the last century. While America has changed, many of our regulations, unfortunately, have not.

That is one of the purposes of this legislation that's before us today. It is meant to set the stage by making sure stakeholders are aware of the playing field and are not creating conflicting or duplicative obligations or requirements. So the SMART IoT Act will create the first compendium of essentially who is doing what in the IoT space. This includes the efforts undertaken by private industry as well as a review of what agencies are doing.

Removing regulatory barriers to innovation is one of the most important duties of this committee. Doing so allows our economy to grow, our workers to flourish, and innovation to occur here in the United States. The best way to start is to know what is out there already or being developed today.

It's important to note that since January of 2017 more than 3 million new jobs have been created in America. The U.S. unemployment rate, now at 3.9 percent, is the lowest seen in this country since the year 2000, and what's more, this comes as more Americans rejoin the workforce, millions once again finding work after years of hardship.

So creating jobs and opportunity is a goal shared by all of us on this committee, in fact, reflected in the bipartisan work on the SMART IoT Act. Chairman Latta and Representative Welch have been working on these issues for several years now. Glad to see that this progress has been made and we have a great opportunity, going forward, to do even more.

So, Mr. Chairman and members of both sides of the aisle, thanks for your good work on this. We have a couple hearings going on simultaneously, as I am sure our witnesses and members know.

So some of us will be popping back and forth. But we value your testimony that we have here and the good bipartisan work.

And with that, I yield back the remaining balance of my time.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning, and thank you to our witnesses for appearing before theSubcommittee. Today we will hear testimony about a draft bill, the SMART IoT Act, to support the development of the Internet of Things here in the United States. This bipartisan effort underscores one of the key goals of the Energy and Commerce Committee: helping American entrepreneurs and established businesses expand to create jobs for American workers and help improve the lives of consumers.

I would like to thank Chairman Latta and Representative Welch for working on this issue and finding a bipartisan path forward. This is what we do at the Energy

and Commerce Committee and particularly on this subcommittee when faced with new technology policy questions.

The Internet of Things, or IoT, holds the promise to connect workers, suppliers and products through more efficient networks that can save time, money and resources.

Building this network will not be easy. It requires engineers, entrepreneurs and visionaries. It also requires public policies that foresee a world designed for the next-century policies that are forward looking, and that reflect a world to come of self-driving cars, self-organizing materials, and innovations we have yet to even think of. These must replace many of our still-existing rules and policies that reflect the old technologies of the last century. While America has changed, many of our regulations have not.

That is one of the purposes of the legislation we will discuss today. It is meant to set the stage by making sure stakeholders are aware of the playing field and are not creating conflicting or duplicative obligations or requirements. The SMART IoT Act will create the first compendium of essentially who is doing what in the IoT space. This includes the efforts undertaken by private industry as well as a review of what agencies are doing.

Removing regulatory barriers to innovation is one of the most importantduties of this Committee. Doing so allows our economy to grow, our workers to flourish and our citizens to benefit. The best way to start is to know what is out there already or being developed today.

Since January 2017 over three million new jobs have been created in America. The U.S. unemployment rate is 3.9 percent, the lowest seen in this country since the year 2000. What's more, this comes as more Americans rejoin the workforce, millions once again finding work after years of hardship.

Creating jobs and opportunity is a goal shared by all of us on this Committee, a fact reflected in the bi-partisan work on the SMART IoT Act. Chairman Latta and Representative Welch have been working on these issues for several years now, and I'm glad to see the progress they have made.

We have made great progress over the last two years in restoring jobs for American workers, restarting American manufacturing, and creating opportunities for Americans of all ages and backgrounds. But there is more work yet to be done. Legislation such as the draft bill we consider today is one way that we will continue to fulfill our duty to the American people to remove barriers to success while promoting policies that help our workforce.

American ingenuity and leadership is once again transforming the world.That is something we can all be proud of. Thank you Chairman Latta for the leadership you have shown, and thanks as well to all the Members of this Subcommittee.

Thank you Mr. Chairman and I yield back the balance of my time.

Mr. LATTA. Well, thank you very much. The gentleman yields back, and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes.

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 on the draft SMART Internet of Things Act is the next step in this subcommittee's review of new and evolving technological development and I commend Chairman Latta and Representative Welch for working together over the last several years to explore and learn how the Internet of Things, or IoT, can enrich our lives, help us be more efficient, and grow the U.S. economy.

Today, more and more people have multiple internet-connected devices in their homes, things like thermostats, vacuums, and digital personal assistants, and more and more people are wearing internet-connected devices such as fitness trackers. But IoT is not limited to consumer products. Connected devices of all kinds are

used in practically every industry sector like manufacturing, agriculture, and medicine.

We have learned about drones that fly into dangerous areas to assess hazards, sensors helping farmers understand the topography acidity of their land, and doctors receiving real-time data from monitors so that patients in remote areas do not have to travel for daily appointments.

And today we are considering a bipartisan draft bill that would direct the Department of Commerce to conduct a comprehensive study and report on the Internet of Things. Commerce will survey the industry sectors that make internet-connected devices as well as all industry sectors that use those devices. The study will also look at how the Federal Government oversees the use and development of connected devices, which agencies deal with the Internet of Things, what expertise those agencies have, and what entities those agencies interact with, and the study will identify government resources available to consumers and small businesses to help them evaluate connected devices.

The report will provide a one-stop source of how businesses are integrating connectivity and how the Federal Government is helping the country adapt to this age of connectivity. Federal and local government agencies could also use the report to better coordinate their work and I hope the study will encourage them to do so. And any report will be a snapshot in time, but given the integration of IoT into all parts of our lives in the global economy, the report will provide a jumping-off point for more work.

I would certainly like to see cybersecurity issues given more emphasis when we look at IoT. Throughout our review, cybersecurity was the issue that came up most often. Cybersecurity is imperative to keeping ourselves and our country safe from malicious actors.

And I know some stakeholders have asked that cybersecurity be specifically called out in the study. I would support such a change. But whether it's made part of the study required by this bill or not, Congress must take action to ensure that strong cybersecurity and data security are fundamental to IoT.

So I am glad that this subcommittee is working on this bipartisan legislation and I'd like to yield the balance of my time to the sponsor, Congressman Welch.

OPENING STATEMENT OF HON. PETER WELCH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VERMONT

Mr. WELCH. Thank you very much, and I want to thank Chairman Latta and Ranking Member Schakowsky for this hearing. It was great to work with Mr. Latta too in the IoT Working Group— 21 members that had hearings in advance.

We are trying to get educated before we pass legislation, which isn't necessarily how we usually operate. But this is a huge opportunity with the Internet of Things. McKinsey and Company did a study and says that it can be between $4 and $11 trillion annually by 2025. So that's really quite extraordinary.

My colleagues have already spoken about what many of these opportunities are and also, Ranking Member Schakowsky, I think pointing out some of the implications that we have to contend with with labor is really, really important for all of us to keep in mind.

But I'll just give one example. In Vermont, the brutal pressure on our dairy farmers right now—the price is down, the costs are up—and technology is helping some of those farmers hang on. And Mangan Brothers, a dairy farm in East Fairfield, Vermont, has a computerized internet-based milking system that's really been helpful to them. They installed a milking parlor about two decades ago and now what happens when the cow comes in they have a pedometer on their leg, and as soon as the cow crosses the threshold of the milking parlor the sensor picks up which cow it is and relays the information to the computer and all the statistics about the cow's movements and body temperature and other pertinent information is sent to the computer, and it's even relevant for when the breedings are done just based on activity spikes. It also gives them a report at the end of every milking day with respect to the salt content and that's an indicator that allows the farmers to take steps to avoid diseases.

So it's a big deal in terms of productivity for them and it is made possible by the Internet of Things. And just the last point in my last few seconds, the only way we are going to have the Internet of Things in rural America is to have broadband in rural America, and that's another enormous challenge we have and it's woefully underserved.

So we can talk all we want about the Internet of Things, but unless we have broadband it's not going to happen.

So I yield back and thank my colleagues for the time.

Mr. LATTA. The gentleman yields back, and I just want to say just briefly I really appreciate all the work that you and I have done on IoT and also not only chairing the working group but also working together chairing the rural broadband, so I appreciate all you've been doing and thank you very much.

That now concludes members' opening statements and the chair now reminds members that pursuant to committee rules, all members opening statements will be made part of the record.

And, again, I want to thank all of our witnesses for being with us today. We greatly appreciate you taking the time to testify before the subcommittee.

Today's witnesses will have the opportunity to give 5-minute statements followed by a round of questions from our members.

Our witness panel for today's hearing will include Mr. Tim Day, the Senior Vice President of the Chamber Technology Engagement Center at the U.S. Chamber of Commerce, Ms. Michelle Richardson, Deputy Director of the Freedom Security and Technology Project at the Center for Democracy and Technology, and Dipti Vachani, Vice President of the Internet of Things Group and General Manager of the Strategy and Solutions Engineering Division at Intel.

And, again, I want to thank you all for being here today and Mr. Day, you are recognized for 5 minutes. If you'd just pull that mic up close and turn the mic on, the microphone is yours.

**STATEMENTS OF TIM DAY, SENIOR VICE PRESIDENT, CHAM-
BER TECHNOLOGY ENGAGEMENT CENTER, U.S. CHAMBER
OF COMMERCE; MICHELLE RICHARDSON, DEPUTY DIREC-
TOR, FREEDOM, SECURITY, AND TECHNOLOGY PROJECT,
CENTER FOR DEMOCRACY AND TECHNOLOGY; DIPTI
VACHANI, VICE PRESIDENT, INTERNET OF THINGS GROUP,
GENERAL MANAGER, PLATFORM MANAGEMENT AND CUS-
TOMER ENGINEERING, INTEL CORPORATION**

STATEMENT OF TIM DAY

Mr. DAY. Thank you very much.

Good morning, Chairman Latta, Ranking Member Schakowsky, and distinguished members of the House Subcommittee of Digital Commerce and Consumer Protection.

Thank you for the opportunity today to testify about the Internet of Things. I am Tim Day, Senior Vice President of the Chamber's Technology Engagement Center, or C 09TEC. The Chamber established C 09TEC 3 years ago to tell the story of how technology can empower all Americans. At C 09TEC, we have focused our work on autonomous vehicles, unmanned aircraft, telecommunications, and the new economy.

All of these issues and technologies are connected and supported by the Internet of Things. Everyone participating in this hearing today is in one way or another one of the nearly 11 billion internet-connected devices projected by Gartner to be in use today world-wide.

Whether we are streaming this hearing on a smart phone, whether or not we have asked Amazon, Alexa, or Google Home di-rections to the Rayburn House Office Building, or a wearable counted the number of steps it took to get here, we all have been connected and our lives are being improved by the Internet of Things.

Not only does IoT technology directly benefit consumers, it is also making businesses smarter and more efficient. For example, the agricultural sector for better crop yields, health care for improved patient outcomes, and manufacturing for improved operations and maintenance. One study has shown that industrial manufacturing IoT spending is predicted to increase to $890 billion worldwide by 2020. And, of course, government also stands to benefit from IoT by creating efficiencies in public services, by finding new value for citizens, enhancing capabilities, and streamlining processes. IoT may provide a much-needed answer for agencies seeking to meet increasing citizen needs with decreasing budgets.

And, Chairman Latta, back home in the Buckeye State, Colum-bus, which was awarded the DoT's 2016 Smart Cities Challenge Grant, is using IoT in research and development to create smart vehicle technologies. Another study has shown that wireless pro-viders will invest $275 billion towards building 5G networks, which will be part of the connectivity backbone of smart cities and IoT. This investment will add $500 billion in GDP and 3 million jobs to the American economy. This number pales in comparison to the $11 trillion worldwide economic impact that is predicted by 2025 for IoT.

Needless to say, IoT is an economic game changer. The Chamber's president and CEO, Tom Donohue, has stated that technology must be embraced as the growth driver and game changer that it is. That is why it is so critical that the United States maintain leadership in IoT by adopting the right regulatory framework.

I would like to suggest a couple of ideas for your consideration to strike the correct regulatory balance. Congress and agencies should do more to reduce the regulatory burdens, compliance costs, and overlap. Government should evaluate existing regulatory activities and bring together stakeholders in government industry to shape IoT policy.

Legislation like the DIGIT Act and the draft legislation today, the SMART IoT Act, are much-needed steps in the right direction to achieve this goal. Additionally, actions like those done by the FCC led by Commissioner Carr to streamline communications siting rules are also to be praised. As IoT is still in its infancy, policymakers should avoid the temptation to impose prescriptive regulations on IoT and single out IoT for regulation for issues such as privacy.

Congress should continue a policy of technology neutrality and, finally, a skilled workforce will also be critical to the development of this new technology and investment in human capital will determine which countries lead, going forward in this space.

We are currently witnessing a new industrial revolution led by advanced technology including IoT, which is a force for good that should be fostered by smart regulatory frameworks that encourage investment, promote innovation, as well as connect and empower all Americans.

Thank you for this opportunity. I look forward to your questions.
[The prepared statement of Mr. Day follows:]

_TEC

U.S. Chamber of Commerce
Technology Engagement Center

Statement of the Chamber Technology Engagement Center

ON: HEARING ON "Internet of Things Legislation"

TO: U.S. HOUSE ENERGY AND COMMERCE COMMITTEE, SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

DATE: May 22, 2018

1615 H Street NW | Washington, DC | 20062

BEFORE THE U.S. HOUSE ENERGY AND COMMERCE COMMITTEE,
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION
Hearing on "Internet of Things Legislation"
Testimony of Tim Day
Senior Vice President, Chamber Technology Engagement Center

May 22, 2018

Good morning, Chairman Latta, Ranking Member Schakowsky, and distinguished members of the House Subcommittee on Digital Commerce and Consumer Protection. My name is Tim Day and I am the Senior Vice President of the Chamber Technology Engagement Center (or C_TEC). C_TEC was created to promote the role of technology in our economy and to advocate for rational policies that drive economic growth, spur innovation, and create jobs. C_TEC understands the transformative opportunities IoT presents for consumers, businesses, and our country's economy. C_TEC also appreciates that regulatory and other barriers can impede the development of a nascent IoT and delay the full realization of its many benefits.

IoT represents the next evolution of the Internet and mobility. Much like the Internet's earlier phases, IoT will flourish under a flexible, non-regulatory policy regime. Light regulation and uniform federal policy fostered the explosion of both wireline and wireless connectivity. Today's mobile Internet ecosystem is a driver of innovation, economic growth, and improved consumer welfare. This transformative growth has occurred largely because of the United States' measured approach to regulation.

The lesson for IoT is clear: farsighted regulatory policies that relieve regulatory barriers have a positive effect on the growth of technologies and services. The winners in this process equally are clear: consumers, who not only benefit from enhanced and expanded services, but also from the economic growth and increased opportunities that flow from them.

Given the unqualified success of this approach, the focus of policymakers should be on ensuring a similar enabling environment for IoT. The U.S. government should ensure innovators have the freedom to develop solutions that will drive widespread adoption. As developed below, several steps will help policymakers promote IoT while appropriately addressing challenges and ensuring broader goals. The Administration should:

- **Work to pass the Developing Innovation and Growing the Internet of Things ("DIGIT") Act**. The DIGIT Act will bring together stakeholders in government and industry to shape IoT policy, ensuring that the United States realizes the full economic potential of IoT and remains a leader in this next chapter of the Internet.

- **Reduce regulatory burdens, compliance costs, and overlap**. A multitude of uncoordinated state and federal efforts in IoT is creating an uncertain regulatory environment. Government should evaluate existing regulatory activities and ensure that they are supportive of IoT and do not constitute unintentional barriers. *Today's draft study language takes a step in the right direction to alleviate these burdens.*

- **Remove barriers to investment and infrastructure deployment at all levels.** Infrastructure will be critical for IoT deployment, and the government should look for ways to promote deployment and upgrades of communications networks.

- **Champion voluntary, industry-led, globally recognized, and consensus-based processes for technical and interoperability standards.** Historically, the most effective process for developing standards has been driven by the private sector through a variety of open participation, globally recognized, voluntary, and consensus-based standards groups, industry consortia, and companies.

- **Encourage industry and government collaboration to solve evolving security and privacy challenges.** Prescriptive regulation is unnecessary and unwise at this early stage. Approaches to security and privacy must remain collaborative, flexible, and innovative over the long term—enabling solutions to evolve at the pace of the market.

- **Promote a skilled workforce capable of operating in the digital future.** Investment in human capital will determine which countries lead in the IoT.

I.   THE "INTERNET OF THINGS" HOLDS INCREDIBLE PROMISE FOR OUR ECONOMY AND QUALITY OF LIFE

The IoT is empowering people to interact with technology and improve their lives—not only as an evolving technology, but also as a catalyst for innovation. At its core, IoT encompasses unprecedented connectivity. Former Acting Chairman Ohlhausen of the Federal Trade Commission ("FTC") aptly described IoT as "[t]he next phase of Internet development [that] is focusing on connecting devices and other objects to the Internet, without the active role of a live person, so that they can collect and communicate information on their own and, in many instances, take action based on the information they send and receive."[1] While it is an evolving concept, IoT includes a myriad of objects—including tags, sensors, and devices—that interact with each other through hardware and software applications to extract meaningful information.

Without question, IoT has revolutionary potential. One study projects the number of IoT devices by 2020 will reach 20.4 billion.[2] Analysts predict that IoT will have a total economic impact in the trillions of dollars. By some accounts, "the IoT has a total potential economic impact of $3.9 trillion to $11 trillion a year by 2025."[3] In C_TEC's view, "[t]he Internet of Things could add as much as $15 trillion to global GDP over the next twenty years."[4]

---

[1] "The Internet of Things and The FTC: Does Innovation Require Intervention?," Remarks of Commissioner Maureen K. Ohlhausen, U.S. Chamber of Commerce (Oct. 18, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internetthingsremarks.pdf.

[2] Liam Tung, "IoT devices will outnumber the population this year for the first time," ZDNet (Feb. 7, 2017) *available at* https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.

[3] McKinsey Global Institute, Report, Unlocking the Potential of the Internet of Things, at 2 (Jun. 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[4] Letter from William L. Kovacs, U.S. Chamber of Commerce, to Donald S. Clark, Federal Trade Commission,

The benefits of increased connectivity will come from two main areas: consumer-facing IoT and industrial or enterprise IoT. While consumer-facing IoT is what most people think of first, the industrial IoT is expected to account for the lion's share of GDP growth. It is important that policymakers do not conflate consumer-facing and industrial IoT.

As C_TEC recognizes, "[t]he Internet of Things will lead to smarter homes, smarter cities, enhanced healthcare, and improved efficiency and productivity."[5] Consumer IoT promises life-changing innovations. Smart homes and home monitoring will promote efficiency, security, and even aging-in-place. Personal wearable and medical devices will improve care and lead to innovations in insurance. Connected and autonomous transportation will improve urban planning and automotive safety in smart cities. Even media platforms will be affected, as smart TVs and Virtual Reality will impact how consumers experience the world.

Industrial IoT offers equally important innovations, with enormous potential across the global marketplace in agriculture, manufacturing, transportation, and utilities, to name a few. Industrial IoT can protect employees, increase productivity, manage inventory, improve transportation safety and congestion, conduct predictive maintenance, and spur economic growth and competition. With many potentially disruptive technologies promising higher productivity and greener production, industrial IoT may change the global production of goods and services.

Of course, government also stands to benefit from IoT, which can create efficiencies in public services. By finding new value for citizens, enhancing capabilities, and streamlining processes, IoT may provide a much-needed answer for agencies seeking to meet increasing citizen needs with decreasing budgets. The General Services Administration ("GSA"), for example, is using IoT for building maintenance.[6] Connected apps and devices also have the potential to revolutionize public safety, law enforcement, and military operations.

Much is still unknown about the future of IoT, including industry structures, business models, distribution and supply chains, and the uses and flows of data from IoT devices. Ultimately, the benefits of IoT will be limited only by the capacity of innovators, and by government decisions to allow barriers to persist or instead to pursue policies that support innovation.

II.   REGULATION OR LEGISLATION WOULD BE PREMATURE GIVEN THE EARLY AND RAPIDLY EVOLVING NATURE OF IOT TECHNOLOGY

The transformative potential of IoT will be realized only in a hospitable regulatory environment. IoT is at a similar stage as the Internet was in the 1990s—emerging commercially,

---

Project No. P135405, at 2 (dated Jan. 10, 2014),
https://www.uschamber.com/sites/default/files/documents/files/1.10.14-%20Comments%20on%20the%20Internet%20of%20Things.pdf ("Chamber IoT Letter").
[5] *Id.*
[6] *See* GovLoop, Report, The Internet of Things: Preparing Yourself for a Connected Government, https://www.vion.com/assets/site_18/files/gl_guide_iot_final%20(3).pdf.

with diversity and experimentation, competing standards, and unclear consumer expectations. The Internet's unbridled success results from a minimal regulatory framework, which has been the foundation for the United States' global Internet leadership for decades.

That historical record should inform any federal approach to IoT. Prescriptive legislation is unnecessary and unwise. Premature or reflexive regulation can have unintended consequences, by mandating specifications that become obsolete, or worse, by inadvertently creating security vulnerabilities. Those well-documented risks increase when the government tries to regulate a technologically evolving field like IoT. Unnecessary restrictions here risk limiting opportunities—and U.S. competitiveness—in the global marketplace.

Regulators should refrain from reflexive regulation at this juncture. Even after a national IoT strategy is developed, they should proceed with caution. IoT technology and use will change rapidly, and should be guided by technological advancements, not regulatory classifications or silos.[7] The U.S. government should exercise regulatory restraint, reduce barriers, and empower innovators to develop products that will drive demand.

III. PRIVATE SECTOR IOT INNOVATION DEPENDS ON INFRASTRUCTURE, VOLUNTARY STANDARDS, AND TECHNICAL NEUTRALITY

A. Infrastructure Investment Will Be Critical to the Future of IoT

Widespread adoption of IoT in homes, cities, and industries will place demands on communication infrastructures and services. Infrastructure will be critical, and the government should look for ways to promote investment, deployment, and upgrades of communications networks, including next-generation cellular ("5G") and Wi-Fi. Lack of infrastructure will hinder IoT.

Federal policy has long sought to promote infrastructure improvements to expand communications networks. According to Accenture, one component of the wireless infrastructure necessary—5G—will lead to $275 billion in investment that will create 3 million new jobs and $500 billion in U.S. GDP growth.[8] This investment is even more critical in a world of burgeoning demand for data services, including IoT. Wireless broadband availability is not only covering more of the population, infrastructure providers are "laying the rails" inside buildings, underground in metros, on university and corporate campuses, in stadiums, retail outlets, and on airplanes. Infrastructure must be built where people and objects congregate.

Congress and the Federal Communications Commission ("FCC"), however, have noted that "unreasonable delays" and limits through zoning and access restrictions at the state and local

---

[7] Ohlhausen 2014 Remarks, at 1-2 ("It is thus vital that government officials, like myself, approach new technologies with a dose of regulatory humility. We can accomplish this by educating ourselves and others about innovation, understanding its effects on consumers and the marketplace, and identifying benefits and likely harms.").

[8] "Smart Cities: How 5G Help Municipalities Become Vibrant Smart Cities" Accenture (2017) *available at* https://www.accenture.com/t20170222T202102Z__w__/us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

level have been "obstruct[ing] the provision of wireless services."[9] FCC Commissioner Brendan Carr's plan to reduce these regulatory barriers and make America 5G ready is also a step in the right direction to deploy connectivity.[10] More can be done and both Congress and agencies should reduce regulation and limit federal, state, and local barriers to infrastructure deployment. Infrastructure investment will not only be critical to realizing IoT's full potential, it is capable of rapidly creating jobs and technologies that will maintain the nation's technological, political, and economic position.[11]

B. Technical Standards for IoT Should Remain Open and Voluntary

Technical standardization can reduce barriers to entry to IoT markets and increase economies of scale. However, standards need to be voluntary and carefully designed so that they do not constrain innovation. Historically, the most effective process for developing technical and interoperability standards has been driven by the private sector through open participation, globally recognized, voluntary, and consensus-based standards organizations, industry consortia, and individual companies working together. Governments and policymakers should encourage open standards and commercially available solutions to accelerate innovation and adoption.

The IoT marketplace currently is aligning around industry verticals that are starting to deploy solutions. Although a fragmented ecosystem with non-interoperable technologies could undermine the efficiencies achieved by large economies of scale, tying industry at this early stage to burdensome, conflicting, or one-size-fits-all standards would be harmful. Rapid innovation likely will mean that early approaches quickly will be surpassed. In addition, mandatory standards could tie users to a specific vendor or country requirement to the exclusion of others, which may drive up costs and create barriers to innovation.

Voluntary, industry-led, globally recognized standards can drive secure, flexible, and interoperable solutions that scale across a global IoT ecosystem. Recent standardization efforts for cybersecurity provide a useful example. Like IoT, efforts to improve cybersecurity must reflect the borderless and interconnected nature of our digital environment. Cybersecurity efforts are optimal when they reflect globally recognized standards and industry-driven practices. Cybersecurity standards, guidance, and best practices typically are led by the private sector and adopted on a voluntary basis; they are most effective when developed and recognized globally.[12]

---

[9] *Petition for Declaratory Ruling to Clarify Provisions of Section 332(7)(B)*, Order, 24 FCC Rcd 13994, 14006 (2009); *see also* Spectrum Act provisions promoting colocation of wireless equipment, 47 U.S.C. § 1455, and regulations implementing same, 47 C.F.R. § 1.40001. As the FCC and courts have observed, "'[d]espite the widely acknowledged need for additional wireless infrastructure, the process of deploying these facilities can be expensive, cumbersome, and time-consuming …[and] local and Federal review processes can slow deployment substantially, even in cases that do not present significant concerns.'" *Montgomery County Md. v. FCC*, 811 F.3d 121, 125-26 (2016) (quoting *In re Acceleration of Broadband Deployment by Improving Wireless Facilities Siting Policies*, 29 FCC Rcd. 12865 ¶¶ 9-10 (Oct. 17, 2014), amended by 30 FCC Rcd. 31 (Jan. 5, 2015)).
[10] Tim Day, "Here's How to Make Cities Smarter," *Above the Fold* (Mar. 22, 2018) *available at* https://www.uschamber.com/series/above-the-fold/here-s-how-make-cities-smarter.
[11] Jordan Crenshaw, "Three Ways to Bring Communications Regulations into the Digital Age," *Above the Fold* (Nov. 15, 2017) *available at* https://www.uschamber.com/series/above-the-fold/three-ways-bring-communications-regulations-the-digital-age.

[12] Letter from Ann M. Beauchesne, U.S. Chamber of Commerce to Michael Hogan and Elaine Newton, National

Ultimately, technological maturity and user choice will identify optimal standardization. Whether the topic is interoperability, IP address assignments, cybersecurity, or other technical questions, government should encourage industry collaboration in open participation, globally recognized, consensus-based, and voluntary standards efforts. Government also should champion appropriate standards efforts internationally. This is consistent with federal law promoting commercially driven solutions and reflects the need for standards to mature long before even being considered for incorporation into federal regulatory obligations.[13]

C.   Privacy Concerns Should be Addressed in a Technologically Neutral Way

Without evidence of heightened privacy concerns or consumer harm, there is no reason not to allow the IoT market mature under the frameworks that exist for protecting consumers' legitimate privacy interests. In its 2015 Staff Report on IoT, the FTC concluded that there was not yet a need to regulate consumer-facing IoT privacy.[14] C_TEC agrees. As with other technologies, the onus is on industry to safeguard consumers and their data, and to communicate appropriate information, consistent with existing privacy regimes. Any consideration of consumer-based IoT privacy should be part of a bigger discussion, which can examine the immense benefits from new uses, as well as best practices, disclosure, and self-regulation.[15]

Prescriptive regulation entails significant costs. We are in the early stages of IoT, and it is not yet clear what heightened privacy concerns IoT poses, if any. Indeed, the privacy issues raised by IoT may be similar to those raised by existing technologies, such as cloud computing; existing approaches are evolving at the pace of the market to safeguard legitimate privacy interests. Moreover, the FTC has not been shy about monitoring consumer-facing IoT and pursuing fraud, misrepresentation, and allegedly unreasonable practices, as it does with other consumer-facing technologies and products.[16]

The FTC and others must resist a temptation to pursue prescriptive solutions to hypothetical problems.[17] For example, in its Staff Report, the FTC suggested practices for data minimization. Because such reports inadvertently can become the basis for enforcement or

---

Institute of Standards and Technology (NIST) re: Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Sept. 24, 2015).

[13] *See, e.g.,* Office of Management and Budget, OMB Circular A-119, https://www.whitehouse.gov/sites/default/files/omb/inforeg/revised_circular_a-119_as_of_1_22.pdf; *see also* National Technology Transfer and Advancement Act, Public Law 104-113 (1996).

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

[15] For example, the automotive industry has voluntarily developed and adopted best practices and guidelines to protect consumer privacy. These principles are based on the Fair Information Practice Principles. See Privacy Principles for Vehicle Technologies and Services (Nov. 13, 2014), http://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services.

[16] *See, e.g.,* TRENDNet, Inc., (Feb. 2014) (the FTC's "first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices– commonly referred to as the 'Internet of Things.'")

[16] Michael Hendrix, "With the Internet of Things, What's to Fear?" (Jan. 29, 2015), https://www.uschamberfoundation.org/blog/post/internet-things-whats-fear/42532.

[17] Registered Perspective on Copyright Review, H. Comm. on the Judiciary (Apr. 29, 2015) (Statement of the U.S. Chamber of Commerce).

regulation as they filter through government, government should not follow a "precautionary principle" that might prematurely elevate concerns and chill innovation.

IV. A NATIONAL STRATEGY SHOULD PROMOTE INVESTMENT, REDUCE REGULATION, AND CHAMPION MARKET-BASED SOLUTIONS GLOBALLY

Congress should consider how to streamline regulation and remove barriers at the federal, state, and local levels. As the National Telecommunications and Information Administration (NTIA) noted, a "patchwork of regulation threatens to increase costs and delay the launch of new products and services. That, in turn, could dampen investment."[18] Economies of scale mean that larger markets will be important to innovation and connectedness. NTIA should champion an enabling environment domestically and globally.

A. Overlapping Federal Approaches Introduce Regulatory Uncertainty and Duplicate Efforts

A multitude of uncoordinated state and federal efforts in IoT is creating an uncertain regulatory environment. Multiple federal agencies may have jurisdiction over aspects of IoT, including overlapping rule-making and enforcement authority. State governments and agencies also are active in IoT, resulting in a confusing patchwork of regulations that can interfere with product development and consumer expectations. Many federal and state activities have not kept pace with technological developments. Policymakers should seek to simplify the regulatory process and curtail multiple regulatory frameworks that serve as barriers to IoT.

To illustrate, whereas a company making a device for a car previously may have worked with a single government agency, a company developing connected devices for cars today could very well be subject to overlapping or inconsistent federal oversight from a consumer protection regulator (the FTC), a transportation safety regulator (NHTSA), and a spectrum regulator (FCC), among others. A company making medical IoT devices might be subject to the FDA, FTC and FCC oversight, and a UAS company might be subject to the FAA, FTC, and FCC jurisdiction. In this environment, inter-agency coordination is a must to avoid stifling innovation, slowing GDP growth, reducing predictability, and multiplying burdens. Today's legislation at issue is a step in the right direction toward unraveling the web of duplicative regulatory frameworks.

State and local interests also can impede rapid, scaled deployment. Vague state laws, such as those about gathering consumer data, can stifle innovation. Technical mandates, like those mandating a smartphone "kill switch" or encryption, can balkanize markets, interfere with product development and distort consumer expectations. Finally, barriers to infrastructure deployment from zoning and land use limitations can slow the building and upgrading of wireless facilities that will be essential to IoT. The federal government should look for those barriers and seek to eliminate them.

---

[18] Alan Davidson and Linda Kinney, "Fostering Investment and Innovation in Smart Cities and the Internet of Things (IoT)," NTIA, (Feb. 25, 2016), https://www.ntia.doc.gov/blog/2016/fostering-investment-and-innovation-smart-cities-and-internet-things-iot.

A national strategy for IoT can forestall problems by sending a clear message that over-regulation or poorly-designed regulation threatens IoT growth. A national strategy can encourage regulators to focus on activities that would expand, rather than limit, the use of the IoT. This is critical for U.S. competitiveness, particularly as other countries adopt policies to encourage IoT innovation within their borders.[19]

B.   Policymakers Should Promote a Skilled Workforce for the Digital Future

Educational systems in most countries, including the United States, are not keeping pace with the demands of a rapidly changing digital world. IoT will place a new premium on skills, innovation, and adaptability, and policymakers must understand how to adapt the education system to better align with technological advancements. Indeed, investment in human capital development will be a critical determinant of which nations lead in the IoT. The United States must continue to foster and educate a technologically savvy workforce, through investments in education and other policies that promote a skilled workforce.

C.   Policymakers Should Champion Innovation, Openness, and Technology Neutrality Internationally

Many countries are promoting IoT—establishing national blueprints with time-bound goals, investing in research and deployment, and launching public-private partnerships. At the same time, regional and intergovernmental organizations are staking out early roles on IoT policy and technology. Economies of scale mean that these international activities may impact IoT deployment and adoption. Policymakers should support American IoT innovation by ensuring that the U.S. stays ahead and globally champions policies that support IoT, such as open, consensus-based, and globally recognized standardization efforts, open markets, the seamless flow of information, and technology neutrality.

Countries like China, Korea, India, Germany, Brazil, and others are moving ahead on IoT. In May 2014, the Korean government published its plan for building the IoT with the aim of a hyper-connected, "digital revolution."[20] Some countries, like China and India, are providing financial incentives or subsidies for IoT. India's Smart City plan is part of a larger agenda of creating Industrial Corridors between India's big metropolitan cities and seeks to create seven new smart cities. Brazil, in turn, is encouraging IoT with favorable tax policies, and Germany has launched innovation clusters tied to IoT.

The U.S. government must remain vigilant, and guard against global efforts that might endanger the open, consensus-based, private sector-led system of standards development that fosters innovation. NTIA recognizes the importance of such a policy in the recently updated

---

[19] For example, Germany is working to remove barriers to testing autonomous vehicles on public roads, and the U.K. plans to test on public roads in 2017 and permit full operation in 2020. Michael Nienaber, "Germany Keen to Test Self-Driving Cars on the Road," Reuters, (Apr. 12, 2016), http://www.reuters.com/article/us-germany-autos-merkel-idUSKCN0X915A; "Costas Pitas, Britain to Test Driverless Cars on Motorways from Next Year," Reuters, (Mar. 12, 2016), http://uk.reuters.com/article/uk-britain-autos-driverless-idUKKCN0WE0HX.

[20] Ministry of Science, ICT, and Future Planning, Master Plan for Building the Internet of Things that Leads the Hyper-Connected, Digital Revolution (Aug. 2014).

Circular A-119.[21] The U.S. government also should remain vigilant against data privacy measures that distort competition. Forced localization, including requirements to use local servers and infrastructure to store data, is an immediate threat to the growth of IoT. NTIA and the U.S. government must step up efforts to avoid measures that require data localization, including advocating for strong, enforceable rules in trade agreements and countering unequal treatment for companies headquartered in the United States.

V.   CONCLUSION

IoT is already and will continue to impact the daily lives of all Americans. This connected technology is revolutionizing the health, manufacturing, transportation, and agricultural sectors to name a few. IoT is also becoming an economic game-changer which will inject billions of dollars into the U.S. economy. That is why it is so important for the United States to lead international in technology. In order for this to be achieved, Congress and the agencies that oversee IoT should avoid duplicative as well as overly-prescriptive and burdensome regulation that impede innovation. Technology, including IoT, is a force for good that should be fostered by smart regulatory frameworks that encourage investment, promote innovation, as well as connect and empower Americans from all walks of life.

---

[21] *See, supra,* n.18.

Mr. LATTA. Thank you very much for your testimony.

Ms. Richardson, you are recognized for 5 minutes.

STATEMENT OF MICHELLE RICHARDSON

Ms. RICHARDSON. Chairman Latta, Ranking Member Schakowsky, thank you for the opportunity to testify today on behalf of the Center for Democracy and Technology.

CDT is a nonprofit technology policy organization dedicated to protecting civil liberties and human rights in a digital world including privacy, free speech, and access to information.

We believe the Internet of Things has the power to enrich people's lives in ways both big and small. But we also recognize that the Internet of Things poses unique privacy and security challenges. Many of these devices collect information that is intensely personal yet ungoverned by U.S. policy and privacy law. It has also become common to hear of serious security breaches which have allowed hackers to use IoT devices to either steal information or participate as part of a botnet.

CDT's preference for technology policy is for private industry to voluntarily create and adopt standards. The government plays an important role in setting standards and incentivizing good behavior, especially in sectors where security failures had extreme consequences or in the consumer market when users don't have a fair shot at understanding or managing products.

Congress has the authority and the responsibility to determine whether the current government and private balance is the right one. We hope this bill will help collect information to assess that in two ways. First, we hope the SMART IoT Act will collect information to determine whether voluntary standards and privacy standards are not only being created whether they are being adopted by a critical mass of industry players. Voluntary standards are the default in the IoT space and billions of devices are up and operating on the internet, and more are coming. The foundational question we should be asking is whether this approach is working as a general matter.

Second, the study should tease out any overlap or gaps in government oversight of these IoT devices. Cross-agency coordination is crucial to sharing information and will help make sure that the government is not issuing conflicting guidance or requirements.

Now, we recommend the bill clearly state that nothing in it should be interpreted to discourage agencies from continuing work in critical areas like connected cars or health devices. Agencies like the FDA and NHTSA are driving standards for devices or systems that have literal life or death consequences and that work cannot wait.

While industry deserves an overarching government plan for IoT, IoT is already too large and too diverse to cabin in a single agency, and developing sector-specific expertise will ensure that government involvement is supported by the technical and policy knowledge needed to make the right decisions.

After you receive this report, we expect that you will find that one of the largest gaps in standards and oversight is in the consumer market. As Ms. Vachani mentions in the IoT report for Intel, most IoT devices and applications relate to industrial products,

smart cities, and the health industry. Many of these devices are subject to practical and regulatory limits already. For example, some of these devices are embedded in critical infrastructure, which is already regulated writ large, and some of these devices are really quite simple and do not collect personal information or offer computing power that makes them attractive hacking targets. Think of sensors that only measure water pressure or county the number of cars that pass through an intersection. The users of these sorts of devices also are often more sophisticated and the corporate versus corporate relationship can contractually ensure that IoT devices continue to work safely.

But the consumer ecosystem does not have many of these checks and balances. Consumers are stuck in a take it or leave it system and they will not have the option to leave it much longer, as connectivity is built into everything. Lay users just do not have the technical capacity to understand and control the current crop of IoT devices on the market. They also have few legal remedies when something does go wrong. If security fails, devices can be a gateway to stealing personal information or subject the owner to actual spying. Failures can harm a person or her property in the real world like smart locks that can remotely open front doors. And these devices can be taken over as part of a botnet that can send scam email or, in the case of the Mirai botnet, take down websites and internet access, more generally.

In other words, there's a lot at stake in the consumer market and the current system is just not working. We are hoping that this committee finds the report to be just the jumping off point for better oversight of consumer products and we look forward to working with you and your staff on this bill.

[The prepared statement of Ms. Richardson follows:]

cdt CENTER FOR
DEMOCRACY
& TECHNOLOGY

Testimony of
Michelle Richardson, Deputy Director
Center for Democracy and Technology, Freedom, Security, and Technology Project

before the
House Energy and Commerce Committee,
Subcommittee on Digital Commerce and Consumer Protection

Internet of Things Legislation
May 22, 2018

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We believe the Internet of Things (IoT) has the power to enrich people's lives. Connected devices can add convenience, efficiency, transparency, and control to simple, everyday activities from vacuuming one's house, to providing cutting edge advances in medicine, and everything in between.

CDT does, however, have continuing concerns about the security of IoT devices and the privacy of the information they collect and transmit. To that end, we regularly work with federal agencies like the National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration (NTIA) and the Federal Trade Commission

1

(FTC) to develop voluntary standards or best practices that will improve privacy and security.[1]
We additionally work with Congress on oversight activities and legislation.[2]

Summary

CDT has always recommended that the government take a soft touch in shaping
technology and has endorsed the use of voluntary standards, especially relating to
cybersecurity. We have also recognized that the government may have a legitimate role in
overseeing sectors that pose a unique threat to safety or products that are unreasonably
beyond accountability to consumers. The draft State of Modern Application, Research, and
Trends of IoT Act (SMART IoT Act)[3] begins to compile the information necessary to evaluate
whether these private sector and government efforts are sufficiently addressing the security of
the IoT ecosystem. It is a question that Congress has the authority and responsibility to ask.

To that end, we believe the lists of industry standard-setting efforts and government
oversight activities that would be created by this bill can help inform the Committee's oversight
and legislative plans. Our statement below recommends amendments to the SMART IoT Act to
ensure that the resulting report both returns meaningful information by which Congress can
evaluate the state of the field and that the study does not discourage agencies from continuing
with urgent cybersecurity efforts that are currently underway.

---

[1] See for example, CDT Comments to NTIA/NHTSA Connected Cars Workshop, July 31, 2017, at
https://cdt.org/files/2017/08/2017-0731-2-ConnectedCarComments.pdf, CDT Comments to NTIA on The
Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the
Internet of Things (IoT), Mar. 10, 2017, at
https://cdt.org/files/2017/03/CDT_NTIA_IoT_comments_Mar2017.pdf, CDT Comments to FTC Workshop
on IoT, June 1, 2013, at https://cdt.org/files/pdfs/CDT-Internet-of-Things-Comments.pdf.

[2] CDT Support for S. 1691, Cybersecurity Improvement Act, (115th Cong.), at www.warner.senate.gov,
Testimony of Justin Brookman before the Senate Judiciary Committee, The Connected World: Examining
the Internet of Things, Feb. 11, 2015, at https://cdt.org/insight/testimony-of-justin-brookman-before-
senate-commerce-on-internet-of-things/.
[3] Draft dated May 15, 2018, at https://docs.house.gov/meetings/IF/IF17/20180522/108341/BILLS-115pih-
TodirecttheSecretaryofCom.pdf.

The SMART IoT Act Should Address Whether the Private Sector is Implementing

Voluntary Standards and Whether They are Improving Security

Section 2(a)(1) directs the Secretary to survey the IoT industry and create a list of 1) the

sectors that develop or use IoT devices, 2) ways the IoT is developed and used, 3) public or

private partnerships that promote the adoption of IoT devices, and 4) industry-based bodies who

have or are developing standards for connected devices.

While this list will create an expansive primer of the IoT industry, the committee's

oversight and legislative function will benefit most from understanding the status of voluntary

standard setting efforts. The Committee may benefit from shifting the emphasis of this section

from creating a comprehensive list of all actors in the ecosystem to obtaining information about

whether existing standards have been implemented - even if that means scoping the sectors

that the report would cover.

It is important to note that NIST and NTIA have begun this process.[4] NISTIR 8200

(Draft), for example, reflects an interagency working group's effort to catalog different

international standards and whether they have been adopted. It does not purport to cover every

possible guideline relevant to IoT, but estimates that most of the reviewed sectors have

incomplete standards, and those that do exist have not been implemented. Exploring this deficit

in more detail will provide more actionable information than just a list of the governing

documents.

---

[4] NISTIR 8200 (DRAFT), Interagency Report on Status of International Cybersecurity Standardization for
the Internet of Things (IoT), at https://csrc.nist.gov/publications/detail/nistir/8200/draft, NTIA
Multistakeholder Process: IoT Security Upgradability and Patchability, draft list of standard setting
organizations at https://www.ntia.doc.gov/files/ntia/publications/handout-standardstargeted_0426.pdf.

We understand that some may chafe at the suggestion that the government should conduct such an evaluation. But the conclusion that government intervention is unnecessary or unwise is premised on industry adopting practices that deliver a sufficient level of security. And even if the review was to find a suboptimal adoption rate, it does not follow that direct government regulation would be the first or best response.

<u>Agency Work to Oversee Critical IoT Sectors and Create Neutral Standards and Guidance Must Continue While the Bill's Study is Conducted</u>

CDT also recommends that the bill clarify that the study for which it calls should not discourage existing agency IoT workstreams. Agencies are developing guidance now on IoT devices that pose risk of injury or even death in the case of a significant security failure. For example, guidance on connected cars or medical devices could prevent serious injury and should not be delayed.

This includes the work of NIST to develop guidance on managing IoT cybersecurity and privacy risks within federal information systems.[5] This effort to more explicitly map NIST's risk management framework and security and privacy controls on to government systems is critical. The US government has repeatedly acknowledged that cyber threats have become one of our country's most pressing national security concerns and designing government systems that can

---

[5] NIST, Considerations for Managing IoT Cybersecurity & Privacy Risk (Draft), at https://www.nist.gov/sites/default/files/documents/2018/04/13/iot_program_discussion_draft_april_2018.pdf.

better withstand attack or penetration is a priority of both the White House[6] and the Department of Homeland Security.[7]

In fact, NIST's privacy and security engineering guidance should be quickly embraced by federal agencies and the IT Modernization Board so that going forward, new government devices or services are created at the outset with state of the industry controls. While there may be debate over whether and how different companies should adopt NIST standards or guidance, it should be noncontroversial that the government follows its own advice on how to develop more secure systems.

<u>The Energy and Commerce Committee Should Use the Results of the Study to Advance Standards for Consumer Products that Aren't Overseen by Other Agencies</u>

As currently scoped, the SMART IoT Act will return information on an incredibly diverse range of devices and systems that are used by many different constituencies ranging from sophisticated corporations to everyday consumers. Coupled with the bill's review of federal jurisdiction, one would expect to find that consumer facing products like home devices or wearables to be in a sweet spot of under-regulation and this committee's jurisdiction. Congressional committees and federal agencies that regulate products that could cause acute physical or financial harm have added cybersecurity to the list of factors or components that

---

[6] EO 18,833 Enhancing the Effectiveness of Agency Chief Information Officers, May 15, 2018 at https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-effectiveness-agency-chief-information-officers/, American Technology Council, Report to the President on Federal IT Modernization, December 2017, at https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf, EO 13,800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11 2017, at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[7] Department of Homeland Security, Cybersecurity Strategy, May 15, 2018, at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

they oversee. Yet there are many everyday devices whose security failures are more likely to result in a breach of personal information or contribute to a botnet that spreads malware that are falling through the cracks.

Consumer products also suffer from unique security weaknesses. They may be operated by lay users who are not equipped to make informed choices about what products to buy or how to reduce security risks that the products pose. These products may have complicated supply chains with components created by companies outside of US jurisdiction or companies that are unconcerned about reputational harm that can result from serious security failures. Consumer IoT devices may also be abandoned by manufacturers before the end of their life cycle because there is little to no recourse for everyday consumers whose devices no longer receive necessary updates.

As CDT discusses in its recently published report *Strict Products Liability and the Internet of Things*,[8] consumers face a dearth of meaningful options; they often do not have access to digestible information to guide their purchasing decisions, products can include inherently exploitable designs, and consumers usually do not have legal recourse when things go wrong. It has created a particularly unaccountable slice of the IoT market that this Committee should pursue.

Conclusion

CDT thanks the Committee for the chance to speak about the SMART IoT Act. Recent years have seen a new depth and breadth to IoT security failures - cars that inexplicably

---

[8] Benjamin Dean, CDT, April 2018, at https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

accelerate, medical devices that over-administer medication, webcams that are hacked into botnet service--and we appreciate Congress' interest in studying the problem. We look forward to working with you further on oversight and legislative options for developing a more secure IoT.

Mr. LATTA. Well, thank you very much for your testimony.

Ms. Vachani, you are recognized for 5 minutes.

STATEMENT OF DIPTI VACHANI

Ms. VACHANI. Thank you.

Thank you, Mr. Chairman, Ranking Member Schakowsky, and members of the subcommittee.

I appreciate the opportunity to testify today on behalf of Intel Corporation and I commend you and Congressman Welch for your leadership on the SMART IoT Act.

First, I would like to turn to the vast benefits of the IoT and discuss real-life IoT use cases that are relevant to the committee's jurisdiction. Gartner predicts that IoT technology will be in 95 percent of electronics for new product design by 2020. The transformational, societal, and economic benefits that will flow from this broad deployment of IoT technology is what energizes Intel. And the SMART IoT Act is a welcome indication that this enthusiasm is matched by this subcommittee. The IoT is already transforming sectors like health care, smart cities, and transportation.

I would like to go over a few use cases. Smart health care—less than .01 percent of patient data is available beyond the bedside for health care teams to make clinical decisions. To solve this problem, Medical Informatics, Intel, and Dell partnered on an FDA-cleared IoT platform called Sickbay. Sickbay continuously captures patient data from the bedside medical devices and transforms it into actionable intelligence. This enables care teams to make better and fast decisions and predict patient deterioration before it occurs. In the last 4 1A½ years, Texas Children's Hospital used Sickbay to improve health care for 2.1 million patients.

Smart cities—92 percent of the world's population lacks access to clean air and leading to millions of deaths annually. To address this, Intel and Bosch developed IoT-powered pollution monitoring systems that provide intelligent data and enable real-time analysis. These IoT systems are used by governments to improve air quality in congested cities like Pune, India, by factory owners to track emissions and provide safety checks for all workers, by construction site managers to provide air quality warnings and improve efficiency, and by cities to provide residents with recommended times for exercising outdoors.

Use case number three, transportation—as the subcommittee is aware, the impact of autonomous vehicles will be life changing, particularly in our disabled community and aging population. The number of U.S. residents aged 78 and older will increase by 53.7 million by 2030, compared to just 30.9 million in 2014. Many of these residents live in communities with poor or no public transportation. AVs will offer vastly improved mobility benefits. Intel applauds the committee's leadership on AV.

Next, I would like to offer Intel's strong support for the SMART IoT Act and respectfully offer recommendations to enhance the legislation. Nations are racing to lead in this competitive IoT sector. It has been Intel's strong desire that the Federal Government be more proactive in ensuring U.S. IoT leadership in declaring the U.S. the IoT a national priority for the innovation in investment and competitiveness.

We applaud the subcommittee for its bipartisan work to set America on its leadership path by ensuring an IoT study and recommendations to promote IoT adoptions to grow our economy.

I was on the Hill last October to unveil a broadly supported industry report on IoT. Intel recommendations to the SMART IoT reflect this report. First, we urge the subcommittee to include a robust definition in IoT that is nonproprietary, neutral regarding technologies and applications, and contemplates both the consumer and the industrial IoT. In fact, industrial, smart city, and connected health will make up 70 percent of the use cases.

Second, we urge you to seek specific recommendations that would be highly impactful on laying the groundwork for the national IoT strategy. This includes recommendations on incentives for the Federal Government and agencies to adopt IoT technologies to advance their Federal mission including smart infrastructure solutions. How the Federal Government can best support global industry-led IoT standard efforts and avoid new regulations that duplicate existing industry standards and a criteria for the Federal Government to invest in IoT public-private partnerships and testbeds.

Thank you for the opportunity to share Intel's thoughts on the SMART IoT Act. We look forward to working with you to see this bipartisan bill enacted into law—that first step towards a national IoT strategy—and ensure U.S. leadership in this transformational sector.

[The prepared statement of Ms. Vachani follows:]

PREPARED STATEMENT FOR THE RECORD OF

INTEL CORPORATION

For the

UNITED STATES HOUSE ENERGY AND COMMERCE

SUBCOMMITTEE ON DIGITAL COMMERCE

AND CONSUMER PROTECTION

Hearing On

INTERNET OF THINGS LEGISLATION

MAY 22, 2018

Intel Corporation (Intel) respectfully submits this statement for the record in conjunction with the Energy and Commerce Committee Subcommittee on Digital Commerce and Consumer Protection hearing entitled, "Internet of Things Legislation."

Our statement focuses on the opportunity to unleash the enormous potential of the Internet of Things ("IoT") to positively impact the quality of life for Americans by enabling transformational economic and societal benefits across the consumer and industrial marketplace. The IoT already is enabling more efficient manufacturing, improved healthcare delivery, and new retail experiences, as well as increasingly smarter and more livable cities for American communities. By investing in this vast transformational potential of the IoT, pursuant to a clear national IoT strategy, U.S. policymakers can help ensure that the country's IoT technology evolves at the forefront of innovation, driving America's global competitiveness and growing our economy.

Witness: Dipti Vachani is Vice President of the Internet of Things Group and General Manager of the Platform Management and Customer Engineering organization at Intel Corporation. Her organization is responsible for delivering platform products that scale across IoT vertical segments, customer enablement, and optimizing products across the Internet of Things Group portfolio. Intel's IoT portfolio spans hardware, software, security and services across a wide range of market segments, including automotive and transportation, manufacturing, healthcare, smart video, retail, smart buildings, and smart cities. For more than 30 years, Intel has made significant investments, driven exciting innovations, and led activities across industries in order to foster standards and best practices, and supported what has evolved to become the IoT. At Intel, we like to say the IoT is an overnight transformation over thirty years in the making.

INTEL AND THE INTERNET OF THINGS

The Evolution of IoT at Intel

The evolution of IoT goes back more than 30 years at Intel, a leader in the space from the start. In 1972, Intel introduced the Intel 4004, the world's first commercially available microprocessor – an invention foundational to the "computer revolution." The late 1970s brought 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 utilizing real-time operating systems.

The early 2000s saw an unprecedented uptake in Internet usage as PC and mobile markets exploded. This "connectivity" trend wasn't limited to connecting people; embedded systems introduced in the 1990s were now 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, while and consumers enjoyed 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, ranging from the datacenter to cloud computing to wireless communications to M2M, formed the basis of what is now widely known as the IoT. And Intel has been a leader in this technology evolution from the start.

Moore's Law, named after Intel co-founder Gordon E. Moore, is the business model that drives the semiconductor industry. It states the number of transistors in an integrated circuit doubles approximately every two years. In essence, the marketplace experiences a doubling of computing capability at approximately the same price every other year. This explosion of networked devices also began to represent another "law" of scaling, known as 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. This law enables the Network Effect, whereby the value of a product or service is dependent on the number of users. Together, Moore's Law and Metcalfe's Law demonstrate how the power of intelligent, connected devices can unleash innovation, leading to the creation of platforms for new applications and services.

Defining the IoT

The IoT is here, and already is transforming the way we live and work. The IoT offers massive potential for society and business to build a more connected, productive, and engaging world. At its core, the IoT is: "Things" (devices) securely connected through a network to the cloud (datacenter), from which data can be shared and analyzed to create value (solving problems or enabling new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet; share and analyze the data generated by these things; and extract meaningful and actionable insights.

These opportunities are extensive and exciting, with the ability to transform entire industries and our lives for the better. The IoT encompasses two major segments: Consumer IoT and Industrial IoT. The "Consumer IoT," which garners much of the attention in this space, connects devices like smart thermostats, household appliances, wearables, and smart phones. The "Industrial IoT," which is going to be the dominant market for IoT use cases with the most

significant GDP impact, connects devices in industrial environments like factory equipment, retail systems, security cameras, medical devices, and digital signs.[1]

Intel expects the IoT evolution will include three major phases:

- **Phase 1 - Connect the Unconnected:** Because IoT capabilities were built from legacy embedded businesses, all of those embedded devices needed to be able to communicate, share data, and stream information to the back end (data access layer).

- **Phase 2 (today) - Intelligent Interconnected Things:** Today we are in the era where everything is connected and "smart." This is fueled by the advances in machine learning, speech recognition, and artificial intelligence.

- **Phase 3 - Software Defined Autonomous:** In the not so distant future, complex systems will function freely and be able to make important decisions in real-time, and devices will learn from their environment and utilize that learning to improve performance.

Securing the IoT

Security is foundational to the IoT. Intel's IoT hardware and software are designed from the beginning with security, with the goal of delivering trusted data with a tight integration of hardware- and software-based security that starts where data is most resilient to attack. To do this, we build security into the transistors in our chips. We also build security into the software used in the "things," as well as the way in which data is moved from these things or devices to the cloud. In total, we believe reliance upon a hardware- and software-layered approach to security helps achieve the best results and helps minimize and compartmentalize threats when problems do arise. We fully realize safety and security are essential for the promise of the IoT to be realized. Therefore, while the nature of threats continue to evolve in frequency and potency, so do our innovations.

And the market for IoT security is maturing and growing rapidly. We are seeing a significant increase in the amount of investment in security not only by Intel, but across the IoT landscape. From 2017 to 2022, the IoT security market is expected to grow from $6.62 billion to $29.02 billion, at a Compound Annual Growth Rate of over 34 percent.[2] Notably, we are seeing more companies investing in hardware-based security mechanisms, rather than just software-based technologies that are vulnerable to hackers.

---

[1] National IoT Strategy Dialogue Report (Oct. 2017), https://www.itic.org/dotAsset/bdce6de4-8a00-49c5-a7a9-4dfb95609a76.pdf (attached as Appendix 1).

[2] Internet of Things Security Market Worth $29.02 Billion by 2022, Markets and Markets, https://www.marketsandmarkets.com/PressReleases/iot-security.asp.

Developing IoT Standards

In order to accelerate market adoption of secure IoT solutions that are interoperable and scalable across a global IoT ecosystem, Intel and others have come together to drive a voluntary, global, industry-led, open set of standards that enable cost-effective IoT technology solutions. In addition to partnering with entities like NIST (on voluntary frameworks for cyber-physical systems, cybersecurity, and networking) and IEEE (to build standards specifications to meet IoT use cases developed by IoT consortia), we have come together to create global IoT standards consortia to collaboratively create global IoT standards and overcome the technology barriers to accelerate IoT adoption.

Examples of leading global IoT standards consortia include:

- Open Fog Consortium – 57 members – Driving Interoperability that seamlessly bridges the "cloud to things" continuum.

- The Open Group – 111 members – Developing standards-based, open, secure, interoperable process control architecture.

- OPC Foundation – 515 members – Interoperability standard for the secure and reliable exchange of data in the industrial automation space and other industries.

- AVNU Alliance – 67 members – Creating interoperable ecosystem servicing the precise timing and low latency requirements of diverse applications (automotive, consumer, audio/video, industrial) using open standards through certification.

- Open Connectivity Foundation & IoTivity – 340+ members – Ensuring secure interoperability by delivering a standard communications platform and open source implementation for devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem.

- 3rd Generation Partnership Project (3GPP) – 370+ members – Uniting multiple telecommunications standard development organizations and providing a stable environment to produce the Reports and Specifications that define cellular telecommunications network technologies such as 5G.

WHY CONGRESS SHOULD CARE: THE VAST SOCIETAL AND ECONOMIC IMPACT OF THE IOT

Why should policymakers care about investing in the IoT in America? By 2020, Gartner predicts that IoT technology will be in 95 percent of electronics for new product designs.[3] Therefore,

---

[3] Gartner's Top 10 Predictions for IT in 2018 and Beyond, Forbes (Oct. 2017), https://www.forbes.com/sites/louiscolumbus/2017/10/03/gartners-top-10-predictions-for-it-in-2018-and-beyond/#7a04a27f45bb.

the potential impact of IoT technology to address important societal and economic challenges in areas ranging from transportation, healthcare, smart cities, manufacturing, smart buildings, and industrial sectors is remarkable. It is critical that these IoT benefits are realized in this nation in a way that enables the U.S. to not only keep pace with, but stay at the forefront of, global innovation.

These transformational societal and economic benefits that will flow from the broad deployment of IoT technology is what energizes our team at Intel, and the SMART IOT Act is a welcome indication that this enthusiasm is matched by leaders in Congress. Indeed, the SMART IoT Act will create the foundational work for a national IoT strategy that prioritizes IoT growth in the U.S. and investment in technologies that can accelerate these benefits for America's communities and businesses.

Massive Economic and Societal Impact

The new markets and services generated by the IoT will add trillions of dollars to the global economy. Accenture estimates that the IoT could add $14.2 trillion to the worldwide economy by 2020.[4] Of this, $6 trillion will be spent on IoT solutions between 2015 and 2020, according to PwC.[5] And Gartner forecasts that the use of connected "things" will reach 20.4 billion globally by 2020.[6]

Countries are racing to lead in this highly competitive IoT race because they know that their communities and industries can be positively transformed by the IoT, as these technologies help solve societal challenges, while making businesses more effective and responsive, and adding new sources of revenue. The U.S. must position itself to lead in this transformational technology evolution. A national IoT study and recommendations to advance the IoT in the U.S. as set forth in the SMART IOT Act – lay the groundwork for a national IoT strategy – that will set the nation on the path to achieve this leadership goal.

Here are a just a handful of IoT use cases which Intel has deployed with our partners, demonstrating the positive impact that the IoT already is having on our lives and communities:

Use Case #1: Smart Healthcare (Texas Children's Hospital)

IoT applications in the healthcare sector are transforming and saving lives every day. For example, using IoT solutions, nearly 5 million patients' healthcare conditions were remotely monitored across the globe in 2015, representing a 51 percent increase from the previous year.

---

[4] 2017 Roundup of Internet of Things Forecasts, Forbes (Dec. 2017), https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#67cd37561480.

[5] *Id.*

[6] State of the Internet of Things, Verizon (2017), https://www.verizon.com/about/sites/default/files/Verizon-2017-State-of-the-Market-IoT-Report.pdf.

That number is expected to continue its upward trajectory, as remote healthcare services provide essential benefits to patients, while helping bring down associated health care costs.

Yet, currently, much of the data from patient monitoring devices is "siloed" and proprietary, and therefore underutilized. And with downstream systems not designed to manage or transform physiologic data, healthcare teams cannot effectively use data to optimize care delivery for individual patients or predict events. To tackle this challenge, new FDA-cleared IoT solution Sickbay – by Intel Solutions Alliance Member Medical Informatics Corporation, Intel and Dell – enables real-time, data driven medicine and patient-centered healthcare. The Sickbay IoT platform continuously captures patient data from any medical device or system and transforms that data into web-based clinical applications that make the data actionable. This actionable intelligence enables health care teams to make better and faster decisions and predict patient health deterioration before it occurs to save lives. Sickbay already is implemented at six healthcare institutions, including Texas Children's Hospital, which pioneered the technology that allows for viewing of real-time data from cardiac monitors and vents. Texas Children's Hospital used Sickbay to collect data on 302 beds over 4.5 years, which included 2.1 million patients.

Use Case #2: Smart Cities (Global)

The World Health Organization estimates that 92 percent of the world's population does not have access to clean air, and Bosch states reports that 3.2 million deaths occur annually due to air pollution.[7] This figure underscores a massive global societal and economic challenge. In fact, the World Bank Estimates that, in 2013, air pollution was responsible for $225 billion in lost productivity. Through air quality monitoring systems, such as those being deployed through Intel's IoT partnership with Bosch, we are addressing this challenge. The Intel & Bosch-developed IoT-powered pollution monitor systems provide intelligent data and enable real-time analysis of ambient air pollution. This Intel-powered IoT solution is being utilized by governments and traffic authorities across the globe to improve air quality in the most congested urban areas like Pune, India (a sprawling city of over 3.115 million in 94.15 mi^2); by factory owners to track emissions and provide safety checks for workers; by worksite managers at construction sites to provide early warning signals and improve efficiency and work conditions; and in communities around the world to provide residents with air quality warnings and recommended times for fitness activities to lower health incidents from air pollution.

Use Case #3: Smart Transportation (San Diego, CA)

Traffic congestion presents a number of problems for communities. IoT traffic management can alleviate the time spent in traffic jams and reduce drive times, thus improving the quality of life for drivers and passengers, as well as reducing the economic losses which arise from this wasted time in traffic. IoT traffic management solutions also can reduce air pollution by smoothing traffic flow, reducing idling times, and improving traffic monitoring activities.

---

[7] Bosch (visited May 18, 2018), http://www.boschclimo.com/.

For example, Intel, together with Current by GE and AT&T, are providing IoT technology built into street lights. These unique intelligent nodes are embedded with multiple sensors that can be used to collect data related to air quality, weather, vibration, noise and lighting. The City of San Diego has the largest urban sensor project in the world. This technology has allowed for the city to reduce energy consumption and improve the quality of life for its residents. IoT initiatives like this can help to further address the problems of sound levels and better respond to weather conditions like rain, flooding, snow, ice, and other situations. IoT can even be used to deal with other challenges such as mapping health patterns and addressing crime trends.

Moreover, autonomous vehicles will have an enormous impact in increasing mobility for our aging and disabled populations. The number of U.S. residents age 70 and older is projected to increase to 53.7 million in 2030, compared to 30.9 million just 4 years ago. Approximately 16 million people over the age of 65 live in communities where public transportation is poor or non-existent. With the advent of autonomous vehicles, disabled and physically-challenged individuals will have the opportunity to move and travel more easily than ever before.

Use Case #4: Smart Buildings (New York City)

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, Rudin Management, a large, commercial real estate company in New York City, deployed Intel's Smart Building IoT solution to better manage its utility consumption. This IoT deployment saved Rudin $1.8 million in just one building over three years, and reduced electric consumption by nine percent. And this is only one building. Consider the potential IoT impact for the over 5 million commercial buildings and industrial facilities in America, with a current combined annual energy cost of more than $202 billion.

U.S. GLOBAL LEADERSHIP

It has been Intel's strong recommendation to see the U.S. government overtly adopt a more proactive national strategy when it comes to harnessing the economic and societal benefits of the IoT. In order to truly take a global leadership role, the U.S. must first declare the IoT a national priority for innovation, investment and competitiveness. We strongly applaud the Committee for its bipartisan effort to set America on the path to make this vision a reality. The Committee's work in drafting the SMART IOT Act creates the opportunity for the U.S. to identify the state of the IoT in America, and begin to do the foundational work to develop a meaningful and comprehensive national IoT strategy based on the Department of Commerce's recommendations.

Therefore, Intel supports the concept of requiring a national study to survey the IoT industry, as well as agency activity and resources. We also strongly support the requirement that the IoT report is submitted to Congress with recommendations on how best to promote adoption of the IoT to grow the U.S. economy. For policymakers who are responsible for ensuring that the

IoT ecosystem reaches its full economic and societal potential in America, interaction between key agencies and the Congress is both important and appropriate.

Intel Recommendations for the SMART IOT Act

IoT Terminology and Definition. We respectfully encourage the Committee to:

- Use the term "IoT device" in place of "internet-connected device." The latter is a very broad term, including devices that are not IoT.

- Include a robust definition of the IoT that is aligned with the definition in the recently unveiled National IoT Strategy Dialogue Report (attached as Appendix 1),[8] which was widely supported by the Information Technology Industry Council, the U.S. Chamber of Commerce, and the Semiconductor Industry Association. This definition is non-proprietary and is neutral with respect to technologies, applications and deployments. It also broadly defines the IoT to include consumer and industrial IOT sectors, to reflect the reality of the IoT marketplace. Contrary to popular belief, the IoT is not primarily about consumer applications. Rather, industrial, smart city, and connected health applications will account for 70 percent of the IoT market.[9] We recommend that the legislation contemplate both consumer and industrial IoT applications by adopting the non-proprietary and neutral definition in the National IoT Strategy Dialogue Report.

Additional Guidance to the Department of Commerce. We see opportunity in this legislation to identify aspects where Department of Commerce recommendations would be highly impactful in laying the groundwork for a meaningful national IoT strategy. To this end, we encourage the Committee to seek specific recommendations from the Department including:

- How to prioritize the development of a national IoT strategy that will grow the American economy and drive global competitiveness;

- Incentives for federal departments and agencies to adopt interoperable, scalable and secure (multi-layer hardware and software) IoT technologies for data-driven solutions to advance their federal missions, including smart infrastructure solutions;

- How to ensure the federal government does not adopt new regulations that are duplicative to existing or already underway industry-led-standards, best practices and regulations that cover IoT technologies;
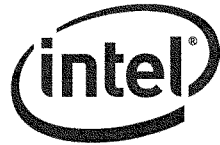
---

[8] National IoT Strategy Dialogue Report (Oct. 2017), https://www.itic.org/dotAsset/bdce6de4-8a00-49c5-a7a9-4dfb95609a76.pdf (attached as Appendix 1).

[9] 2017 Roundup of Internet of Things Forecasts, Forbes (Dec. 2017), https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#67cd37561480

- How federal departments and agencies can best support and promote leading global, industry-led IoT standards efforts, and engage as a key participant where appropriate;

- How to coordinate across federal departments and agencies to prevent inconsistent, duplicative, or unnecessary new IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors;

- Criteria for the federal government to invest in IoT public-private partnerships, research and testbeds, such as those being driven by leading global industry consortia; and

- How the federal government can best advocate internationally for foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders necessary for a thriving global IoT marketplace, and prevent harmful policies against U.S. companies in the application of laws and regulations impacting IoT technologies.

Thank you for the opportunity to share Intel's thoughts on the IoT marketplace and the SMART IOT Act. We look forward to working with the Committee to see this bipartisan legislation enacted into law as a productive first step toward a National IoT Strategy. With these efforts, Congress will set America on the path to realize the vast economic and societal benefits of the IoT, and ensure U.S. leadership in this globally competitive marketplace that will define the 21st century.

APPENDIX 1 – National IoT Strategy Dialogue Report (Oct. 2017)

National IOT Strategy Dialogue

intel

SAMSUNG

ITI

SIA SEMICONDUCTOR INDUSTRY ASSOCIATION

_TEC
U.S. Chamber of Commerce
Technology Engagement Center

INTRODUCTION

The U.S. technology sector is the envy of the world. Following the advent of the Internet, the United States has led every major technological revolution in no small part due to the innovative policy approach of the federal government. We are at the next major technological turning point as we witness the widespread proliferation of the Internet of Things (IoT). To lead the world and fully realize the potential of all the economic, societal, and innovative benefits the IoT will deliver, the United States must have a national strategy to promote investment, development, and widespread utilization of the IoT. To help guide this goal, we are pleased to unveil this report, which has been developed through collaboration and discussion among leading industry, academic, governmental, and other stakeholders in the IoT. With the adoption of these strategic policy recommendations, we believe the United States will be the unquestioned leader in the IoT.

I want to thank all those who participated in the National IoT Strategy Dialogue (NISD) discussions and development of this report. In particular, I want to thank NISD Co-Chair Marjorie Dickman and Intel Corporation for the leadership and strategic vision in the development of this report. As Intel's global expert on IoT policy, her sage guidance and time commitment were invaluable. Further, I want to thank Samsung and NISD Co-Chair John Godfrey for providing the platform to launch this important initiative, together with Intel and the Information Technology Industry Council (ITI), at their 2016 IoT event in Washington. Lastly, numerous companies and associations participated in NISD and contributed to the ideas in this report. In particular, we want to thank the Semiconductor Industry Association (SIA) and the U.S. Chamber of Commerce Technology Engagement Center for their partnership in unveiling this report.

Fully harnessing the transformative nature of the IoT is a tremendous opportunity for the United States. We encourage the U.S. government to act on this report's strategic policy recommendations – starting with adopting a National IoT Strategy.

Sincerely,

Dean C. Garfield
President and CEO
Information Technology Industry Council

In June 2016, Intel, Samsung, and the Informational Technology Industry Council (ITI) launched the National IoT Strategy Dialogue (NISD), an initiative to convene industry partners and organizations to collaboratively develop strategic recommendations for U.S. policymakers on the Internet of Things (IoT). The launch of this IoT initiative answered the call of a chorus of technology leaders seeking a forum to proactively coordinate and drive industry's trusted advisor role in helping the United States to fully realize the vast benefits of IoT for economic and societal good.

NISD has grown significantly since its launch a year ago. In addition to broad industry engagement, we have reached out extensively to a wide range of government stakeholders engaged in IoT policy for their input. Government participants in this collaborative effort include the Department of Commerce (DOC), Department of Health and Human Services (HHS), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), White House Office of Science and Technology Policy (OSTP), National Telecommunications Information Administration (NTIA), and Food and Drug Administration (FDA). Industry and other external participants include ITI, the Semiconductor Industry Association (SIA), CTIA the Wireless Association, Advanced Medical Technology Association (AdvaMed), World Bank, and Information Technology and Innovation Foundation (ITIF). It became clear from these discussions among government and industry experts that a National IoT Strategy is a much-needed first step to drive U.S. IoT leadership, and some of the most important elements of a national strategy will require affirmative action from Congress and the administration.

This breadth of industry participation is indicative of the fact that the expansive technology sector is critical to the IoT's success. IoT solutions consist of hardware, software, security, and services across a wide range of market segments, including automotive and transportation, energy, healthcare, smart manufacturing, retail, smart buildings, and smart homes. Not since the advent of the Internet has there been such a technological shift that presents an opportunity for U.S. consumers, businesses, government, and the economy at large.

Among its many benefits, the IoT will enable increased safety in our communities, offer consumers significant improvements in their daily lives, make government and business more efficient and productive, and create new job opportunities by stimulating economic growth in all sectors of the economy, similar to prior technology evolutions that have been critical to America's leadership and long-term growth. The IoT will fundamentally transform our lives for the better, bringing us a society and environment where everything is smarter and more connected, from smart cities and smart cars, to intelligent wind farms, precision agriculture, and next generation health care.

What is at stake at this moment is whether the United States will be able to win the global race to test, develop, and deploy these beneficial technologies. With these vast economic and societal benefits in mind, NISD was launched with the goal of collaboratively working with policymakers to develop a much needed strategic roadmap to position the United States as the global IoT leader now and for decades to come. To this end, we are focusing on the advancement of pro-innovation public policies, market incentives, and regulatory frameworks, as well as government use and adoption of IoT to showcase America's global leadership.

Our strategic recommendations seek to lay the foundation to drive scalable U.S. IoT infrastructure investment; facilitate interoperability; foster security; promote voluntary, industry-led, global consensus-based IoT standards and best practices; and leverage public-private partnerships (PPPs).

Why is a strategic plan necessary for America? Because U.S. IoT success and leadership will not occur without appropriate planning nor will it happen in a policy vacuum. The positive social and economic potential of the IoT is massive and capturing the lead in this area appeals to every developed nation. It is estimated that IoT will produce a total economic impact of $3.9 to $11 trillion per year globally by 2025, equivalent to 11 percent of the world economy.[1] This vast economic impact already has led many other countries to promote the adoption of IoT across multiple sectors; the United States must not just follow suit, but rather proactively chart a strategic course to sustainably surpass these countries if we want a competitive advantage in the future of manufacturing, transportation, agriculture, energy, finance, healthcare, and other key sectors of high gross domestic product (GDP) impact that are being rapidly transformed by the IoT.

This report provides strategic recommendations for the U.S. government to work with industry to drive American IoT leadership. We are eager to support Congress and the Trump Administration in taking these steps to create a policy and regulatory environment that will attract unparalleled private sector investment and innovation in the IoT, thereby modernizing the nation's infrastructure, improving American manufacturing, and growing GDP. We thank all of the individuals, organizations, and government entities that collaborated with us throughout this process and look forward to collaboratively advancing these strategic recommendations and achieving U.S. IoT leadership.

Sincerely,

Marjorie Dickman, Co-Chair, National IoT Strategy Dialogue
Global Director & Associate General Counsel, Internet of Things & Automated Driving Policy
Intel Corporation

John Godfrey, Co-Chair, National IoT Strategy Dialogue
Senior Vice President, Public Policy, Office of U.S. Public Affairs (USPA)
Samsung Electronics America

Vince Jesaitis
Vice President, Government Affairs
Information Technology Industry Council

EXECUTIVE SUMMARY

This report makes the following strategic recommendations for Congress and the Trump Administration to establish America as the leader in the Internet of Things (IoT):

1. Prerequisite – IoT Definition: Congress and the administration should adopt this broad-based IoT definition as an initial level-set for any future policymaking regarding the IoT:

- The IoT consists of "things" (devices) connected through a network to the cloud (datacenter) from which data can be shared and analyzed to create value (solve problems or enable new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet, share and analyze the data generated by these "things," and extract meaningful insights; those insights create new opportunities, help solve problems, and implement solutions in the physical world.

2. Prioritization of a National IoT Strategy: Congress should promptly enact, and the president sign into law, the bipartisan *Developing Innovation and Growing the Internet of Things (DIGIT) Act* (S. 88/H.R. 686) to make a National IoT Strategy a priority and position America to lead the global IoT future.

3. Ensuring Consistent IoT Standards and Rules at the Federal Level and Internationally:

- Federal agencies should not adopt new regulations where existing standards, best practices, and regulations exist, or are underway that would include IoT technology, or where the costs of new regulations have not been offset by the reform of previous regulations.

- Based upon existing authority, or the grant of new authority where necessary, the White House and Congress should direct federal agencies to support and promote leading global, industry-led IoT standards efforts, and the U.S. government should engage as a key participant where appropriate.

- The Department of Commerce (DOC) should coordinate across federal agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors.

- The federal government should advocate internationally for our foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders, and prevent discrimination against U.S. companies in the application of laws and regulations.

**4. Commitment to Security of the IoT:**

- Congress and the administration should incentivize multi-layered protection of IoT solutions using hardware- and software-integrated security. Any legislation providing funding for IoT solutions or smart technology should include this in the eligibility criteria for federal funding.

- Congress and the administration should encourage flexible federal policies that promote ongoing innovation and best practices for hardware- and software-integrated security.

- It must be a federal priority to continue to build upon and invest in cybersecurity multi-stakeholder efforts, leveraging the best of our public and private sector experts and resources to constantly improve the security of the IoT and other technologies. The federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats, and develop best practices for IoT security and data privacy. DOC and its agencies, such as the National Institute of Standards and Technology (NIST) and the National Telecommunications Information Administration (NTIA), as well as the Department of Homeland Security (DHS), are the appropriate entities to continue to lead such efforts.

- Congress should direct the Federal Trade Commission (FTC), Small Business Administration (SBA), and Federal Communications Commission (FCC) – with input from industry – to develop complementary cybersecurity hygiene education and awareness outreach initiatives for consumers and small businesses. These initiatives should focus on security tools and best practices for Internet-connected things to help better secure devices and wireless networks from intrusions.

- Congress should direct federal departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for federal assets based on voluntary, industry-led, consensus-based, global standards. Secure solutions, with multi-layered hardware- and software-level capabilities, must be a government procurement requirement for both IoT and non-IoT solutions to protect the nation.

5. Prioritization of Smart Infrastructure Solutions: Congress and the administration should make it a federal priority in infrastructure legislation to both fund and incentivize smart, data-driven IoT solutions that advance federal agency missions.

- To modernize the nation's transportation system, infrastructure legislation should fund and incentivize smart IoT solutions on a technology-neutral basis in a way that boosts market-driven investment, including investing in technologies that will accelerate the safe deployment of automated vehicles.

- Infrastructure legislation should promote the deployment of key foundational technologies like 5G mobile broadband networks that will serve as the core architecture for the IoT. Congress should also direct the NTIA and FCC to allocate commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies to address the breadth of IoT use cases today and into the future.

- Infrastructure legislation should fund and incentivize smart government building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of both civilian and military buildings.

6. Invest in IoT Public-Private Partnerships (PPPs), Research, and Testbeds: To ensure U.S. global IoT leadership, the federal government should invest in IoT PPPs, research, and testbeds, such as those being driven by leading global industry consortia like the Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), and OpenFog Consortium (OpenFog).
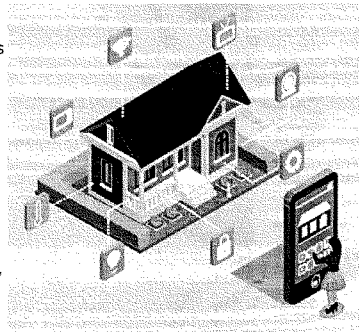
STRATEGIC RECOMMENDATIONS ████████████████████

The following is a set of strategic recommendations for Congress and the Trump Administration to set America on a path of U.S. Internet of Things (IoT) leadership for decades to come. We provide a blueprint of specific and timely steps to enable the development and deployment of the IoT in the United States, thus, enabling the nation's global competitiveness across numerous key market sectors. Some of our recommendations require direct investment of resources, while others entail a commitment by the United States to lead the continuous IoT technology evolution that is transforming the global economy. In the aggregate, these strategic recommendations will deliver national alignment and efficiency across an innovation ecosystem to ensure that America realizes the vast economic and societal benefits of the IoT.
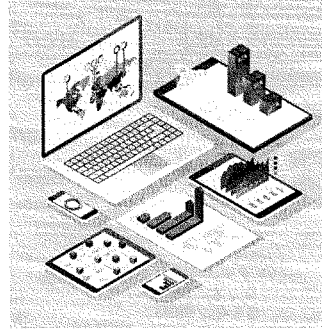
1. Prerequisite: IoT Definition

The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud. Commonly referred to as the IoT, this new reality is being driven by the convergence of increasingly connected devices, compute and data economics, and the proliferation and acceleration of cloud and big data analytics. This shift in technology is 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.[2]

In recent years, we have seen many proprietary definitions of the IoT that tend to focus on specific business interests. However, it is important to have an agreed upon definition of the IoT that comprehends the fullest breadth of IoT applications. At its simplest, the IoT consists of "things" (devices) connected through a network to the cloud (datacenter) from which data can be shared and analyzed to create value (solve problems or enable new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet, share and analyze the data generated by these "things," and extract meaningful insights; those insights create new opportunities, help solve problems, and implement solutions in the physical world.

The IoT encompasses two major segments: Consumer IoT and Industrial IoT. The Consumer IoT connects devices like smart TVs, household appliances, gaming consoles, wearables, and smart phones. The Industrial IoT connects devices in industrial environments like factory equipment, retail systems, medical devices, and digital signs.

Recommendation: Congress and the administration should adopt this broad-based IoT definition as an initial level-set for any future policymaking regarding the IoT.

2. Prioritization of a National IoT Strategy

It is imperative that the U.S. federal government declares the IoT a strategic national priority in 2017. This effort must begin with a simple, yet profound, declaration of a national IoT vision.

The federal government must declare IoT investment, innovation, and competitiveness a U.S. priority and institute an expedient process and timeline for the development of a National IoT Strategy in conjunction with the private sector. This strategy must be built with a strong commitment to scalability, interoperability, and security, as well as with sufficient flexibility to address the inevitable reality that IoT technologies and their applications will continually evolve.

Success in developing and implementing a meaningful national IoT strategy will require leadership at the highest levels of the U.S. government in partnership with the private sector. This strong leadership is needed to take the strategic steps necessary to facilitate policies that accelerate development and deployment of the IoT in the United States, and ensure that U.S. government, businesses, and consumers can leverage the wide range of benefits the IoT offers. Without a clear strategic vision for enabling and adopting IoT solutions across many key market sectors, the United States is certain to fall behind as other countries reap the vast economic and societal benefits of these technologies, along with the benefits that accrue from creating and owning the expertise behind the IoT. However, by implementing a clear strategic plan with a series of impactful steps, the United States can and will lead the world – and drive GDP – for decades to come.

The bipartisan *Developing Innovation and Growing the Internet of Things (DIGIT) Act*, (S. 88/H.R. 686) sets forth a collaborative process for developing a National IoT Strategy. Specifically, it would require the federal government, under the leadership of the Secretary of Commerce, to convene a working group of federal entities that would consult with private sector stakeholders to provide recommendations to Congress on how to plan for and encourage the proliferation of the IoT in the United States. This joint government-industry process would produce a unified vision and critical first step toward development and implementation of America's National IoT Strategy.

<u>Recommendation:</u> **Congress should promptly enact, and the president sign into law, the bipartisan DIGIT Act to make a National IoT Strategy a priority and to position America to lead the global IoT future.**

3. Ensuring Consistent IoT Standards and Rules at the Federal Level and Internationally

As emphasized in the Department of Commerce's (DOC) IoT green paper,[4] voluntary, consensus-based, global standards developed through open participation efforts will drive interoperability, scale, and IoT investment. Depending upon existing authorities, the White House and Congress should work to direct federal agencies to support and promote such global, industry-led IoT standards efforts – many of which have been underway for years.

The U.S. government should support industry in continuing to lead IoT standards development and engage as a key participant where appropriate. Government should avoid adopting new regulations where existing standards, industry voluntary practices, and regulations exist, or are underway, that would otherwise encompass IoT technology. Moreover, consistent with the intent of Executive Orders 13771 and 13777,[5] federal agencies should not adopt new regulations where the costs have not been offset by the reform of previous regulations.

Recommendation: **Federal agencies should not adopt new regulations where existing standards, best practices, and regulations exist, or are underway that would include IoT technology, or where the costs of new regulations have not been offset by the reform of previous regulations.**

Some leading examples of global standards efforts with broad private sector membership include the Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), OpenFog Consortium (OpenFog), and GSMA's initiative on IoT device self-certification:[6]

- **IIC:** Launched in March 2014, the IIC is a global, member-supported organization that promotes the accelerated growth of the Industrial IoT by coordinating ecosystem initiatives to securely connect, control, and integrate assets and systems of assets with people, processes, and data using common architectures, interoperability, and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.[7]

- **OCF:** Launched in February 2016 to bring together the competing Open Internet Consortium and AllSeen Alliance, the OCF is defining connectivity requirements to improve interoperability between the billions of devices making up the IoT. OCF will deliver a specification, an open source implementation, and a certification program ensuring interoperability regardless of manufacturer, form factor, operating system, service provider, or physical transport technology.[8]

- **OpenFog:** Launched in November 2015, Open Fog is driving industry and academic leadership in fog computing architecture, testbed development, and a variety of interoperability and composability deliverables that seamlessly leverage cloud and edge architectures to enable end-to-end IoT scenarios.[9]
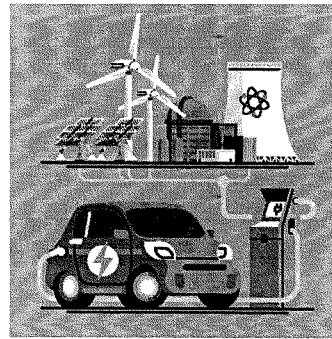
- **GSMA:** The embedded SIM certification initiative,[10] launched in November 2010, will provide a mechanism for the remote provisioning and management of machine to machine connections in a more efficient and secure manner through the use of tested embedded subscriber identity modules.

Industry-led, global standards efforts with respect to security (see pg. 14), interoperability, scalability, and other key tenets will accelerate IoT adoption, drive competition, and enable cost-effective introduction of new technologies in a scalable way. Government adoption of IoT solutions should follow and adopt industry-led standards, thereby, ensuring that government-deployed solutions will benefit from the scope and scale of the broader IoT and not be relegated to a proprietary or isolated silo.

<u>Recommendation:</u> **Based upon existing authority, or the grant of new authority where necessary, the White House and Congress should direct federal agencies to support and promote leading global, industry-led IoT standards efforts, and the U.S. government should engage as a key participant where appropriate.**

In addition to ensuring that each U.S. federal agency supports the international, industry-led standards development process for the IoT within its own sector, government must ensure coordination across these agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations. Indeed, one of the greatest benefits of the IoT is its power to aggregate data intelligence from devices and systems from diverse sources, crossing traditional industry boundaries. For example, to improve traffic congestion, real-time data and rich insights about transportation patterns can be gleaned from automobiles, street lights, and traffic sensors along roadways. Similarly, to improve public health, data can come from wearables, connected medical devices, environmental sensors, doctors' offices, and even restaurants. The interconnection of the data and devices across these boundaries is essential for IoT innovation and growth.
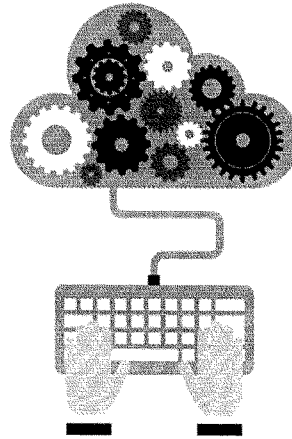
These changes in traditional industry boundaries can blur historical regulatory distinctions, and there is a significant risk that fragmented regulatory approaches across the government could prevent these and other IoT benefits from being realized. If federal regulatory agencies implement different, incompatible technical standards, or impose different, inflexible security or privacy obligations, the consequences will include the fragmentation of the IoT, barriers to scale, and lost opportunities for the United States. For this reason, coordination across government agencies is essential to prevent a patchwork of inconsistent policies which could disrupt the IoT's transformative potential.

As discussed above, agencies should avoid imposing new regulations where existing standards, voluntary industry standards and best practices, or government regulations already address the devices, services, or sectors that make up the IoT. Federal agencies should continue to partner with the private sector on multi-stakeholder efforts and global industry standards organizations (as discussed below) rather than defaulting to the imposition of new government regulations. Furthermore, where regulations are deemed necessary based on facts and market failure (not hypotheticals), agencies should adopt consistent, flexible approaches. DOC should lead this effort with respect to the horizontal, industry-crossing aspects of the IoT instead of each agency developing its own unique and possibly inconsistent guidelines or regulations.

Recommendation: DOC should coordinate across federal agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors.

But ensuring consistency in federal agency policies is not sufficient; the U.S. government must also strongly encourage our foreign counterparts to participate in and support global, industry-led IoT standardization activities. Many of these Standards-Setting Organizations (SSOs) have formed technical study groups to ascertain whether, and to what extent, additional standards development may be necessary to advance the IoT. These SSOs attract experts and participation from across the globe, as well as across various industry sectors that will be impacted by and benefit from the IoT.

It is critical to the success of the IoT that the U.S. government advocate internationally for other governments to support these SSOs' multi-stakeholder processes and participate when appropriate. When other countries insist on pursuing non-SSO processes the U.S. government should strongly encourage them to allow full industry participation and to look to existing or pending global standards before undertaking any activity that may be duplicative of, or conflict with, global, industry-led IoT standards. We also strongly encourage the U.S. government to include in its international advocacy a common definition of the IoT (see pg. 8) and a statement of policy that will accelerate development and adoption of IoT technologies (consistent with the recommendations in this report).

For example, as the Department of Homeland Security (DHS) concluded in its Strategic Principles for Securing the Internet of Things report, "IoT is part of a global ecosystem, and other countries and international organizations are beginning to evaluate many of the[] same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules. As DHS becomes increasingly focused on IoT efforts, we must engage with our international partners and the private sector to support the development of international standards and ensure they align with our commitment to fostering innovation and promoting security."[11]

Furthermore, in today's globally connected world, international commerce cannot function without data freely flowing across borders. The free movement of data allows U.S. companies of all sizes and in all industries to bring new innovations to global markets – driving investment, growth, and job creation in America. Cross-border data flows particularly enable small- and medium-sized enterprises (SMEs) to compete in the global economy, which is essential to maximizing the benefits of the IoT. Unfortunately, some governments around the world are considering, or are already imposing, digital trade barriers. American companies have the most to lose if these barriers are not addressed.
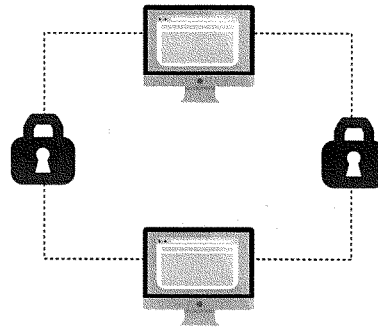
Therefore, in order to support the growth of the IoT and the continued competitiveness of the American economy, the federal government should aggressively protect cross-border data flows through trade agreements and other enforceable mechanisms with trading partners. Specifically, these agreements must include binding provisions protecting cross-border data flows and preventing data localization requirements, which mandate U.S. companies to store, process, or handle their data within the local country's borders. They also must include provisions on transparency, predictability, and nondiscrimination in the application of laws and regulations, on trade in goods and services, and on protection of intellectual property. The U.S. government should leverage these commitments to respond to unfavorable trade policies that could undermine existing rights and obligations of U.S. companies, and which would discourage U.S. investment and threaten scalability of the IoT.

Recommendation: The federal government should advocate internationally for our foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders, and prevent discrimination against U.S. companies in the application of laws and regulations.

4. Commitment to Security of the IoT

A strong commitment to the vast benefits of the IoT must be accompanied by an equally strong commitment to ensuring the security of the IoT ecosystem. As advocates of the expansive benefits of the IoT, we are equally convinced that an appropriate federal policy framework prioritizing joint industry-government, multi-stakeholder initiatives for IoT security is a foundational component of our nation's IoT success. Federal policies must promote security for IoT solutions from end-to-end (device-to-network-to-cloud), and include both legacy systems and new deployments.

With billions of connected devices generating more than 44 zettabytes of data by 2020,[12] security of this data and the networks and systems they transit will be critical to enable scale of IoT deployments. That is why we emphasize the importance of having security designed into the IoT systems from the outset. Secure systems, including all connected things that generate the data, and send the data through the communications network to the cloud and back, are critical to enabling trusted data exchange and scale, thereby unlocking the full potential of the IoT.

Numerous government-industry collaborative efforts have considered how to address the question of IoT security, and they have come to similar key conclusions. There is general agreement on five important fronts:
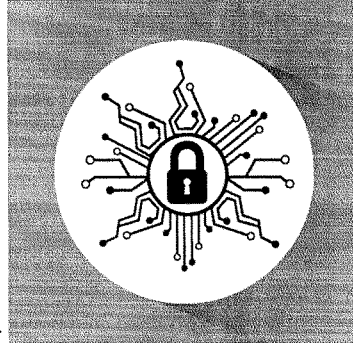
- Multi-layered protection using hardware- and software-integrated security at the outset that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment is critical;

- Federal policies must be sufficiently flexible for industry to innovate and address the ever-changing threat landscape;

- Government-convened, multi-stakeholder processes – bringing together security experts across government, industry, and academia – have a proven track record of success and should be continually honed and replicated;

- As new technologies develop and threat landscapes evolve, ongoing and evolving small business and consumer education on how to appropriately secure connected devices is critical; and

- Improved federal procurement requirements for multi-layered hardware- and software-integrated cybersecurity solutions must be a priority.

Integration of Security at the Outset: Industry agrees on the importance of integrating security into the hardware and the software components of IoT solutions from the beginning of the design process – from the smallest microcontroller (MCU) at the edge of the network to the most advanced server central processing unit (CPU) in the data center, and all gateways and devices in between. Specifically, multi-layered protection using hardware- and software-integrated security that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment is critical.

These hardware- and software-level security capabilities will create redundancies, which prevent intrusions and enable robust, secure, trusted end-to-end IoT solutions. Industry appreciates that we must deliver and evoke consumer trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

Recommendation: Congress and the administration should incentivize multi-layered protection of IoT solutions using hardware- and software-integrated security. Any legislation providing funding for IoT solutions or smart technology should include this in the eligibility criteria for federal funding.

Flexibility of Federal Policies: There is a vast array of technologies that are, and will be, deployed in the global marketplace and the IoT will be one subset in that expanse of marketplace technologies. Accordingly, it is critical that security is viewed in a comprehensive manner rather than forcing one subset of the ever-changing technology landscape in a regulatory silo targeted at IoT alone. Indeed, while security is critical for IoT technologies – as it is for all current and future technologies – IoT-specific security legislation or regulation is not the answer.

Security is a continuous process of risk management that is an ongoing and evolving challenge for all technologies, including the IoT. Thus, it is imperative for government to tread carefully in its policy response to any cyberattack. There is no single "silver bullet" in risk management and mitigation. Reflexive or prescriptive legislative or regulatory solutions are not the right mechanism to address complex hardware and software engineering challenges. Nor are technology mandates prescribing a specific security solution, which will become quickly outdated as technology advances. For this reason there is broad agreement that in order to be effective, federal policies must focus on best-known methods and be sufficiently flexible to address new vulnerabilities in the constantly evolving threat landscape, whether with respect to the IoT or other technologies.

These policies must focus on the desired outcome (multi-layered hardware and software security) rather than attempting to specify the technologies or techniques that must be used. Therefore, in order to best enable secure solutions, government must avoid technology mandates that require a specific technology solution as they will quickly become obsolete and can have the potential (and unintended consequence) of increasing susceptibility to new cyberattacks.

Recommendation: Congress and the administration should encourage flexible federal policies that promote ongoing innovation and best practices for hardware- and software-integrated security.

Multi-stakeholder Processes: The interests of the government, consumers, and industry are aligned in the shared desire to minimize vulnerabilities and create safe devices, networks, products, and services that are as secure as possible. Consequently, the most productive and impactful activities designed to enhance cybersecurity take place through voluntary consultation and close collaboration with the private sector. We strongly encourage that this approach continue.

For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework was published in February 2014 following a collaborative, multi-stakeholder process involving industry, academia, and government agencies. According to NIST, "[t]he original goal was to develop a voluntary framework to help organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid, but the framework has been widely adopted by many types of organizations across the country and around the world."[13] NIST, in collaboration with industry, academia, and other government agencies continues to update the framework on an ongoing basis. In January 2017, NIST issued a draft update to the Cybersecurity Framework, providing new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity.[14]

In addition, in mid-2014, NIST established the Cyber-Physical Systems Public Working Group (CPS PWG).[16] Cyber-physical systems (CPS) are smart systems that include engineered interacting (interconnected) networks of physical and computational components.[17] The CPS PWG brought together a wide range of public, private, and academic experts from the United States and around the globe in an open public forum to help define and shape key characteristics of CPS, with the objective of better managing development and implementation within and across multiple smart application domains including smart manufacturing, transportation, energy, and healthcare.[18] The CPS PWG established five expert subgroups to deep dive on important CPS issues including cybersecurity, privacy, data interoperability, vocabulary and reference architecture, timing and synchronization, and use cases. After two years of intense collaboration, the CPS PWG completed the CPS Framework Release 1.0 in May 2016 which documented the work of the five subgroups. [19] As the Framework states, "CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT."[20] This is an ongoing activity. After public review and finalization of the Framework, the applicability of this approach will be assessed in selected CPS domains leading to a planned future road mapping activity to both improve the CPS Framework and develop understanding and action plans to support its use in multiple CPS domains.[21]
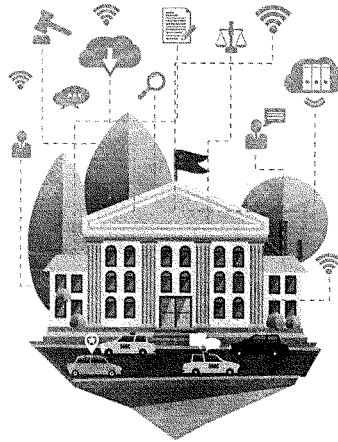
Similarly, the multi-stakeholder efforts undertaken by the DOC and convened by the National Telecommunications Information Administration (NTIA) should be utilized to a greater and ongoing extent in addressing complex security issues. The current NTIA Cybersecurity Vulnerabilities multi-stakeholder process, as well as the current NTIA IoT Security Upgradability and Patching multi-stakeholder process, provide examples of public-private collaboration to address pressing security needs while maintaining the necessary flexibility that rigid regulatory approaches would prevent. NTIA's Cybersecurity Vulnerabilities multi-stakeholder process, which launched in September 2015, is a "collaboration between security researchers and software and system developers and owners to address security vulnerability disclosure."[22] In December 2016 stakeholder participants released a set of initial findings, recommendations, and resources, and NTIA continues to work with stakeholders on further developments and outreach.[23]

Similarly, the NTIA-convened IoT Security and Upgradability and Patching multi-stakeholder process launched in October 2016 to help with the recognized need for a secure lifecycle approach to IoT devices, focused on developing a broad, shared definition around security upgradability for Consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers.

These voluntary, broad-based efforts exemplify a proven track record of success in improving security innovation and protection through multi-stakeholder efforts and public-private collaboration. Other examples include DHS' Strategic Principles for Securing the IoT, released in November 2016 after consultation with industry stakeholders. The DHS paper sets forth non-binding principles for mitigating IoT security risks for those who "develop, manufacture, implement, or use network connected devices"[24] and notes that, while there is "no one-size-fits-all solution for mitigating IoT security risks across the diversity of IoT devices[,]" "widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security posture of IoT."[25] Moreover, the technology industry also leads and contributes to other significant cybersecurity public-private partnerships with the federal government, including information sharing, analysis, and emergency response with government and industry peers such as the Department of Defense's (DoD) Defense Industrial Base Cybersecurity Information Sharing Program (cybersecurity information sharing and incident reporting); the Information Technology Information Sharing and Analysis Center (sharing of cybersecurity threats and insights); and DHS' Sector Coordinating Councils (coordination of critical infrastructure security and resilience).
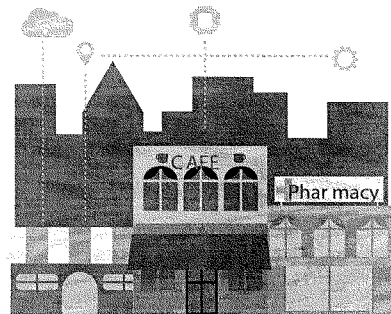
We applaud and encourage the federal government to continue its leadership as a convener and thought leader in this regard. As DHS – the nation's expert agency responsible for safeguarding the American people and our homeland's critical infrastructure – states in its Strategic Principles: "As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector ... The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security."[26] Industry is in broad agreement that we must continue to leverage America's private sector, academic, and other third party experts to collaboratively address cybersecurity of the IoT and other technologies, and further invest in these important and forward-thinking multi-stakeholder and public-private efforts currently underway. Policymakers should seek to reinforce this collaborative environment to encourage innovative, private-public cooperation on these issues, rather than top-down regulations that may duplicate ongoing work or become quickly outdated by the evolving threat landscape.

Recommendation: **It must be a federal priority to continue to build upon and invest in cybersecurity multi-stakeholder efforts, leveraging the best of our public and private sector experts and resources to constantly improve the security of the IoT and other technologies. The federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats, and develop best practices for IoT security and data privacy. DOC and its agencies such as NIST and NTIA, as well as DHS, are the appropriate entities to continue to lead such efforts.**

Consumer and Small Business Education: Consumer education and awareness of threats and how consumers can protect themselves must be a critical part of the nation's cybersecurity plan. The October 2016 Distributed Denial of Service (DDoS) attack on Dyn (a cloud-based Internet performance management company) – which targeted many now-connected legacy devices – highlights the importance of consumer cybersecurity education. In this regard, we encourage innovative efforts like the Federal Trade Commission (FTC) Home Inspector Challenge announced in January, where the agency is challenging the public to create an innovative tool that will help protect consumers from security vulnerabilities in software of home devices connected to the IoT with a focus on addressing risks created by legacy devices and of out-of-date software.[27] Similarly, we support efforts like the FTC's Start with Security guidance to help small business secure the IoT devices they deploy on their networks. [28]

There are other steps that should be taken as well. For example, the Small Business Administration (SBA) has established programs to educate small- and medium-sized business (SMBs) owners about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans.[29] Congress can reinforce these and other existing programs by providing more resources for agencies to educate SMBs on risk management and promote the use of processes and procedures to protect information systems against cybersecurity threats. As a result, SMBs would not only implement better cybersecurity practices, but also contribute to more secure supply chains for large businesses and the federal government.

Moreover, as new technologies develop and threat landscapes evolve, ongoing and evolving consumer education on how to appropriately secure Internet-connected personal devices like smart phones, baby monitors, and cameras, as well as home wireless networks, becomes even more important. To this end, there is broad agreement that the appropriate expert federal agencies like the FTC and Federal Communications Commission (FCC) should educate consumers on cybersecurity tools on an ongoing basis and encourage the use of cybersecurity best practices that incentivize good cyber hygiene.

Recommendation: Congress should direct the FTC, SBA, and FCC – with input from industry – to develop complementary cybersecurity hygiene education and awareness outreach initiatives for consumers and small businesses. These initiatives should focus on security tools and best practices for Internet-connected things to help better secure devices and wireless networks from intrusions.

Federal Procurement: A 2015 Veracode study compared civilian federal agencies to the private sector and found that federal agencies rank last in fixing security problems and even fail to comply with existing security requirements 76 percent of the time.[30] In today's threat environment, this should be unacceptable. The federal government must address this problem, largely involving legacy systems, both promptly and comprehensively in order to protect federal assets. We encourage Congress and the administration to immediately require federal departments and agencies to comply with existing security requirements, at the very minimum, and deploy multi-layered hardware- and software-integrated cybersecurity solutions to protect legacy and new assets.

In addition, the federal government should upgrade its IT systems. Secure, interoperable (non-proprietary), and scalable IoT solutions can vastly improve the federal government's efficiency and productivity, helping to meet department and agency missions in a more timely manner and saving significant taxpayer dollars. Moreover, upgrading to hardened end-to-end (device to cloud) IoT solutions will protect storage, device identification and authentication, software authentication, and enable a trusted execution environment that will be far more secure than legacy systems that can be rife with vulnerabilities. We must prioritize federal procurement requirements for such multi-layered protection using hardware- and software-integrated security. Doing so would help secure not only federal assets, but also drive awareness and deployment for contractors and other stakeholders that interface with the federal government.

Recommendation: Congress should direct federal departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for federal assets, based on voluntary, industry-led, consensus-based, global standards. Secure solutions, with multi-layered hardware- and software-level capabilities, must be a government procurement requirement for both IoT and non-IoT solutions in order to protect the nation.

## 5. Prioritization of Smart Infrastructure Solutions

As U.S. policymakers consider how best to address America's infrastructure, we appreciate the challenge facing Congress and the administration in efficiently allocating limited federal taxpayer dollars and attracting private sector investment. We recognize the importance of federal and state physical infrastructure spending such as building new highways and repairing roads and bridges. These expenditures are necessary, and importantly, create immediate job growth in construction and related sectors that is positive for American families. Moreover, physical infrastructure spending, when enhanced by the capabilities of IoT solutions, will not only increase jobs in the short-term but also drive economic growth in the medium- and long-term. Thus, we stand at a fortuitous moment in America's history when physical and digital capabilities can be harnessed simultaneously to generate maximum returns on public investments.

For this reason, we urge Congress and the administration to also prioritize smart, data-driven infrastructure solutions to drive U.S. leadership and economic growth over the medium- and long-term. Building IoT solutions into our infrastructure will create thousands of new construction jobs in the short-term — while also saving significant taxpayer dollars, helping solve longstanding societal challenges, and boosting America's economy over the long-term. In fact, "studies find that investments in IT-enabled infrastructure can have 60 percent greater productivity impacts than investments in roads alone" because "making physical infrastructure smart will enable ... network effects, enabling smart vehicles, smart logistics, and other related improvements."[31] These network effects are critical to driving medium- and long-term growth because they "unlock new economic opportunities, create jobs, and improve people's quality of life"[32] long after short-term job growth and construction ends.

Therefore, as America's policymakers draft legislation to improve and modernize the nation's infrastructure, we encourage Congress and the administration to make significant investments in deploying 21st century, data-driven solutions in both new and existing infrastructure – whether building from the ground up or repairing older assets. We support a mix of federally-funded projects and tax incentives, as well as PPPs, to accelerate these smart infrastructure investments in the United States. These smart IoT solutions can significantly increase infrastructure safety, efficiency, and reliability by improving real-time decision-making and management of infrastructure assets, enabling predictive maintenance, lowering long-term infrastructure costs, and increasing infrastructure life-span. To this end, legislation must have a clear and articulate goal of transforming traditional infrastructure into smart, 21st century infrastructure to enable increased connectivity, security, compute capabilities, and data-centric decision-making. Legislation also must promote the advancement of associated policies needed to accomplish this objective, or else this much needed infrastructure transition will lag.[33]
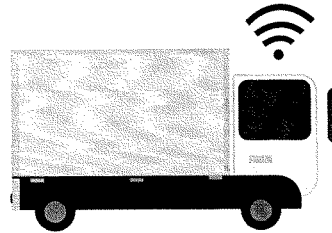
Moreover, consistent with prior recommendations in this report, infrastructure legislation should require these smart IoT solutions to meet the following criteria: end-to-end solutions that enable data-driven decisions utilizing hardware, analytics software, non-proprietary networks, sensors, gateways, and servers; multi-layered protection using hardware- and software-integrated security from the outset that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment; solutions based on industry-led, global, consensus-based standards and not government mandates; and interoperable, scalable, secure platforms and technologies.
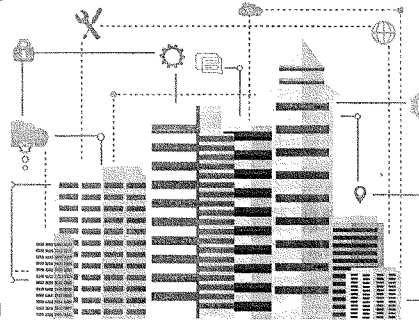
Specifically, we recommend deploying data-driven IoT infrastructure solutions to address federal agency missions, as well as to future proof the nation's transportation system, electric grid modernization and reliability, water management facilities, government buildings, public safety broadband networks, and critical infrastructure.

Federal Agencies: The infrastructure package is an excellent opportunity to leverage the benefits that government can achieve as a user of data-driven, IoT solutions – with the goal of making the U.S. government the IoT showcase for the world. Just as the IoT will transform the private sector through innovation and efficiency, so too can the IoT help government agencies achieve their own missions more effectively and at lower cost. Additionally, government reliance upon IoT as an early adopter, including new public-private collaborative uses of IoT solutions, also will help stimulate and accelerate private sector IoT investment in the America.

Recommendation: **Congress and the administration should make it a federal priority in infrastructure legislation to both fund and incentivize smart, data-driven IoT solutions that advance federal agency missions.**

Transportation and Automated Vehicles: We encourage investment in smart infrastructure to improve and modernize the nation's transportation system and accelerate the safe deployment of automated vehicles. Indeed, transportation is one of the most promising sectors for the IoT. The International Data Corporation (IDC) has projected that global revenue from the transportation sector will reach $325 billion by 2018. By converting vast amounts of data into meaningful and actionable intelligence, IoT infrastructure solutions will help solve transportation safety, efficiency, and mobility challenges.

For example, "[s]mart traffic lights that sense ebbs and flows and adjust accordingly can reduce travel time in cities by 25 percent."[34] IoT infrastructure solutions also will "help maximize the use of existing transportation infrastructure and even improve its maintenance and repair,"[35] as well as modernizing any new infrastructure – making the nation's roads and highways "smarter, more efficient, safer, and more durable."[36] Moreover, "[a]pplying a digital layer allows for real-time insight into infrastructure performance, which can generate substantial economic and public safety benefits through preventative maintenance and early warning systems." [37]

We must also invest in the modern infrastructure necessary to accelerate the safe deployment of automated vehicles. This means investing in consistent digital signage, smart sensors, and clear road markings if America is to attract significant investment and lead the world in this competitive sector. "Shoddy infrastructure has become a roadblock to the development of self-driving cars, vexing engineers and adding time and cost. Poor markings and uneven signage on the 3 million miles of paved roads in the United States are forcing automakers to develop more sophisticated sensors and maps to compensate."[38] To address this barrier to automated vehicle deployment, Congress should direct the Department of Transportation (DOT) to allocate a substantial portion of its innovation funding[39] to IoT transportation solutions and automated vehicle infrastructure projects, including the integration of next generation mobile broadband networks to improve transportation safety. Congress also should ensure that these upgrades and implementations are immediately eligible for funding under the existing highway transportation authorization.[40] They also should tie a share of federal surface transportation funding to states' actual improvements in transportation system performance using IoT solutions which would promote an incentive to invest in cost-efficient digital infrastructure.[41]

Moreover, as stated in the Conference Report accompanying the *Fixing America's Surface Transportation (FAST) Act*, Congress should "ensure[] that [DOT] programs are implemented and Intelligent Transportation Systems (ITS) are deployed in a technology neutral manner. The FAST Act promotes technology neutral policies that accelerate vehicle and transportation safety research, development, and deployment by promoting innovation and competitive market-based outcomes, while using federal funds efficiently and leveraging private sector investment across the automotive, transportation, and technology sectors."[42] Clearly, Congress recognized that when government seeks to directly or indirectly choose technologies, however well-intended, these decisions lag behind and often thwart marketplace innovation.
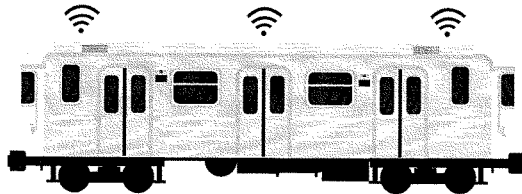
Accordingly, Congress should direct DOT to award innovation funding on a technology-neutral basis to help enable and accelerate industry-driven innovation and investment, maximizing the return on U.S. taxpayer dollars.

Industry, not government, should be driving innovation in the transportation and automotive sectors; government should not be using taxpayer dollars to create a market for government-favored technologies or to choose technology winners and losers. Public policies that encourage innovation, competition, and market-driven investment are critical to enable self-driving vehicles to reach their full potential in the United States, realize maximum economic and safety benefits for Americans, and become widely available across the nation in a timely and globally competitive manner.

Recommendation: To modernize the nation's transportation system, infrastructure legislation should fund and incentivize smart IoT solutions on a technology-neutral basis in a way that boosts market-driven investment, including investing in technologies that will accelerate the safe deployment of automated vehicles.

5G and Next Generation Mobile Broadband Networks: When considering infrastructure legislation, it also will be important how the federal government addresses key foundational technologies that will serve as the core architecture for the IoT. Most significantly, in the next few years, 5G – the rapidly emerging successor to today's 4G – will bring communications and computing together in a fundamental shift for the United States and the world in a way that is essential to lay the foundation for our IoT future. 5G will be defined by a heterogeneous network of wireless communications technologies – including Wi-Fi, LTE-Advanced, mmWave, and others – combined with a virtualized core and intelligent edge services. It will not only increase capacity, but it will also enable even the smallest devices to perform heavy computational tasks by bringing the cloud to the edge of the network. According to Intel's Communication and Devices Group, moving to 5G will transform our daily lives. For instance, "autonomous vehicles will be able to make decisions in milliseconds to keep drivers and vehicles safe. Drones will aid in disaster recovery efforts, providing real-time data for emergency responders. Smart cities will monitor air and water quality through millions of sensors, giving them insights needed to provide a better quality of life."[43] And this is just the start.

Evidence of the global race to secure 5G leadership is everywhere and should be viewed by U.S. policymakers as both a wakeup call, as well as a challenge to move intelligently and swiftly.[44] For example, 5G deployments are already underway in Russia for the 2018 FIFA World Cup,[45] in South Korea for the 2018 Winter Olympics,[46] and in Japan for the 2020 Summer Olympics.[47]
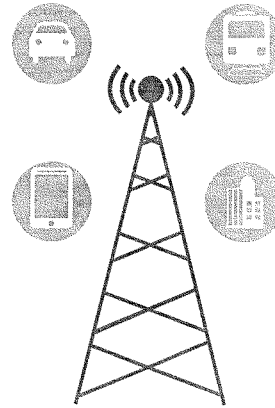
China started large-scale testing of 5G networks this year, and China Mobile aims to continue with deployment testing in 2018 with commercial operations starting in 2020.[48] Meanwhile, Europe has a 5G Action Plan to boost the deployment of 5G infrastructure and services across the Digital Single Market with the objective of making 5G a reality for all citizens and businesses by 2020.[49] Clearly, the global 5G race is on.

Moreover, 5G offers the benefits of extensive global private industry investment, coupled with strong consumer demand, similar to its previous cellular iterations of 3G and 4G. These benefits propel technologies to the forefront and enable them to evolve at the pace of innovation – which will be key to the long-term evolution and scale of the IoT. Accordingly, for the United States to lead the IoT future, it is vital that the nation's infrastructure strategy recognizes this worldwide marketplace direction and enormous industry investment in 5G – and that America invests wisely in this innovative communications and computing technology platform.
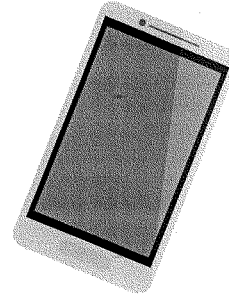
In addition, with respect to spectrum and mobile broadband networks more generally, today's communication infrastructure – comprised of a diverse portfolio of licensed and unlicensed spectrum – will be challenged by the rapid and extensive proliferation of IoT devices and services. Connecting tens of billions of things to each other, to people, and to the cloud will place unprecedented demands on today's wireless networks and generate many zettabytes of data.[50] Our nation's infrastructure must continue to evolve to meet these rapidly increasing capacity and computational demands across the growing breadth of IoT applications, many unimaginable today. And these applications will vary widely in their requirements and the diverse set of wireless communications technologies used. Thus, rather than designate specific IoT bands or technical standards, the federal government should continue to foster private investment and public-private collaboration.

Government can accomplish this objective by allocating commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies. This will enable service providers and innovators to make use of the most appropriate communications spectrum and technologies for their IoT applications. For example, emergency medical services may require guaranteed low-latency, high-reliability communication between an instrument carried by a first responder and a doctor at a central location, while a distributed network of moisture sensors for drought-tolerant farming may need very low power consumption (for long battery life) with less dependence on instantaneous delivery. The federal government also should identify additional government-used spectrum for clearing and/or sharing with commercial wireless services and streamline the regulatory environment for deployment of communications network infrastructure.

Recommendation: Infrastructure legislation should promote the deployment of key foundational technologies like 5G mobile broadband networks that will serve as the core architecture for the IoT, and Congress should direct NTIA and the FCC allocate commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies to address the breadth of IoT use cases today and into the future.

Smart Buildings: As part of an infrastructure package, we encourage Congress to allocate funding to smart building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of civilian and military buildings. Such IoT solutions should connect, secure, and manage actionable data from existing and new building systems (e.g., heating, ventilation, and air conditioning (HVAC), electricity, lighting, water, natural gas) to achieve the following operational efficiency goals: enable remote monitoring of building assets; enable predictive maintenance of building assets; improve building comfort for increased productivity; improve real-time decision-making regarding building assets; and lower long-term building and asset costs for increased sustainability and life-span. For example, water mains embedded with Internet-connected sensors can detect and transmit information on leaks. Smart traffic lights that adjust with ebbs and flows of traffic can reduce travel time in cities by 25 percent.[51]

The criteria for smart building solutions (similar to those discussed above) should be the following: secure, scalable, interoperable IoT platforms; end-to-end solutions that utilize hardware, analytics software, non-proprietary networks, sensors, gateways, and servers to enable data-driven decisions; multi-layered protection of building assets using hardware- and software-integrated security that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment. These smart building IoT solutions should be a priority consideration in the design, renovation, or retrofit of all civilian and military construction projects including any new or existing office space, housing, commercial, and other facilities. These projects should serve as scalable models for implementation of data-driven IoT solutions to enable asset optimization in civilian and military buildings across the nation.

Including smart building goals in federal facilities will save the government considerable public resources and federal taxpayer dollars. At a time when the federal government is looking for ways to save money, embrace smart technology, and spur innovation, electing to embrace IoT technologies across its vast government and military facility base would be a wise use of limited resources. Supporting the use of large scale smart building testbeds would also encourage local and state governments to follow the federal government's lead in adopting cutting-edge and resource-saving IoT technologies.

Recommendation: Infrastructure legislation should fund and incentivize smart government building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of both civilian and military buildings.

6. Invest in IoT PPPs, Research, and Testbeds

Government and industry collaboration can be one of our nation's best assets to accelerate the deployment of the IoT in America in a globally competitive manner. Using public and private resources to facilitate IoT testbeds and research – while leveraging existing industry standards and investments – will accelerate the nation's future toward IoT leadership. Viable PPPs will entail logical investments for both government and industry, as well as ensure scalability of IoT innovations and sustainability of deployments over the long term.

Therefore, as part of our National IoT Strategy, U.S. policymakers should encourage the deployment of globally competitive and rapidly scalable PPPs, research initiatives, and testbeds. These joint public-private efforts should span the breadth of IoT sectors from automotive and energy to agriculture and manufacturing – like those being launched by global industry-led efforts such as IIC. Through this collaborative innovation, we can transform America's landscape to smart cities and communities that use IoT solutions to improve traffic management, public safety, air quality, energy reliability, and water management. Such IoT PPPs, research, and testbeds are critical to accelerate the nation's IoT infrastructure and, accordingly, essential to U.S. leadership in this transformative technology evolution.

Specifically, we recommend that U.S. policymakers encourage and participate in IoT PPPs, research, and testbeds including, but not limited to, these areas:

- **Trusted Data and Secure Compute:** Industry has long touted security as a foundation for the IoT. Indeed, powerful computing with integrated hardware and software level security is critical to the IoT's success. For example, securing connected vehicles and the supporting infrastructure is foundational to keeping passengers safe and secure, and requires an end-to-end system (vehicle-to-network-to-cloud) approach. Not only must every connected vehicle be safeguarded against cyber threats, but every device connected to the vehicle and the personal information available via these devices must also be kept private as it moves between the vehicle, connected devices, connected infrastructure, and the cloud.
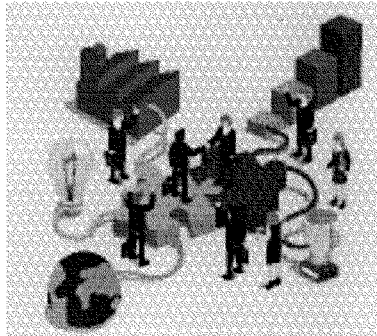
- **Artificial Intelligence (AI):** AI and IoT are interdependent; IoT has enabled the collection and use of data across multiple devices, paving the way for the development of AI technologies that rely on and learn from this data. We have already begun to see how AI can benefit people and society in fields as diverse as healthcare, transportation, the environment, criminal justice, and economic inclusion. For example, autonomous vehicles, the product of the IoT and AI, collect and analyze data that will enhance human safety, increase productivity, and yield economic gains for society. Intel has been investing in companies with expertise in functional safety and doing foundational research in Deep Learning for many years, and is working to ensure that our products, from the thing (vehicle) to the network to the cloud, are capable of bringing the intelligence needed for the vehicle to sense and adapt.

- **Open, Standards-Based Platforms:** Global standards, such as those being driven by IIC, OCF, OpenFog, and the Open Fabrics Alliance[52] can accelerate adoption, drive competition, and enable the cost-effective introduction of new technologies. For example, the tech industry is partnering with the auto industry to research and define standards to accelerate autonomous driving deployments and create economies of scale that enable rapid marketplace adoption. This will enable industry leaders to contribute core technology including platform software, machine learning algorithms, and data collected from vehicle sensors to enable a safe and secure driving experience. And, as noted above, the IoT industry is contributing broadly to the global consortia efforts of organizations like IIC, OCF, and OpenFog in researching and developing interoperable standards for IoT platforms.

Industry is leading IoT PPPs, research, and testbed efforts, often in concert with academia and government partners, around globe. The U.S. government should participate in these activities. However, government should refrain from directing the activity in order to allow industry to innovate, develop, and adopt flexible solutions. Specifically, government participants should not use their participation in PPPs, research, or testbed activities to steer industry innovation toward a government-favored technology, or as an indirect "carrot" mechanism to pick technology winners and losers.

Recommendation: To ensure U.S. global IoT leadership, the federal government should invest in IoT PPPs, research, and testbeds, such as those being driven by leading global industry consortia like IIC, OCF, and OpenFog.

71

[1] McKinsey and Company, Unlocking the Potential of the Internet of Things, June 2015 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.
[2] Intel Corporation, Internet of Things Policy Framework, at 1, http://www.intel.com/content/dam/www/public-/us/en/documents/corporate-information/policy-iot-framework.pdf.
[3] Developing Innovation and Growing the Internet of Things (DIGIT) Act, S. 88, 115th Cong. (2016), https://www.congress.gov/bill/115th-congress/senate-bill/88.
[4] U.S. Dept. of Commerce, Fostering the Advancement of the Internet of Things, at 44-48 (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.
[5] Executive Order 13771, Presidential Executive Order on Reducing Regulation and Controlling Regulatory Costs (Jan. 30, 2017); Executive Order 13777, Enforcing the Regulatory Reform Agenda (Feb. 24, 2017).
[6] See Comments of Information Technology Industry Council, Docket No. 160331306-6306-01, at 12 (June 2, 2016); Comments of the U.S. Chamber of Commerce Technology Engagement Center, Docket No. 170105023-7023-01, at 5 (Mar. 13, 2017); Comments of the Consumer Technology Association, Docket No. 170105023-7023-01, at 13-14 (Mar. 13, 2017).
[7] For more information, see Industrial Internet Consortium http://www.iiconsortium.org/about-us.htm (last visited May 23, 2017).
[8] For more information, see Open Connectivity Foundation, https://openconnectivity.org/about (last visited May 23, 2017).
[9] For more information, see OpenFog Consortium, https://www.openfogconsortium.org/about-us/ (last visited May 23, 2017).
[10] GSMA, Connected Living: The importance of Embedded SIM certification to scale the Internet of Things, http://www.gsma.com/connectedliving/wp-content/uploads/2017/02/1038-FM-GSMA-Test-Cert-eBook-V6.pdf (February 2017).
[11] U.S. Dept. of Homeland Security, Strategic Principles for Securing the Internet of Things, at 14 (Nov. 15, 2016) ("DHS IoT Cybersecurity Principles"), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf..
[12] EMC2/IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things: Executive Summary (Apr. 2014), http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.
[13] U.S. Dept. of Commerce NIST, NIST Releases Update to Cybersecurity Framework (updated Jan. 31, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework..
[14] See U.S. Dept. of Commerce NIST, Framework for Improving Critical Infrastructure Cybersecurity: Draft Version 1.1 (Jan. 10, 2017), https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.
[15] Id. at 14.
[16] U.S. Dept. of Commerce NIST, CPS PWG, https://pages.nist.gov/cpspwg/ (last visited May 19, 2017).
[17] U.S. Dept. of Commerce NIST, CPS PWG, Framework for Cyber-Physical Systems Release 1.0, at xiii (May 2016), https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf
[18] Id.
[19] Id.
[20] Id. at 1.
[21] Id. at xiii.
[22] U.S. Dept. of Commerce NTIA, Multistakeholder Process: Cybersecurity Vulnerabilities, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (last visited May 19, 2017).
[23] Id.
[24] DHS IoT Cybersecurity Principles at 4.
[25] Id. at 5.
[25] Id. at 4.
[27] Press Release, FTC, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security..

[28] FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov-/tips-advice/business-center/guidance/start-security-guide-business.

[29] See, e.g., SBA Learning Center, Cybersecurity for Small Businesses, https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses (last visited May 23, 2017).

[30] Arik Hesseldahl, Why the Federal Government Sucks at Cyber Security, Recode (June 23, 2015), https://www.recode.net/2015/6/23/11563798/why-the-federal-government-sucks-at-cybersecurity..

[31] Peter L. Singer, Investing in "Innovation Infrastructure" to Restore U.S. Growth, ITIF at 9 (Jan. 2017) ("ITIF Innovation Infrastructure"), http://www2.itif.org/2017-innovation-infrastructure.pdf?_ga=2.236106113.1093994383.-1495464199-421905161.1495464159..

[32] Robert D. Atkinson et al., A Policymaker's Guide to Smart Infrastructure, ITIF at 1 (May 2016) ("ITIF Policymaker's Guide"), http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf. See also Innovation Infrastructure at 9 (stating, "[S]mart infrastructure is likely to have bigger productivity payoffs than … pouring more concrete or laying pipe.").

[33] ITIF Policymaker's Guide at 26.

[34] ITIF Innovation Infrastructure at 9.

[35] ITIF Policymaker's Guide at 12.

[36] Id. at 10.

[37] Id. at 21.

[38] Alexandria Sage, Where's the lane? Self-driving cars confused by shabby U.S. roadways, Reuters (Mar. 31, 2016), http://www.reuters.com/article/us-autos-autonomous-infrastructure-insig-idUSKCN0WX131.

[39] The FAST Act authorized $305 billion over fiscal years 2016 through 2020 for highway, highway and motor vehicle safety, public transportation, motor carrier safety, hazardous materials safety, rail, and research, technology and statistics programs. See The Fixing America's Surface Transportation Act, H.R.22, 114th Cong., Title VI – Innovation (2015), https://www.fhwa.dot.gov/fastact/.

[40] See, e.g., ITIF Policymaker's Guide at 25.

[41] See, e.g., id.

[42] H.R. Rep. No. 114-357, at 507 (2015), http://www.gpo.gov/fdsys/pkg/CRPT-114hrpt357/pdf/CRPT-114hrpt357.pdf.

[43] Aicha Evans, Intel Accelerates the Future with World's First Global 5G Modem, Intel (Jan. 4, 2017), https://newsroom.intel.com/editorials/intel-accelerates-the-future-with-first-global-5g-modem/.

[44] Testimony of Doug Davis, Intel, U.S. Senate Cmte. on Commerce, Science and Transportation, Subcmte. on Surface Transportation et al., at 5 (June 28, 2016), available at https://www.commerce.senate.gov/public/_cache/files/46c728ce-377e-4060-9cac-55db2230ddf8/17D163EB418271C1D3BBC8D572D589EE.doug-davis-testimony.pdf.

[45] Luke Johnson, Huawei to introduce 5G networks for 2018 FIFA World Cup, Trusted Reviews (Nov. 19, 2014), http://www.trustedreviews.com/news/huawei-to-introduce-5g-networks-for-2018-fifa-world-cup..

[46] James F. Larson, PyeongChang 2108, the "5G Olympics", Korea's Information Society (Apr. 7, 2016, 8:51 PM), http://www.koreainformationsociety.com/2016/04/pyeongchang-2018-5g-olympics.html.

[47] Eric Auchard, Nokia, NTT DoCoMo prepare for 5G ahead of Tokyo Olympics launch, Reuters (Mar. 2, 2015), http://www.reuters.com/article/us-telecoms-mwc-ntt-docomo-idUSKBN0LY0FD20150302..

[48] Tim Hardwick, China Mobile to Begin Large-Scale 5G Testing This Year, MacRumors (Feb. 22, 2017, 2:11 AM), https://www.macrumors.com/2017/02/22/china-mobile-5g-testing-qualcomm/..

[49] European Commission, Digital Single Market: 5G for Europe Action Plan, https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan (last visited May 22, 2017).

[50] Press Release, Intel, Intel Accelerates Path to 5G (Feb. 22, 2016), https://newsroom.intel.com/news-releases/intel-accelerates-path-to-5g/.

[51] ITIF Innovation Infrastructure at 9.

[52] See Industrial Internet Consortium, http://www.iiconsortium.org/ (last visited May 23, 2017); Open Connectivity Foundation, https://openconnectivity.org/ (last visited May 23, 2017); OpenFog Consortium, https://www.openfogconsortium.org/ (last visited May 23, 2017); Open Fabrics Alliance, https://www.openfabrics.org/ (last visited May 23, 2017).

Mr. LATTA. Well, again, I want to thank our witnesses for being with us today. We really appreciate your testimony, and that will conclude our testimony from our witnesses and we'll begin our questioning from our members, and I will recognize myself for 5 minutes.

Mr. Day, do you believe a compendium of all current Federal action on IoT-related issues will help promote interagency collaboration and consistent federal action?

Mr. DAY. Thank you, Mr. Chairman, and again, I think what we've heard is that the Internet of Things holds incredible promise for our economy and the quality of life for citizens.

I do. I think the draft that we have before us today helps with increased transparency and how government regulates this technology in a better way.

We are firm believers that the government should make data available and complying a list of Federal policies that affect IoT, I believe, would go a long way in enabling the companies that we are working with at the Chamber and others and especially also small and startup companies to understand the regulatory environment that we are faced with today.

Mr. LATTA. Yes, let me ask you about that right there because I know that when my friend from Vermont and I were doing our Working Group meetings—and actually we had them right here in this room—it didn't make any difference if you're from the East Coast, the West Coast, the Midwest, what type you're in, as Ms. Vachani was talking about, from everything from health care to manufacturing to FinTech, you name it.

There was one thing that we heard from everyone—that we needed to make sure that we have a soft touch regulation out there so people can be out there innovating and it's no—we didn't hear anybody ever say that they were against regulations but not to have anything that was over burdensome that they couldn't go out and regulate.

When you're talking about these smaller companies out there, could you talk to me or talk to the committee a little bit about what you have heard from them some of the major hurdles that they're facing right now or things that need to be overcome?

Mr. DAY. Absolutely, and I think what's exciting about this is that this does impact middle America, the coasts. Everyone, as you said, is impacted by this and I think when you're a small business and a startup, and my focus at the U.S. Chamber of Commerce in the emerging technology space, it is just that. It's emerging. It's changing by the day.

We are still learning what the technology means and so I think there needs to be a structure but not too prescriptive in the approach and, you know, quite frankly, business leaders and new startups and entrepreneurs are looking to run their businesses with the support of the government but not being told exactly how to do it because we are still working on the benefits and how this actually applies to the companies that we are working with.

And so I think what business leaders want to know is give me the ability to invest, to be able to take my idea to the next step but don't regulate me so much that I am not able to produce quality results and in the end be successful as a startup.

Mr. LATTA. Thank you.

Ms. Vachani, again, I would like to turn a question to you now. What are some of the IoT applications that Intel is focused on and can you explain how those applications benefit the economy and jobs?

And, again, I was very interested because I know you were going through the health care, the manufacturing, the transportation, and construction, but if you could get a little bit more in depth with that I would appreciate it.

Ms. VACHANI. Absolutely. So we have over 500 market-ready solutions that we work with the industry to create because one of the common misconceptions about IoT it's vertical, right.

You have a retail solution and you have an industrial solution, and honestly, when you look across the board, our customers are looking at solutions that go across multiple industries.

And so there are multi-industry solutions. They don't necessarily sit in one nice little box as a vertical, and so you will see an industrial environment where they're trying to do predictive maintenance at the same time as inventory management, the same time as building management, and you see several different vertical like solutions coming together into one application.

And we believe that the maximum benefit is when these solutions start to come together. One of the areas that I want to reflect on is that the U.S. is actually a leader worldwide in our innovation that we have in IoT.

So you will see solutions overseas that have Intel or other companies within the United States technology, our AI applications, our software, that are driving innovation around the world, and that's expanding our economy just the same because that's created here in the United States.

It's built here by us and by our companies that are innovating at a faster rate.

Mr. LATTA. In my last 24 seconds follow up with that because, again, it's good to hear the United States is leading on this. What's happening across the globe that is making the United States be the innovator out there?

Ms. VACHANI. Well, I think that what we come down to is we have some companies here that are able to look at these solutions like Intel, truly, and that goes from the data center all the way to the thing.

And so we can look at this problem holistically and that's important that we do that, as well as some of the new technologies that we come up with with specifically integrated circuits as well as the software and artificial intelligence and the leadership in artificial intelligence within this country.

Mr. LATTA. Well, thank you very much. My time has expired and I yield back, and I recognize the gentlelady from Illinois, the Ranking Member of the subcommittee, for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

Connected devices can follow us through every aspect of our lives, collecting data. At the same time, the committee has spent a lot of time looking at how the data collected about us is used by companies and by the government.

We heard from Facebook about how much data it collects, how it shared that data with third parties, and how it used our data to sell advertising. As more and more devices collect data about us, that data can be used to affect our decision making.

So, Ms. Richardson, let me ask you some questions. While IoT devices provide benefits, are you concerned about their data collection?

Ms. RICHARDSON. Absolutely. The way the U.S. works its privacy law is to do it categorically, to cover, for example, communications, financial data, health information held by doctors, and if you don't fall into one of these categories you're just not protected and there are very few, if any, limits on how the information can be collected and used.

It's going to be possible that a lot of these IoT devices are going to collect data that is not covered by one of these categories already and that would be one of the benefits of having a baseline comprehensive privacy law in the United States as we would not have so many cracks and you would see the IoT data have some procedural rights for Americans.

Ms. SCHAKOWSKY. I would like to work with you on that.

Five years ago, we were barely talking about location data or facial recognition and now we are talking about genetic information also.

Ms. Richardson, should we be concerned about what personal information is out there and how the kinds of personal information available to collect change over time?

Ms. RICHARDSON. Yes. The information that is collected by these devices is really unique. You only have to go back a few years before we widely collected things, like you mentioned, that reflect, let's say, your heartbeat, your location, the food you eat, where you go, the people you know, and it can all be aggregated in ways that give a very rich picture about people in ways that they might be shocked to know.

I think one of the things you saw at your hearing with Facebook is that the surprise factor is really what upsets people in many ways.

So this is something we need to watch more closely and, hopefully, a universal privacy law would be able to protect that sort of really sensitive information right now.

Ms. SCHAKOWSKY. So it's clear that privacy legislation is absolutely necessary. I like the way you talk about it in a nonsiloed way.

In fact, the Federal Trade Commission has recommended many times that Congress enact comprehensive privacy legislation.

Ms. Richardson, again, the SMART IoT Act would examine how different industries are using and developing IoT. Could such a resource be helpful in the development of best practices for privacy and IoT devices?

Ms. RICHARDSON. Yes. I think that would help us get a better view of where the industry is going. I think you're going to find, though, that there are very few when it comes to privacy and for the most part the standards are about interoperability, technical standards, and cybersecurity, and you're going to find a really big gap here.

Ms. SCHAKOWSKY. So the FTC recommended in the past that privacy legislation should not be IoT specific. Do you agree with that?

Ms. RICHARDSON. Absolutely. We want a forward-looking tech-neutral law that will be able to cover all sorts of information regardless of the type of device or entity that's creating it.

Ms. SCHAKOWSKY. So Mr. Day said that one of the things that we need to worry about is too much regulation standing in the way. Don't you think there's a balance, though, of making sure that we set some rules of the road, some guidelines that industry needs to follow?

Ms. RICHARDSON. Yes, and in a way those can drive innovations themselves. You end up having requirements that inspire new solutions to protect privacy and security.

And CDT does believe in a light touch but there are a few places that government intervention—or oversight is maybe a better word—is most urgent and that's where you look at things like cars or pacemakers and devices that really have life or death consequences if something goes wrong, and I think we are seeing the consumer market is just an area where everyday people are not able to make informed decisions about the devices they're buying, the information that's collected and then how to secure the devices.

Mr. LATTA. Thank you. The gentlelady yields back.

The chair now recognizes the gentleman from Pennsylvania for 5 minutes.

Mr. COSTELLO. Thank you, Mr. Chair.

I want to sort of continue down that path of consumer-facing devices and speak a little bit more about being a small business owner or a startup, and approaching the infrastructure purchase questions from an adequate security measure perspective.

In what direction do we need to head—and it may not be necessarily government, it may just be more industry—in what direction do we have to head in order to make sure that we are getting it right.

A rather open-ended question, but why don't I start with you, Ms. Richardson?

Ms. RICHARDSON. As far as security standards go, we have endorsed tech-neutral cybersecurity controls. So these are really top-level decisions that both the manufacturers and the operators can make.

So, for example, when you're building a device you should always have the capacity to update the software, right, and you could say that without getting a really prescriptive technology, description of how to do that and each company can decide how to do that.

And there is a list of maybe a half dozen of these sorts of practices that I think are reasonably set as the baseline and they include other things like being able to have passwords or other authenticators that can be changed and things like that.

Mr. COSTELLO. Following through on that, steps or approaches that small and medium enterprises can utilize to overcome concerns or difficulties relating to the system integration side of IoT solutions, to—go ahead.

Ms. RICHARDSON. Can you repeat the question about system integration?

Mr. COSTELLO. Small and medium enterprises, overcoming their concerns or difficulties relating to system integration of IoT solutions. If you're a really big company, integrating is very easy. If you're a small——

Ms. RICHARDSON. Not actually. It's actually difficult either way.

Honestly, the number-one challenge for IoT right now is scale. Scale is very difficult, right, and even with a company as large as, you would say, Intel, if you look at our market-ready solutions, rarely do we have a solution that only involves Intel. There is others. There's Dell involved—as I mentioned, many of our solutions— Bosch was involved.

And so you're talking about multiple companies coming together to include a complete solution and for a small or medium-sized company that gets even more difficult, right. And this is where the industry standards come into play because when we start to create standards that are interoperable and that we know work together that a small or medium-sized company can create a piece and we know that that piece will work with the rest of the system.

And Intel and many other companies—we were here with Samsung—are working across the industry to help those standards get deployed and become more consistent interoperable.

Mr. COSTELLO. So when you use the term scale there, what are you saying?

Ms. RICHARDSON. What I mean by scale there is we are able to create—I will give you an example. We'll create a proof of concept inside of the walls of Intel in our building and it will look beautiful and work perfectly.

It'll have the in system, the data center. It'll have the store, let's say. It'll do inventory management. As soon as I take that out of my office inside of Intel and try to put into a Levi's store or I try to put it inside of a mall, now it's working with everything else around it and that's when we struggle, because there's other systems. There's old data. There's new data. Maybe the infrastructure is there. Maybe they have connectivity. Maybe they don't.

And so that becomes more difficult for us to deploy and then think about thousands and then add millions to that, right. And that's where we struggle with being able to take that technology and deploy it into multiple instances across the world.

Mr. COSTELLO. That's helpful. You were speaking about industry standards, and depending upon what industry we are talking about—health care, manufacturing, whatever it may be—the place that you go for that industry standard to make its way into code or regulation or whatever the case may be is oftentimes different.

Share with me challenges or frustrations in navigating Federal regulatory agencies to determine IoT industry standards and how we could go about improving that.

Ms. RICHARDSON. Well, one, I would encourage——

Mr. COSTELLO. That's a question for everyone.

Ms. RICHARDSON. Yes. I can start. One, I would encourage you to look at the industry standards that are already available to us because the industry is starting to coalesce around a few standards that go across multiple industries.

Again, we are not saying this is just for industrial or environ-
ment or it's just for retail. This is how we collect data across the
board and that could be a standard.

So I would encourage you to look, and I think that's part of the
recommendations here, is to look at what the industry is already
doing and leverage that because we have come across together in
this space, and I will allow you guys some time.

Mr. LATTA. Yes. Since the gentleman's time has expired, if you
all could just real briefly answer that would be great.

Mr. DAY. Well, I think what we are doing today in discussing is
the right first step. I think between the DIGIT Act and what we
are doing with the legislation in draft form today is that first step
and it's the right approach to some of these issues that we are dis-
cussing and bringing forward today.

Thank you.

Mr. LATTA. Would you like to comment? OK, thank you very
much.

Mr. COSTELLO. Yield back.

Mr. LATTA. The gentleman yields back. His time has expired.

And the chair now recognizes the gentleman from California for
5 minutes.

Mr. CÁRDENAS. Thank you very much, Chairman Latta and
Ranking Member Schakowsky, for having his important hearing
and I would like to thank the witnesses for coming forward and en-
lightening us as to what's going on out there in the real world.

My background is in engineering. I got my electrical engineering
degree from UCSB back in the days when we used punch cards in
our programming, your technical you lack.

So I think a lot has changed, but I think that many of us do wel-
come these changes, and having said that I think that public policy
needs to make sure that we are mindful of this fast-moving effort
of the Internet of Things and how it affects individuals' privacy,
how it affects industries, how it affects jobs, how it affects the jobs
of today and tomorrow, and how do we get American workers ready
and prepared to be the workers of today and tomorrow.

These are the kinds of things that weigh on my mind. During my
careers, I actually owned a small business at one time so I know
what it's like for a small business to be able to pull something off
the shelf in a very efficient cost-effective manner and I think the
Internet of Things is making that much more efficient every single
day and making smaller businesses, especially mom and pops a
heck of a lot more competitive.

Wherein, the old days, maybe back in my days in the '80s and
'90s when I was a business owner, everything was in maybe fives
and tens of thousands of dollars to get an innovative device. Now,
it appears that we can actually get an innovative device that
changes and allows us to be more efficient and hire more individ-
uals and grow our business to the tune of hundreds of dollars. Is
that correct? Do we have devices out there that maybe 20 years ago
to innovate were in the thousands of dollars and today it might be
only a few hundred?

Can one of you give me an example of something that you can
think of that actually touches on that?

Ms. VACHANI. Absolutely. If you think about, for example, the building management that was in New York, the deployment that we did, those were sensors that were not very expensive.

We are talking sensors that are dollars on—as it is, and they can look into a room and save a small business on their costs—their infrastructure costs by looking at occupancy inside of a room and deciding that the AC needs to be turned on because no one's in the room. This isn't expensive technology from that standpoint but it's changing the way we live and the way we operate within our businesses and saving us cost, right.

One of the major ways that this building in New York was able to save money is we found a leak in one of their pipes. Again, we are talking about a sensor that's able to determine that there's a leak in a pipe and will waste, right, and they were able to reduce that cost.

And so from that standpoint, innovation isn't necessarily requiring extensive amount of investment but there are ways where we can start to make decisions very quick when this data comes together.

Mr. CÁRDENAS. Ms. Richardson, I have a question for you about consumer applications and how do you think the Internet of Things devices are being used inside manufacturing workplaces?

I happen to represent a community in Los Angeles that has a big corridor of manufacturing, tens of thousands of manufacturing jobs in my district.

Ms. RICHARDSON. Yes, and I think it's still unknown how this is going to affect the workforce on balance, right. You're going to create new jobs of the people who actually have to create the devices, and we hope that a strong privacy and security practice will create professionals to deal with that also.

I think there are questions to ask about whether they will replace human beings on the job. But there will always be decisions that human beings have to make that we can't let computers do.

So I don't think it will eradicate humans altogether.

Mr. CÁRDENAS. Well, on that note, there are things such as smart helmets and smart glasses that now can be deployed in the workplace, and do you have any comments about how these devices might to affecting somebody's privacy in the workplace?

Ms. RICHARDSON. Yes, and peoples' privacy in the workplace is much more limited than in their home or out in public. This is long established that employers can really control the type of information that they're collecting on their property and while they're conducting their services.

I think, though, when you see a lot of these sorts of applications they don't have to necessarily collect a lot of personal information, right.

This is where, again, the controls built into the products on the front end are important so that you can collect the information necessary for your work but not, let's say, what they do on their breaks or the conversations they're having or things that are really not core to doing the job.

Mr. CÁRDENAS. Thank you. Mr. Welch talked about the cow and I was thinking, wow, I hope that cow is not creeped out about the privacy about every time she walks into the barn.

[Laughter.]

But, Ms. Vachani, I know Intel has been active on the connected worker's front and arguing that they keep workers safe and productive. Can you give us an example of that?

Ms. VACHANI. Absolutely. Actually, there's a really good example with a fireman which resonates with me, right. By connecting a fireman that goes inside a building we now know—by the sensors we can tell what is the oxygen level around him, or her, if the firewoman—the fireman is laying down or standing up, what exact location they're in within the building if they're laying down.

These are opportunities for us to save lives of some of our workers that are working in critical conditions. I think it's essential.

Mr. CÁRDENAS. Thank you. I yield back.

Mr. LATTA. Thank you. The gentleman yields back.

And I am sure they only have happy cows in Vermont.

The chair now recognizes the gentlelady from California for 5 minutes.

Mrs. WALTERS. Thank you, Mr. Chairman.

Mr. Day, do you believe that a review of all regulations guidelines standards and other policy efforts undertaken by Federal agencies is important and do you think it will assist us in ensuring consistent policy of Internet of Things-related matters?

Mr. DAY. Thank you for the question, Congresswoman.

Yes, I do. I think the SMART IoT Act, by studying all sectors of the IoT and how they regulate technology and current policies will go a long way in cutting down overly burdensome regulations and duplicative regulation as well.

I think when you're looking at the broad spectrum of applications here it's critical when you're looking at the impact on self-driving cars to getting a patient through a hospital more efficiently, cost effectively.

It's all important, and I think the legislation before us today will streamline that process and benefit by, frankly, everyone.

Mrs. WALTERS. OK. Thank you.

And Ms. Vachani, can you please discuss the benefits to a connected world both for business like Intel as well as consumers who use Internet of Things products?

Ms. VACHANI. There's multiple benefits through the Internet of Things. Whether it be more efficiency inside of a factory, so predictive maintenance is a very simple use case that we use in factories that allow us to determine if a machine is going down sooner than it actually does go down and that'll prevent the down time for the factory, right.

This is a fundamental analytics that has changed how efficient our factories can be. Let's think of retail where one of the number-one determinations of success or how they lose customers is because the item you're looking for isn't there.

So you go in for a pair of jeans, you don't have your size, you leave, you forget. That's important that we understand what people are looking for and that we have the inventory ready for them and that we understand what inventory you have. Inventory loss is a major loss for our retail businesses, especially brick and mortar businesses.

And then I would also look at cities and how cities are using technologies to do gunshot detection at intersections or monitoring the environment as far as air quality is concerned. And that data enables us to decide if the changes we are making—let's say we have in India electric rickshaws. Are they actually having an impact on our air quality and to make wise decisions based on data rather than hypotheses that we are making things better?

Mrs. WALTERS. OK. Thank you.

Mr. Day, as we continue to advance toward an increasingly connected world, some have expressed concerns with protecting consumer information.

These are vitally important concerns, yet we also must acknowledge that Internet of Things devices in a connected world provide substantial societal benefits.

Can you speak to how we can protect consumer information without losing the upside to a more connected world?

Mr. DAY. I think it's obvious that the Chamber believes that consumers deserve to have their personal data respected by the companies and it's important that we are mindful of that, going forward.

I think the other thing that I mentioned in my opening statement was that technology is not a single all-powerful industry and that I think it's important that this is a part of every industry.

And when we are looking at the Internet of Things, I think it's something that we need to be mindful of but not directly linking the privacy issue to this legislation, as we go forward. But I think it is something, as we've all testified to, that it's important and we need to be considering what data means now, because data is being created in massive amounts and how that is handles is truly important.

And I think that's one of the areas where the Chamber is doing a lot of work and you will be hearing more from us on some of the importance of privacy principles, going forward, as a result of some of the discussions that we've been hearing in Washington lately.

Mrs. WALTERS. OK. Thank you.

Ms. Vachani, as you may know, this committee is very focused on the advancement of self-driving cars. Your testimony discusses the enormous benefit of increased mobility that autonomous vehicles will provide for aging and disabled populations.

Can you expand on this and discuss the role Internet of Things plays?

Ms. VACHANI. Autonomous vehicles, what the connection back to an aging population is if you don't have public transportation for someone to get to the hospital or someone to get to where they want to go for a social benefit, let's say, and having more independence for our elderly population, a vehicle that is autonomous is safer for them to get from point A to point B and that enables them the flexibility and the independence that we want for our elderly population.

Mrs. WALTERS. OK. Thank you.

And I am out of time. Thank you.

Mr. LATTA. Thank you very much. The gentlelady yields back.

And the chair now recognizes the gentlelady from Michigan for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman, and to Ranking Member Schakowsky for the leadership on this issue and to everybody for being here.

I think that it's safe to say that we do have agreement on both sides of the aisle about the significant and revolutionary things that the Internet of Things is bringing to industry and consumers, and you all have certainly talked today about examples where it's already making a difference.

But I continue to have a reservation that's been expressed by a number of other of my colleagues. As we compare the rise of IoT to the development of the internet that the internet thrived because of the light regulatory touch used and I think we are not paying enough attention to security and privacy.

So I have to already say to you, Mr. Day, before I even ask you my questions to say that we should deal with privacy is not something that I am going to be comfortable with because I think that the technology—that the Facebook hearings have showed people had no idea of the amount of data that was being tracked and there isn't security on how that information is being used and we are not protecting even the privacy of an individual.

So I won't go off on that right now. But I had to respond to that comment. But I would like to ask a few questions.

Ms. Richardson, in a market that's rapidly evolving, how have you seen companies balancing getting to the market first with protecting security?

Ms. RICHARDSON. Yes. We often see that privacy and security is what fall short here, and a lot of these controls that are considered to be best practices are not hard from a technical matter.

For example, a couple of years ago the BitTag—the broadband internet technical advisory group—put out a report with a list of maybe 5 to 10 things that were of utmost priority like encryption, right, making sure that the data collected was protected in transit in storage, avoiding hard-coded passwords—this is one of the problems with the Mirai botnet, right. All of those cameras were accessible with the same password the hackers knew and they were able to get all these cameras.

And if you meet some of these baseline best practices you're going to lift all boats, right. It's not going to solve every problem but it will certainly give us herd immunity as users of all these different devices.

Mrs. DINGELL. Thank you.

Ms. Vachani, on the consumer side, have you seen privacy being designed into these products before they're hitting the market?

Ms. VACHANI. Yes. Actually, I will tell you and hope to give you confidence that the security and privacy is utmost imperative when we are designing a solution—where we store data, how that data is transmitted, and we look at that as a fundamental premise as we are integrating these solutions, and we make decisions that are different.

We may store data locally because it makes it easier for us to be able to protect it. And so these criterias are absolutely in the solutions that we create and we—if you look at the solution that we had with regards to the health care monitoring, that's FDA ap-

proved and we follow all HIPAA laws, right. We enable our silicon so that our solution developers are able to follow HIPAA laws.

Mrs. DINGELL. So not to be sarcastic, but as someone who has been hacked at least 15 times, every one of the major ones, and that's one of the difficulties is once that hack occurs—once that data is obtained by somebody you can't put the genie back into the bottle.

Mr. Day, I know your organization is concerned and apprehensive about regulations, as you expressed it. But one of my concerns is going to build right on what I just said—that down the road there will be these massive data breaches that we keep seeing or an abuse of privacy.

We'll convene a hearing. The witnesses will be questioned. Everybody will express outrage and concern, but the damage will have already been done, which was one on Facebook, which I just talked about.

Do you think it would be helpful to develop some clear rules of the road for companies now so we can try to mitigate this for the future?

Mr. DAY. Thank you, Congresswoman, for the question.

And to answer you directly, yes, I firmly believe that and I think I would like to suggest that the offer is extended to work with you and your office on these issues.

In fact, the Chamber is currently going through a process right now on developing privacy principles that we will be working with Congress on.

And so I think probably earlier than later, to be engaging with you and your staff would be a great opportunity.

I will tell you, again, that I firmly believe consumers deserve to have their personal data respected by companies that they're working with and I think that it's critical though that we strike that proper regulatory balance that protects consumers while promoting the technology that we all use every day and appreciate.

Mrs. DINGELL. That's one of the biggest challenges in this committee.

I know I am out of time, Mr. Chairman, but it would be interesting for the record to get what principles they are coalescing around that you mentioned earlier in your testimony. I think it would be useful for all of us.

Mr. LATTA. Thank you very much. The gentlelady yields back.

The chair now recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. Thank you very much. It's great to be here.

Thanks, Mr. Chairman. Thanks for having all the witnesses here. We've had some really interesting hearings in this space. The other day we did quantum computing, which I am still trying to figure out.

The guy said, well, I will make it simple for you—it's like flipping a coin and getting heads or tails is normal. In the quantum world you can flip a coin and get heads and tails at the same time. So that really made it simple for me. I've been thinking about that all weekend, trying to figure out what he actually meant. That's how he explained it.

But it is good that we are getting to a work product out of this so it's important. So that's what I want to focus on today and hopefully things I can understand.

So, Mr. Day, can you briefly explain while voluntary industry-led, globally recognized, and consensus-based processes for Internet of Things standards are so critical and could you name some examples of industry-led efforts that are currently taking place?

Mr. DAY. So with this legislation is, as I testified to, I think is an important first step and I think by having certain standards set and compiling information again by all industries and sectors will benefit all of us and that I think the benefits both to consumers, to industrial, and to government are very clear and, you know, it's everything from keeping a global competitive lead on other countries and that this country needs to continue to be the leader in technology and, again, I think, it's a great attribution to what the subcommittee and full committee has done on a bipartisan basis on self-driving cars to the health care applications that we've discussed.

So there's a whole host and wide variety of areas where this is a true benefit and, again, fully support the draft legislation and the DIGIT Act as well. We have come out in support of that early on and hope to work with the committee, going forward, on passing the legislation.

Mr. GUTHRIE. Thanks. And so, Ms. Richardson, why do you believe compiling a list of industry standard-setting efforts under the SMART IoT Act will be a critical part of helping to inform future congressional action?

Ms. RICHARDSON. Yes, and we would go one step further to say the list should also come with an estimation of whether the standards are being estimated. We don't want you to come back or get a report back that has a thousand standards listed because the next question is going to be well, are these being implemented, right—who's using these and are they working. That's the logical question and I think that's what Congress, advocates, industry is dancing around at this moment—is that process working?

So I would recommend to include that analysis top and that would help you figure out where you really want to focus your efforts, going forward.

Mr. GUTHRIE. OK. Thank you.

And Ms. Vachani, we've heard in the past hearings about the critical need for security and good cyber hygiene both in production lines for IoT devices and within the Federal Government.

What are you doing at Intel to safeguard IoT devices and networks from hacking vulnerabilities and what can small to mid-size businesses do to take meaningful steps to address data security concerns?

Ms. VACHANI. So if I look at Intel's contribution here, our security is fundamentally written into the silicon development. So it's in hardware, its software. It's in the connectivity. So we think of silicon across the board and we think of security across the board.

One of the areas that you talked about was software defined, right. As security standards start to change or as we learn more can we reprogram our devices—can we update those? And so that's included in our assumptions.

So we enable the industry through not only hardware but software security to be able to implement the best known security that we know at this point in our space.

So absolutely paramount in what we do.

Mr. GUTHRIE. OK. Thank you.

I know you mentioned earlier—and I had another hearing but I heard you mention earlier—scale. But could you name what you see as other potential impediments to deployment of IoT and what we should be aware of, going forward?

Ms. VACHANI. Well, we've talked quite a bit about standards and one thing I want to make sure we make the point of is these standards are international, and so scale is just not within the United States.

I would like for us to be competitive internationally and having these standards that were global allows us to provide technology to other countries and export our great experience that we have here.

And so I believe the interoperability and enabling us to be competitive internationally and taking advantage of these international standards will be important for us to be successful.

Mr. GUTHRIE. Thank you, and thank you for your testimony. I appreciate it. It's a little more understandable for someone like me. I asked the guy how could you flip a coin and get both.

Ms. VACHANI. I have no idea.

Mr. GUTHRIE. He says, it's like putting it in a box and the box is continually spinning and that really is the clue.

[Laughter.]

This is coming from a guy who's never solved the golf peg game at Cracker Barrel. So we'll figure it out.

Thanks a lot. I appreciate it, and I yield back.

Mr. LATTA. The gentleman yields back.

The chair recognizes the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you, Mr. Chairman. I want to thank you and the ranking member for having this hearing today and I want to thank the witnesses very much for being here.

I've discussed the potential block chain applications with the subcommittee before including its possibility to allow spectrum sharing as next-generation broadband networks are deployed. As you all know, block chain is a decentralized accounting technology that verifies transactions through a shared ledger system. When a transaction and a block chain is completed, that transaction is verified against a ledger stored on each computer in the network. The IoT and connected devices will facilitate a significant expansion of data transactions likely between multiple different networks and block chain could be used to verify and secure these transactions.

Is there an opportunity for this legislation to more precisely explore how new technologies could facilitate the secure advancement of internet-connected devices? And anyone on the panel can answer that.

Mr. DAY. I will take a first attempt at answering that question. And I agree with you—I think block chain is certainly an area where IoT will offer a lot of benefit.

At the Chamber we are just now beginning to work on our FinTech work and we are calling on members to help us understand the benefits. And so I think there are a number of ways that we should be looking at this.

I think the legislation as drafted, though, is the correct step. It allows for technologies like block chain and others to progress.

But as we are understanding the technology and the benefits thereof we can continue to work with you and other members of Congress on implementing certain regulations as appropriate facing the technology.

Ms. MATSUI. Anyone else?

Ms. VACHANI. Block chain is absolutely a technology that Intel is looking at and one that can be used in IoT applications, so a really good connection there.

I think, though, one of the points that you made when you kicked off as you're looking 5 to 10 years out and you have the benefit of doing so, and so today it's block chain and tomorrow it could be something even more revolutionary and that's why it's important that we consider this not from a very technology-specific standpoint but you're more holistically as to what's necessary for us to be successful, regardless of the implementation technology.

Ms. MATSUI. OK. Narrow band IoT networks are particularly useful for long-range low-power applications. Specifically, these networks improve capacity, spectrum efficiency, and power consumption levels of user devices.

Narrow band IoT networks have potential both nationwide and particularly for rural and indoor coverage. These networks can co-exist with commercial mobile networks and their propagation characteristics could provide better range and reduce coverage costs for consumers in both rural areas and across the country.

Anyone on the panel—what role do narrow band networks have in the IoT ecosystem from a spectrum efficiency cost and deployment perspective?

Ms. VACHANI. I think narrow band is going to help with—there are several elements in narrow band that makes IoT applications you have already referred to—it's lower cost, lower power, and a longer—which enables longer battery life.

So think about we currently have an application where we are sensing the environment for a case of strawberries, right. We want to make sure the humidity is right. We want to make sure the temperature is right. Narrow band allows for that connectivity—the continuous connectivity while extending the battery life and not increasing the cost of something that we'd want to do with a pack of strawberries.

Also understand that when you move to the world of 5G, now all of this comes together. So now we have a narrow band spectrum. 5G includes all of those spectrums—will enable us to be able to pull this together as a complete solution.

It revolutionizes how we think of connectivity and our spectrums because narrow band is included as well as low latency as well as high bandwidth.

Ms. MATSUI. OK. Great.

Anyone else want to comment on that?

OK. Spectrum is the invisible infrastructure and Congressman Guthrie and I are working on this. It underpins our communications infrastructure and adequate supply is necessary to realize the potential on next-generation broadband networks and the IoT. Specifically, agencies should have access to funds made available for engineering research that could lead to the repurposing of spectrum for commercial use.

What role will next-generation networks play in our IoT strategy and how would delivering more spectrum to commercial users help?

Ms. VACHANI. I would summarize it into one word, which is interoperability. If you think about a wider spectrum analysis, so 5G enables low spectrum as well as low latency high bandwidth, and now you have that on one network.

And so you're able to include all of those. Remember I said that it's not very much a vertical solution. We have all kinds of pieces that are coming together into an IoT solution, which can vary in spectrum and once we have a solution that encompasses all those spectrums now it makes deployments easier for our customers, thus enabling scale, which we——

Ms. MATSUI. OK. I've run out of time, so thank you very much.

Ms. VACHANI. Thank you.

Ms. MATSUI. Yield back.

Mr. LATTA. Thank you very much. The gentlelady's time has expired and the chair now recognizes the gentleman from West Virginia for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman, and I apologize to the panel—that we've got a hearing going on downstairs so we are back and forth in between them, and perhaps I've missed some of your testimony that targeted what my questions were.

But I want to begin with saying that I am going to start by assuming you have all read Case's book, "The Third Wave." Two out of three have. I was fascinated with that book—that the possibilities of where we might go long term, it was mentioned about the refrigerator that could speak to you, your clothing could tell you how your—whether your wellness.

Those were all in the long terms. I am somewhat interested in the short term, however, and that is, is there anyone—can you tell me from the three experiences we have up here, is there something in the pipeline of the IoT that might indicate the propensity of an area to have a problem with opioid abuse?

I know some people have—or they've talked about doing it, to be able to develop where that might be. But is there anyone that you know of that's actually got something close to fruition that we could do this? Because we are getting, as we all know, nationally getting hit pretty hard with this and we don't know where the next problem is going to crop up until after. We are reacting rather than being proactive.

So I am curious to see with the Internet of Things in a short term is there someone developing software that might be able to identify where the next problem could crop up?

Ms. VACHANI. Yes. Actually, Intel is working exactly on that problem, concerning the monitoring of medicine and the ability to know exactly where that medicine is going—is it going to the right person, monitoring how many tablets are there and knowing ex-

actly who's taking those—having some facial detection—who's picking up those tablets.

And so absolutely. I believe that you have made a very relevant connection, and thank you for that.

Mr. MCKINLEY. What's the time—do you have a sense of——

Ms. VACHANI. We are seeing an implementation immediately, and it's an evolution over time. We are not going to have facial detection immediately at all of our pharmacies but it'd be interesting.

It's an evolution over time but we are seeing implementations right away in which we can start to monitor medicine better. It's just a matter of is it getting to the right person, how many, and are the right people taking it.

So you think about in the opiate but you can also think about it with elderly patients as well, right, or making sure they are taking their medicines on time.

Mr. MCKINLEY. That may be a worry but, again, the propensity, this community may be hit hard next. That's what I am looking for as well.

The fact that there could be some software that says the drugs—20 million pills are going to one pharmacy, that ought to trigger something.

Ms. VACHANI. Right.

Mr. MCKINLEY. But in the meantime, are there socioeconomic barriers that we need to break down?

So, Mr. Day, you look like you were going to contribute to this conversation.

Mr. DAY. So yes, at the Chamber, Congressman, we have been looking at economic situations across the country and that impact of joblessness and how communities have been impacted by this plight and looking at ways that we can start to examine the linkage between the two.

And I think to the point on monitoring pill bottles and knowing times of when they're taken and monitoring who are getting their prescriptions, et cetera, those are things that are happening now but there is a lot more to be done.

Mr. MCKINLEY. Well, if I could on that, because you touched on something I am kind of sensitive to is the socioeconomic—household income, education level.

Some will use that as the excuse for why West Virginia is leading the Nation in opioid overdose but number two, until last year, was New Hampshire, and New Hampshire has polar opposites on that. It has one of the highest household income. It has the highest education level, and on and on and on, with good socioeconomics.

So I think there's something separating the two between us. So I am just curious if someone's developing something more sophisticated than just going on socioeconomics.

Mr. DAY. I am not personally aware, to be honest with you. But I think it would be an opportunity for us to work together as we continue our work with the Chamber and working with our member companies on various technologies, and I would be happy to do that.

Mr. MCKINLEY. I would like to pursue that.

Ms. VACHANI. I would like to offer that we can follow up with the details of the solution I just.

Mr. McKINLEY. If you could, back to my office, I would appreciate that.

Ms. VACHANI. I would love to do that, if I could help.

Mr. McKINLEY. All of you. Thank you very much.

I yield back my time.

Mr. LATTA. Thank you very much. The gentleman yields back.

The chair now recognizes the gentleman from Vermont, and I want to thank him for all of his hard work not only in this Congress but in the last Congress, working on IoT issues with me.

So thank you very much. The gentleman is recognized for 5 minutes.

Mr. WELCH. Thank you, and thank you as well, Mr. Latta.

I want to focus a little bit on rural America—just to have each of you say what it is we need to do in rural America if we are going to have any opportunity to yield the benefits of IoT.

I will start with you, Mr. Day.

Mr. DAY. So I think one of the most important things, and you mentioned it earlier, Congressman, is the fact that broadband is not in every household in the country and that's first and foremost, I think, for a lot of reasons, I think, for being able to compete globally, being able to be connected and be able to have a business based upon the internet is critical.

And so I think for rural America—and I applaud your efforts. That's first and foremost.

Mr. WELCH. Thanks.

Ms. Richardson.

Ms. RICHARDSON. Well, I think the whole point of having standards and what your bill is discussing is to shift the responsibility for security to the people who can best address it, right—the manufacturers, the operators—and I think this is where low-tech users benefit most from this.

And so to the extent that your rural users are rapidly deploying new technology that they're not familiar with they will certainly benefit from better security standards.

Mr. WELCH. Thanks.

Ms. Vachani.

Ms. VACHANI. Absolutely. I absolutely applaud the benefit to get broadband into rural America but understand that we can do to implement technology today whether it be a cellular signal, right.

I will give you the example of my parents, who still live in the same house that I grew up in and won't leave no matter what I do at this point. Having some type of monitoring, making sure they're getting up in the morning and that they're—oh, somebody's opened the refrigerator, that she's eating—there's elements of that that I think is important that we can do today for rural America with the connectivity that we have and we don't have to limit ourselves to that deployment.

Mr. WELCH. OK. Thank you.

The other broad question—I just want to go down the panel—is about privacy and security. You have talked a little bit about that.

But is there a role that you believe the Congress has to play in ensuring an individual's personal data is protected and is it your view that an individual has to have the control over how his or her

data is being used—something we asked Mr. Zuckerberg when he was here a while ago?

Mr. DAY. Well, again, I think to emphasize the point that consumers have and deserve the right to have their personal data respected by all.

Mr. WELCH. Let's go quickly because I have one more question.

Mr. DAY. As we develop our principles at the Chamber, I look forward to working with you on those details.

Mr. WELCH. Thank you.

Ms. RICHARDSON. We eventually need legislation. That's going to be the only way out of this mess we are in.

Ms. VACHANI. I think working together between government and industry is essential to come up with the solutions.

Mr. WELCH. But there has to be some role that Congress plays. We can't be passive observers of what's going on.

Mr. DAY. Right.

Mr. WELCH. Do you agree with that? Thanks.

Let me ask you, Ms. Vachani—I know Intel has been a leader in IoT advancement and I know you have had a high position as a thought leader in that space for years.

So I want to follow up your testimony and ask if you can expand your suggestions as to the definition that we should use in his bill and why it's so important to get that definition right.

Ms. VACHANI. One of the number-one challenges of scale, and it sounds very simple, is terminology. We talk past each other when we are having—and I see us doing it in the industry, and so we are in this space. We live it and breathe it. But we use different words to represent different things and we are talking past each other.

So one of the fundamental things I've had to do within my organization, within my company as well as outside, is to start to get on the same language and that's one of the things we are asking for this as well is just to get on the same language so we know when we are speaking to each other what we are referring to.

Mr. WELCH. OK. Thank you.

I thank the panel. Very helpful.

And I yield back.

Mr. COSTELLO [presiding]. The gentleman yields back.

The gentleman from Oklahoma, Mr. Mullin, is recognizes for 5 minutes.

Mr. MULLIN. Thank you, Mr. Chairman, and thank our panel for being here.

I have just a few questions, and Ms. Vachani—is that how you pronounce it? I appreciate you being here and I just, for the help of myself and you might have already been asked this question, but as you have heard we were running back and forth between committees.

Ms. VACHANI. No problem.

Mr. MULLIN. Are there barriers or what are the barriers that's keeping the U.S. from leading in the IoT?

Ms. VACHANI. I answered this question of scale but I will answer this question slightly differently, to add to that.

What I find is, if you look at the city level there's quite a bit of innovation going on. I talked about San Diego and what San Diego

is doing within their lights in California. We talked about New York and the building management that's happening in New York. At the city level, I believe that that implementation is taken seriously and there's a lot of innovation happening. But where I think we can make a difference is scale across the city at a nationwide—right.

So these pockets of innovation, how we can reuse, how can we learn, and how can we deploy it more worldwide, more United States wide. That's slightly different than what I see in other countries where we are looking at it more nationally. India, China are looking at it more nationally, and so you'd get the benefit of the individual innovations that are happening at a national level.

Mr. MULLIN. Well, I will use my district, for example, even my personal house. We don't even have slow dial up. The best we can do is 3G through our phone, and 50 percent of my district has little to no access to the internet.

Ms. VACHANI. Yes.

Mr. MULLIN. And so we talk about metropolitan areas. But you're right, we are leaving out the rural pockets, which mileage-wise is the vast majority of our country.

Are the other countries, as you alluded to, are they doing a better job at that and then—and if so, what are they doing that we are not?

Ms. VACHANI. So large parts of India and large parts of China don't have connectivity either, right, and so that isn't an isolated and probably more of an issue there than it is even here.

They are looking at how to deploy faster so that these rural areas do have connectivities—that's one area we could look further at—as well as leveraging the technology that is available.

So going into a factory in another country—they have connectivity, no broadband, but they have some level of 3G—we are able to leverage that to at least start to get some automation within the factory. So, again, taking advantage of the connectivity that we do have a maximizing that, at the same time deploying more robust connectivity.

Mr. MULLIN. So what role can Congress play then? How can we encourage companies or industry to look out farther than just in metropolitan areas?

We did this with electricity. We did this with phone service. This is a new technology that's keeping us from connecting. So what is that we can do? What can Congress do, to put in place, to help encourage that?

Ms. VACHANI. I think we can look at this not in the siloes that we do today. You have the benefit of a holistic view, not just in each department but as a holistic view how we deploy this.

Mr. MULLIN. Right.

Ms. VACHANI. That's the benefit, and then, frankly speaking, how do we invest so that we start to deploy this technology more robustly—is there an investment strategy to that as well.

Mr. MULLIN. Thank you so much.

Switching gears, Ms. Richardson, how difficult is it to secure an IoT device?

Ms. RICHARDSON. I think that would depend on the device itself and how it's connected to the internet. I think there are a handful

of best practices that we see across different sectors and industries, things like encryption, strong password and other authentication models, update ability.

Mr. MULLIN. Have certain security measures been put in place since the 2014 Target breach, especially the Wanna Cry ransom?

Ms. RICHARDSON. There's nothing mandatory and I think these sorts of practices that——

Mr. MULLIN. Should there be?

Ms. RICHARDSON. That's a hard question and I am realistic about mandatory requirements on the private sector. I don't think we are there.

I think, though, the government should explore its own purchasing power. Right now, the Trump administration and some of the agencies are writing privacy and security guidelines in preparation for a big level up in purchase of IT modernization and that would be one way that you could influence the market without forcing anybody to do anything specific.

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

Mr. COSTELLO. The gentleman yields back.

The gentlewoman from New York, Ms. Clarke, is recognize for 5 minutes.

Ms. CLARKE. I thank you, Mr. Chairman, and I thank our ranking member, Ms. Schakowsky. I would like to also thank our panel for their expert testimony here this morning.

As you may be aware, earlier this year I launched the congressional Smart Cities Caucus and I would add Smart Communities with Rep. Darrell Issa. I was inspired to start the Smart Cities Caucus from my personal interactions with seeing the amazing build-out first hand in New York City. The Smart Cities Caucus serves as a bipartisan group of members dedicated to bringing American communities into the 21st century through innovation and technological change. Embracing smart technology will make our communities more sustainable, resilient, efficient, liveable, and competitive in a world in which technology is constantly advancing.

So I would like to ask a couple of questions, first to you, Ms. Richardson. What are your recommendations for the SMART IoT Act considering the interplay of the Smart Cities and which Federal agencies should play an active role in sort of harnessing what we know already?

Ms. RICHARDSON. Well, you have some of the work horses of the cybersecurity world in Commerce, right, so that is a benefit that you have with NIST, NTIA, and other places.

I think when you look at the smart cities you have a couple of different types of devices. You have really basic ones that don't collect personal information, they're low broadband information sharers, right, and they're just water pressure, how many cars passed through here, things like that, that are going to be less risky from both a security and privacy standard.

I hope that your report will highlight some of the more high-risk things that are either facial recognition, location tracking, right. That's the result of many of these things like license plate readers or toll roads and how those are being deployed by the government.

Ms. CLARKE. Ms. Vachani, Intel IoT portfolio includes smart cities, smart buildings, and smart video. What are your recommendations and why are smart cities so important to Intel's IoT portfolio?

Ms. VACHANI. Essentially, the Smart Cities enables us to create an infrastructure for safer cities as well as enabling our cities to do better planning.

If you look at the GE solution that we deployed on smart cities, it does stuff like gunshot detection, right. It's determining if there was a shot and, if so, what we do about it.

It looks at air quality, right, and so this enables us to take advantage of the technology we've built for many other industries. Smart Cities is a culmination of many other technologies we've built maybe for a factory or for a home but we are able to leverage that to improve not only our environment as well as our cities and its planning.

So we see that there's a leverage of our technology across the board and that Smart Cities can take advantage of it.

Ms. CLARKE. And would you just envision for some of my colleagues who are in rural communities how we can look at that ecosystem that is being developed in more densely populated areas and what can be taken from that for more sprawling communities in terms of connecting them in smart ways?

Ms. VACHANI. Yes, and I will go back to the GE solution. The GE solution takes advantage of a light pole. So that's what we are building on top of. It already has electricity. It already has power. You take advantage of that power to connect up sensors and then it uses a 3G connection that goes back up into a data center.

So, again, we are able to take advantage of infrastructure that's already there and built in as best as possible.

Ms. CLARKE. Very well.

And, Mr. Day, anything that you'd like to add in this?

Mr. DAY. Absolutely, and I want to applaud you on your efforts with Congressman Issa with co-chairing that caucus. It's very important, and C–TEC has joined a couple of events and we look forward to continuing to work with you.

But I think when you look at a city, for example, 20 percent of a given city in the United States is dedicated during the work day to parking, and I think one of the things that C 09TEC has been taking as a priority and working with you and others on is the fact that autonomous vehicles will impact both that issue as well as the environment and other issues and I think it, in the end, will prove to be very beneficial for a lot of reasons.

And so smart city activities are critical and what we are trying to do and be creative in our thinking and our approach and how IoT plays in that is paramount and a top priority of ours, going forward.

Ms. CLARKE. Well, thank you very much for your response today, and I yield back, Mr. Chairman.

Mr. COSTELLO. Gentlewoman yields back.

Seeing there are no further members wishing to ask questions, I would like to thank all of our witnesses for being here today.

Before we conclude, I would like to include the following documents to be submitted for the record by unanimous consent: a let-

ter from the Consumer Technology Association, a letter from CTIA, and a letter from EPIC.

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

Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record and I ask that witnesses submit their response within 10 business days upon receipt of the questions.

Without objection, the subcommittee is adjourned. Have a good day.

[Whereupon, at 11:54 a.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]

Consumer
Technology
Association

May 21, 2018

Chairman Bob Latta
Committee on Energy and Commerce;
Subcommittee on Digital Commerce
and Consumer Protection
U.S. House of Representatives

Ranking Member Jan Schakowsky
Committee on Energy and Commerce;
Subcommittee on Digital Commerce
and Consumer Protection
U.S. House of Representatives

Dear Chairman Latta and Ranking Member Schakowsky;

The Consumer Technology Association (CTA)™ would like to thank the Digital Commerce and Consumer Protection Subcommittee for its leadership in proposing policies to support the advancement of innovation and the Internet of Things (IoT).

CTA is the trade association representing the $351 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. Every day, our more than 2,000 member companies are developing extraordinary products and services and creating American jobs. At CTA, we work to advance government policies that encourage innovation and business creation.

The Internet of Things ecosystem is vast, encompassing products and services across every industry and market. CTA estimates that 715 million connected consumer technology devices will be sold in the U.S. this year.[1] This includes devices like laptops, tablets, smartphones, gaming consoles, smart TVs, smart speakers, fitness trackers, smartwatches, connected Wi-Fi cameras, smart doorbells and door locks, connected light bulbs, streaming media players and more.

As the IoT ecosystem has developed, the number and involvement of various government agencies and organizations has grown exponentially. The State of Modern Application, Research, and Trends of IoT Act (SMART IoT Act) would catalogue the work of various federal government agencies and assist in setting a solid baseline and understanding of the IoT ecosystem. The SMART IoT Act would require a report on the state of the internet-connected devices industry in the United States. This is essential in assisting policymakers as they develop policies that foster innovation, eliminate redundancies and determine opportunities for better cooperation between agencies and the industry.

We appreciated the opportunity to provide our feedback on the discussion draft and your willingness to incorporate many of our suggestions. I applaud your thoughtful approach and CTA is happy to lend its support to this effort.

---

[1] CTA Consumer Technology Extended Forecasts 2016-2021 (January 2018 edition)

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

Sincerely,

Gary Shapiro
President and CEO

ctia™

Meredith Attwell Baker

May 22, 2018

Representative Bob Latta
Chairman, Digital Commerce and Consumer Protection Subcommittee
United States House of Representatives
2448 Rayburn House Office Building
Washington, D.C. 20515

Representative Jan Schakowsky
Ranking Member, Digital Commerce and Consumer Protection Subcommittee
United States House of Representatives
2367 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Latta and Ranking Member Schakowsky:

CTIA writes to express its strong support for the State of Modern Application, Research, and Trends of IoT Act, known as the "SMART IoT Act."

The wireless industry, including carriers, device manufacturers and component providers, are actively involved in the Internet of Things ("IoT") ecosystem that will depend on the speed, capacity, and reliability of wireless networks, including 5G. According to a recent study by Accenture, America's wireless industry leads the globe in preparations necessary for IoT, including $300B in network investment over the past 10 years.

Today, wireless carriers and suppliers are focused on deploying 5G networks, with initial rollouts scheduled for later this year. 5G will be 100 times faster than existing 4G networks, enabling safety-critical communications in areas like public safety and transportation. 5G will connect 100 times the number of devices as 4G, accommodating the enormous growth in connected devices, from streetlights to factory machinery to medical implants. 5G will be five times more responsive than 4G, leading to near real-time applications like robotics and remote surgery. These attributes of 5G will allow IoT to achieve its promise of economic growth, efficient operations, and lives saved.

The SMART IoT Act leverages industry efforts to develop innovative and secure IoT applications, and helps coordinate agencies in this rapidly-growing, cross-sector technology. Along with modernizing our nation's infrastructure and creating a robust spectrum pipeline, this bipartisan legislation will ensure continued U.S. leadership in IoT development.

We applaud you both for your work on this important issue and your thoughtful legislation.

Sincerely,

Meredith Attwell Baker
President and CEO

epic.org

May 21, 2018

The Honorable Bob Latta
The Honorable Jan Schakowsky
House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the upcoming hearing on "Internet of Things Legislation."[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things ("IoT")[2] has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. These issues have a significant impact on the future of cybersecurity, and we commend the Subcommittee for exploring them. Congress should develop meaningful safeguards for the privacy and security of Americans' personal data.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is a leading advocate for consumer privacy, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") including 2013 comments on the Internet of Things.[4] And in 2015, EPIC testified at a hearing on "The Internet of Cars" before the House Oversight and Government Reform.[5] EPIC recently submitted comments[6] to the Consumer Product Safety Commission ("CPSC") on the hazards caused by weak privacy and security in IoT products and testified before the Commission.[7]

Privacy, Security, and Physical Safety Risks of the IoT

---

[1] *Internet of Things Legislation*, 115th Cong. (2018), H. Comm. on Energy and Commerce, Subcomm. on Digital Commerce and Consumer Protection (May 22, 2018),
https://energycommerce.house.gov/hearings/internet-of-things-legislation/.

[2] EPIC, Internet of Things (IoT), https://epic.org/privacy/internet/iot/.

[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[4] https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf

[5] Khaliah Barnes, EPIC Associate Director, *The Internet of Cars*, Testimony, 114th Cong. (2015), H. Comm. on Oversight and Government Reform, Subcomm. on Information Technology and Subcomm. on Transportation and Public Assets, (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

[6] EPIC Comments to CPSC, *The Internet of Things and Consumer Product Hazards* (May 2, 2018), https://epic.org/apa/comments/EPIC_CPSC_IoT_May2018.pdf.

[7] Sunny Kang, EPIC International Consumer Counsel, *The Internet of Things and Consumer Product Hazards*, Testimony, CPSC (May 16, 2018), https://www.youtube.com/watch?v=-YSDEkWuxUo&feature=youtu.be.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[8] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[9]

Furthermore, software and hardware vulnerabilities also harm consumers. Last year EPIC joined other consumer advocacy groups in a letter to the CPSC to urge the agency to recall Google Home Mini.[10] Due to a hardware flaw, the device was always listening to conversations and users could not disable it. Therefore, both the intentional designs (e.g., Amazon Alexa) and unintentional flaws (e.g., Google Home Mini) of IoT devices present risks to consumers.

In addition to privacy risks, the IoT also poses risks to physical security and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers. For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse. Researchers have already demonstrated the ability to hack into connected cars and control their operation, which poses potentially catastrophic risks to the public.[11]

It is not only the owners of IoT devices who suffer from the devices' poor security. The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled by cybercriminals who use the botnet to take down web sites by overwhelming the sites with traffic from compromised devices.[12] The IoT was largely to blame for attacks in 2016 that knocked Twitter, Paypal, Reddit, Pinterest, and other popular websites off of the web for most of a day.[13] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[14]

---

[8] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC- AG-Always-On.pdf.

[9] Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too.

[10] Coalition Letter to U.S. Consumer Product Safety Comm. On Google Home Mini (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

[11] *See, e.g.*, Karl Brauer & Akshay Anand, *Braking the Connected Car: The Future of Vehicle Vulnerabilities*, RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car- thetfuturetof-vehicle-vulnerabilities.pdf ; FireEye, *Connected Cars: The Open Road for Hackers* (2016), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for- hackers.pdf.

[12] *See* Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Schneier on Security (Oct. 6, 2016), https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

[13] *See* Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn.com (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[14] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

Effective Regulation of the IoT

These problems will not be solved by the market. Because poor IoT security is something that primarily affects other people, neither the manufacturers nor the owners of those devices have any incentive to fix weak security. Compromised devices still work fine, so most owners of devices that have been pulled into the "botnet of things" had no idea that their IP cameras, DVRs, and home routers are no longer under their own control. As Bruce Schneier said in congressional testimony, a manufacturer who puts a sticker on the box that says "This device costs $20 more and is 30 percent less likely to annoy people you don't know" probably will not get many sales.[15] Moreover, consumers rarely have adequate knowledge about the security of an IoT product when they are determining whether to purchase it. This information asymmetry makes it impossible for market forces to regulate the IoT effectively.

The regulatory environment is currently too weak to protect American consumers. The FTC's authority is insufficient to protect consumers. Unlike other federal agencies, the FTC has virtually no rulemaking authority; its ability to regulate is based on ex post facto enforcement actions. This means that the FTC cannot act until after consumers have already been harmed. Other agencies, such as the Consumer Product Safety Commission, should regulate the IoT. Manufacturers could be liable under tort law using products liability theory, but this legal strategy has not been employed much in the courts.[16]

Consumer Product Safety Commission

It is incumbent upon the CPSC to regulate the privacy and security of IoT devices. Privacy and security are integral to consumer safety. And today, the Internet of Things are the weakest link to privacy and security vulnerabilities in consumer products. IoT devices track personal data by seamlessly integrating into the consumers' activities and lifestyles. They blend into everyday objects. Thus, the ubiquity of IoT sensors and their amassment of granular data pose significant privacy concerns that could threaten physical danger.

We brought the Google Home Mini complaint[17] to the CPSC and not the FTC, precisely because the design defect of the device, intended for the consumer marketplace, created a specific privacy and security risk to consumers. We received a response from the Acting Chairman of the CPSC, stating that "CPSC's authority will not generally extend to situations solely related to consumer privacy or data security, that do not pose a risk of physical injury or illness, or property damage."[18]

This assessment reflects a lack of understanding about the Internet of Things and the new threats facing consumers. As renowned security expert Bruce Schneier has said: "The Internet is

[15] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, 114th Cong. (2016).
[16] Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. Mich. J. L. Reform 913 (2017), http://repository.law.umich.edu/mjlr/vol50/iss4/3.
[17] *See supra* note 7.
[18] CPSC Acting Chairman Ann Marie Buerkle, *Response to EPIC and Consumer Privacy Organizations* (March 23, 2018), https://epic.org/CPSC-response-GoogleHomeMini-3.23.18.pdf.

dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood."[19]

Poorly secured IoT devices are used for botnets that launch network attacks that can cause millions of dollars in property damage and have devastating impacts on real people.[20] Hackers could conceivably exploit vulnerabilities on your "smart" refrigerator to carry out a denial of service attack against the network of a city or hospital. In the past few months alone there have been several such attacks. A ransomware attack known as SamSam took down the entire municipality of Farmington, New Mexico and two hospitals by exploiting vulnerabilities in IoT devices.[21] The city of Atlanta spent 2.6 million dollars to recover from a ransomware attack that impacted municipal functions including the Police Department and the judicial system.[22] It would defy reason to say that unsecured IoT devices do not harm consumers.

Privacy and security hazards should be regulated in the manufacturing and design of consumer products. Companies have little incentive to maintain strong standards without regulation. And consumers do not have enough information to evaluate the privacy and security of these products themselves. This has alarming implications for toys that target children's data, and internet-connected home systems like smoke detectors and security cameras.

Therefore, manufacturers—not consumers—must bear the responsibility to ensure the security of their products.[23] We agree with the UK Government's assessment that "There is a need to move away from placing the burden on consumers to securely configure their devices, and instead ensure that strong security is built in by design."[24]

Current voluntary standards are lax. And current safety regulations are outdated. They are not adequate to address the security hazards of IoT devices. The CPSC should establish mandatory privacy and security standards, and require certification to these standards before IoT devices are allowed into the market stream.

---

[19] Bruce Schneier, *IoT Cybersecurity: What's Plan B?*, Schneier on Security (Oct. 18, 2017), https://www.schneier.com/blog/archives/2017/10/iot_cybersecuri.html.

[20] Bruce Schneier, *Click Here to Kill Everyone*, N.Y. Magazine (Jan. 27, 2017), http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html (describing an attack that used millions of DVRs and other insecure IoT devices to take down Twitter, Netflix, Reddit, and other sites down from the internet).

[21] Bill Siwicki, *71% of IoT medical device ransomware infections caused by user practice issues*, Healthcare IT News (March 5, 2018), http://www.healthcareitnews.com/news/71-iot-medical-device-ransomware-infections-caused-user-practice-issues.

[22] Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare*, Wired (April 23, 2018), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

[23] *See* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. Mich. J. L. Reform 913 (2017), http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr.

[24] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (March 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

The code of practice proposed by the UK government serves as a useful framework for security standards for IoT. In particular, manufacturers should adopt the following:[25]

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Data protection
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. And validate input data

This guidance necessitates privacy and security by design. If the CPSC implements this code of practice, it will shift the responsibility of product safety back to manufacturers where it belongs.

Congress should act to empower regulators to protect consumers from the risks posed by the IoT. We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these and other issues impacting the privacy and security of American consumers.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

---

[25] *Id.*

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

June 26, 2018

Mr. Tim Day
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce
1615 H Street, N.W.
Washington, DC 20062

Dear Mr. Day:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Tuesday, May 22, 2018, to testify at the hearing entitled "Internet of Things Legislation."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, July 11, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.
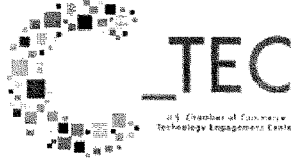
Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

_TEC

Questions for the Record from Hearing Entitled
"Internet of Things Legislation"
U.S. House Energy and Commerce Committee,
Subcommittee on Digital Commerce and Consumer Protection

Responses from Tim Day
Senior Vice President
Chamber Technology Engagement Center ("C_TEC")
U.S. Chamber of Commerce

July 11, 2018

Questions from Chairman Robert Latta

1. *In your opinion, are current efforts, both in the government and among private groups, on IoT issues siloed? Do you believe the SMART IoT Act will help improve collaboration?*

Answer: C_TEC applauds the efforts of Chairman Latta and the Digital Commerce and Consumer Protection Subcommittee to bring about greater collaboration among agencies with regard to the Internet of Things ("IoT") by introducing the SMART IoT Act. Regulatory certainty provides an environment in which innovation and technology can thrive. When technology developers and producers are subject to a patchwork of vague, duplicative or contradictory agency regulations, the pace of innovation slows.

IoT and other internet-connected technology have changed the regulatory landscape for companies that traditionally were regulated by one agency. Now for instance, a company making a device for connected cars could be subject to consumer protection regulations at the Federal Trade Commission ("FTC"), transportation safety regulations at the National Highway Traffic Safety Administration, and spectrum allocation rules at the Federal Communications Commission ("FCC").

While agencies like the FCC and FTC are working together on issues such as internet regulation,[1] the rise of multi-agency jurisdiction over IoT requires policies that increase collaboration. The SMART IoT Act is a step in the right direction toward providing regulators and industry stakeholders information on which agencies are involved in IoT. This information can also inform Congress on ways to streamline and improve IoT regulation.

> 2. *The SMART IoT Act directs the Secretary of Commerce to conduct a study on the IoT ecosystem—both at the public and private level—so that we can create a single source of information on who is doing what in the IoT space. How do you see this benefiting future policy efforts in this area?*

Answer: C_TEC strongly supports the expansion of publicly available government data to solve our nation's challenges.[2] C_TEC applauds the introduction of the SMART IoT Act and its aim to improve information access to Congress and stakeholders about IoT. The SMART IoT Act has the potential to provide Congress with the information necessary to address conflicting and duplicative regulation by assessing which regulatory bodies are engaging the IoT ecosystem.

Questions from Representative Michael Burgess

> 1. *Sector-based Information Sharing and Analysis Centers (ISAC) have been successful in coordinating information sharing between private sector critical infrastructures and the government. These ISACs help industry protect from cyber and physical threats, as well as coordinate responses with government, when appropriate.*
>
> > a. *Will the study on the internet-connected devices industry evaluate the feasibility of establishing an Internet of Things ISAC?*

Answer: The U.S. Chamber of Commerce believes that it is possible the SMART IoT Act could lead to evaluating the feasibility of establishing an IoT ISAC.

> > b. *Would it be appropriate to recognize the Internet of Things Environment as critical infrastructure? If so, what barriers currently exist?*

Answer: IoT technology will have an enormous impact on the national and world economy. By some accounts, "the IoT has a total potential economic impact of $3.9 trillion to $11 trillion a year by 2025."[3] IoT technology is being deployed to enhance

---

[1] FCC-FTC Memorandum of Understanding (December 14, 2017) *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/fcc_fcc_mou_internet_freedom_order_1214_final_0.pdf.

[2] *See, e.g.* Coalition Letter Supporting OPEN Government Act (April 5, 2017) *available at* http://www2.datainnovation.org/2017-OPEN-gov-data-act-support-letter-full.pdf.

[3] McKinsey Global Institute, Report, Unlocking the Potential of the Internet of Things, at 2 (Jun. 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-ofdigitizing-the-physical-world.

public safety as well. For example, cities are now using IoT technology to detect gunshots.[4] IoT will also greatly assist health care professionals to provide services to patients with geographical barriers.

Recognizing the economic and public welfare benefits of IoT technology, nevertheless the Chamber believes that it is premature, given the nature of this fledgling and diverse technology, to determine whether it would be appropriate to designate the entire IoT ecosystem as critical infrastructure.

> 2. *In the past few years, vulnerabilities in information technology systems and programs have led to large-scale cyber-attacks. Often, devices and applications are produced for government and public use by the same company. Will the results of the study help determine the level of vulnerability in the current Internet of Things environment?*

Answer: The Chamber believes that it is possible that the results of the study directed by the SMART IoT Act will help determine the level of cybersecurity vulnerabilities in the IoT environment. The study could enable Congress and other policymakers to learn from the private sector about how companies are identifying security threats and vulnerabilities.[5]

With regard to IoT, the Chamber's members have developed the following security principles[6]:

- Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and adaptable both overtime and cross-border.
- Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.
- National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.
- Global standards are the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.
- Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.
- Everybody is vulnerable; cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.
- End users need to be educated about their roles and responsibilities in this digital age.

---

[4] Stephen Shankland, "The Internet of Things knows when gunfire happens," CNET (July 27, 2014) *available at* https://www.cnet.com/news/internet-of-things-becomes-gunfire-locating-tool-for-cities/.
[5] *See, e.g.,* Andrew Ross, "Fico release free cyber security ratings service to companies worldwide," Information Age (June 19, 2018) *available at https://www.information-age.com/fico-cyber-security-rating-123473126/;* Brian Nordli, "How engineers at NSS labs put the 'security' in cybersecurity," Built in Austin (May 30, 2018) *available at* https://www.builtinaustin.com/2018/05/30/NSS-Labs-Engineering-Spotlight.
[6] Principles for IoT Security, U.S. Chamber of Commerce (September 19, 2017) *available at* https://www.uschamber.com/IoT-security.

- Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.
- The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the internet and our digital future.
- Governments must work together to shut down illegal activities and bring bad actors to justice.

3. *Earlier this year we held a Disruptor Series hearing that explored manufacturing applications of IoT. Can you explain the potential you see in industrial IoT and how the optimization of manufacturing benefits not only businesses, but also consumers?*

Answer: According to one study by Accenture, the industrial IoT technology has the potential to add at least $10.6 trillion in global GDP by 2030.[7] The Chamber's members have emphasized that manufacturers and their supply chain partners are increasingly recognizing the transformational role of IoT solutions in driving growth and improving performance in several areas including:

- Increasing total production and throughput;
- Improving the ability to adjust fluctuating market demand;
- Increasing the number of product variants;
- Increasing visibility across a given business enterprise; and
- Decreasing the cost of production and eventually, prices to consumers.

All of these benefits converge to drive higher levels of productivity for individual workers, companies, industrial sectors and, over time, the overall American economy. These benefits operate to make the United States a better place to locate manufacturing and other high-wage jobs. This leadership in industrial IoT can be fostered by forward-thinking government policies that can be informed by the SMART IoT Act.

---

[7] Mark Purdy and Ladan Davarzani, "The Growth Game-Change: How the Industrial Internet of Things can Drive Progress and Prosperity," at 5, Accenture (2015) *available at* https://www.accenture.com/t20150523T023647Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Industrial-Internet-of-Things-Institute-Report-2015.pdfla=en.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

June 26, 2018

Ms. Michelle Richardson
Deputy Director
Freedom, Security, and Technology Project
Center for Democracy & Technology
1401 K Street, N.W., Suite 200
Washington, DC 20005

Dear Ms. Richardson:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Tuesday, May 22, 2018, to testify at the hearing entitled "Internet of Things Legislation."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, July 11, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

109

Additional Questions for the Record

Internet of Things Legislation
Before the Subcommittee on Digital Commerce and Consumer Protection
The House Committee on Energy and Commerce

Michelle Richardson, Deputy Director
Freedom, Security, and Technology Project, Center for Democracy and Technology
Submitted July 11, 2018

The Honorable Robert E. Latta

1. In your testimony you state that government should take a soft touch approach to regulating in the technology space, especially when the technology is still developing. Can you explain why a soft touch approach is important?

> Answer: The characteristics that have made the Internet such a success—its open, decentralized, and user-controlled nature and its support for innovation and free expression—may be put at risk by heavy-handed government mandates on the private sector. This is not to suggest that government has no role in shaping the development of the Internet of Things (IoT), but only that it take a nuanced and thoughtful approach in consideration of the diverse entities, services and devices that make up the IoT.

Ideally, IoT developers will adopt privacy and security practices that fairly balance their interests with those of users, and as we testified, we believe this bill would be greatly strengthened by an amendment to ensure that the Secretary investigates the *adoption* of these practices. The nuanced and thoughtful government approach we endorse must start with an understanding of the security and privacy realities of the IoT ecosystem.

2. You state in your testimony that compiling a list of industry-standard setting efforts and government activities that will be created by the SMART IoT Act will help inform future congressional action. Why do you believe gathering such information is critical for future IoT policy?

> Answer: The review conducted under the SMART IoT Act will likely return an extensive list of IoT standards that range from highly technical interoperability requirements to generically desirable privacy and security outcomes. We recommend that Congress focus on culling this list to create minimum privacy and security standards for government procurement of IoT devices. This is the logical next step to implement guidance developed by the Departments of Commerce and Homeland Security, the Office of Management and Budget, and the General Services Administration. It is also timely given the administration's efforts at IT modernization and the expected purchases agencies should be making in the near future. While there are competing, but justified views on government intervention in the private sector, it should be non-controversial

that the government needs to secure its own systems and devices. To accomplish this goal, the government must be able to set the minimum privacy and security standards for the IoT devices it purchases.

We also recommend that the SMART IoT Act review be the jumping off point for more oversight of consumer grade IoT devices. Much of IoT is arguably in the purview of agencies who regulate critical infrastructure, transportation and medical devices, but consumer devices are falling through the cracks of our current sectoral approach.

The Honorable Michael C. Burgess

1.   Sector-based Information Sharing and Analysis Centers (ISAC) have been successful in coordinating information sharing between private sector critical infrastructures and the government. These ISACs help industry protect from cyber and physical threats, as well as coordinate responses with government, when appropriate.

   a.   Will the study on the internet-connected devices industry evaluate the feasibility of establishing an Internet of Things ISAC?

      Answer: The SMART IoT Act draft dated May 15, will not evaluate the feasibility of establishing an Internet of Things ISAC.

   b.   Would it be appropriate to recognize the Internet of Things environment as critical infrastructure? If so, what barriers currently exist?

      Answer: Critical infrastructure is defined as:

      systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[1]

      We do not recommend that the IoT sector be designated as a stand-alone sector. By and large, compromises of IoT devices do not pose the catastrophic effects as contemplated by the standard CI designation. Additionally, IoT devices increasingly pervade most existing CI sectors and to the extent they do, they may be considered within the oversight and regulatory authorities of the sector specific agency already. We expect that the list of government oversight activities in Sections 2(a)(2)-(6) in the SMART IoT Act will include such CI routes to IoT oversight and regulation.

---

[1] 42 U.S.C. § 5195c.

If the designation is under consideration solely or primarily to permit the creation of an ISAC, we note that nothing legally prohibits IoT manufacturers or operators from sharing a lot of information with one another or with the government through more informal means. ISACs are only useful if the participants respond to the unique information they provide. Considering that a significant number of consumer IoT manufacturers use hard coded passwords, fail to offer patches for publicly known security flaws, and/or abandon devices after a short period of time, it is unlikely that many IoT manufacturers would be meaningful participants in an ISAC.

2.   In the past few years, vulnerabilities in information technology systems and programs have led to large-scale cyber-attacks. Often devices and applications are produced and administered for government and public use by the same company.

a.   Will the results of the study help determine the level of vulnerability in the current Internet of Things environment?

Answer: As drafted, the SMART IoT Act will only produce a list of standards, working groups, jurisdictions and similar data points. We recommend that the bill be amended to explicitly require an evaluation of whether these standards are being adopted by the private sector. This is no small task, but the committee could choose a few specific sectors to focus on, such as consumer devices. That would help determine the level of vulnerability of IoT devices in those sectors.

3.   We understand that IoT applications and solutions promise to improve lives and offer societal benefits. Can you highlight current examples of how IoT is doing just that and any future applications you see as offering meaningful benefits?

Answer: CDT is excited to witness and participate in the technological evolution that is changing the world around us. But we believe the many benefits of the IoT will only be stymied by continued security and privacy failures and look forward to working with Congress to building an IoT system that people can trust.

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 26, 2018

Ms. Dipti Vachani
Intel Corporation
Vice President, Internet of Things Group
General Manager, Platform Management and Customer Engineering
2200 Mission College Boulevard
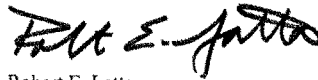Santa Clara, CA 95054

Dear Ms. Vachani:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Tuesday, May 22, 2018, to testify at the hearing entitled "Internet of Things Legislation."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, July 11, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Response of Intel's Dipti Vachani to Additional Questions for the Record

July 11, 2018

The Honorable Robert E. Latta

1. What obstacles do you currently see slowing the progress of IoT adoption and what can Congress do to promote continued innovation in this space?

At Intel, we believe one of the biggest obstacles – and ultimate drivers – for the IoT is scalability across sectors. The adoption of a meaningful National IoT Strategy by the federal government, in partnership with industry, can help address this obstacle and drive U.S. IoT competitiveness. The national strategy should declare IoT investment, innovation and competitiveness a U.S. priority and set forth an expeditious process and timeline for adoption of IoT technology across key market sectors. Intel believes that collaboration between government and industry is critical to address IoT scalability and expedite broader adoption of IoT solutions in America. Without a clear strategic vision, the U.S. risks falling behind other countries in reaping the vast economic and societal benefits of the IoT, along with the benefits that accrue from creating and owning the expertise driving the global IoT ecosystem. A national plan with concrete milestones will ensure that the U.S. leads the world – and increases GDP from the IoT – for decades to come. Moreover, coordination across government agencies is essential to prevent a patchwork of inconsistent policies which could disrupt IoT's transformative potential. The Secretary of Commerce's recommendations to Congress, pursuant to the SMART IOT Act, should provide the framework for working with industry to timely develop and adopt an impactful U.S. National IoT Strategy, including promoting *scalable* federal government IoT projects and investment aligned with agency missions that can highlight U.S leadership and demonstrate the benefits of IoT use cases.

The Honorable Michael C. Burgess

1. Sector-based Information Sharing and Analysis Centers (ISAC) have been successful in coordinating information sharing between private sector critical infrastructures and the government. These ISACs help industry protect from cyber and physical threats, as well as coordinate responses with government, when appropriate.

   a. Will the study on the internet-connected devices industry evaluate the feasibility of establishing an Internet of Things ISAC?

We concur with your assessment that ISACs have been successful in many instances in coordinating information sharing between private sector critical infrastructures and the government. Indeed, Intel and the technology industry contribute to significant cybersecurity public-private partnerships with the federal government, including information sharing, analysis, and emergency response. Examples include the DoD's Defense Industrial Base Cybersecurity Informational Sharing Program (cybersecurity information sharing and incident reporting); the Information Technology Information Sharing and Analysis Center (sharing of cybersecurity threats and insights); and DHS' Sector Coordinating Councils (coordination of critical infrastructure security and resilience).

The IoT study prescribed in the SMART IOT Act focuses on cataloguing industry stakeholders, including those who develop IoT devices, government agencies with jurisdiction over industry sectors engaged in IoT, a comprehensive list of public-private partnerships focused on IoT, industry bodies engaged in establishing regulations, guidelines and best practices that pertain to IoT. The collection of this data, along with the continued coordination and collaboration of the public and private sectors on federal IoT policy and adoption, is an appropriate first step when considering the feasibility of establishing an IoT ISAC or whether sector-specific ISACs similar to the examples above may be more actionable given the breadth of the IoT.

    b. Would it be appropriate to recognize the Internet of Things environment as critical infrastructure? If so, what barriers currently exist?

While some parts of the IoT are included in sectors defined as critical infrastructure, other are not. For example, both a smart thermostat in a home and the smart grid are considered part of the IoT environment, but only the latter is considered critical infrastructure by DHS.

2. In the past few years, vulnerabilities in information technology systems and programs have led to large-scale cyber-attacks. Often devices and applications are produced and administered for government and public use by the same company.

    a. Will the results of the study help determine the level of vulnerability in the current Internet of Things environment?

The SMART IOT Act directs the Secretary of Commerce to develop the IoT study and provide recommendations to Congress, among which could be laying the groundwork to help determine vulnerabilities should the Secretary recommend this. Most important in this effort,

the federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats and continually develop best practices for IoT security.

The Department of Commerce and its agencies, such as the National Institute of Standards and Technology (NIST) and the National Telecommunications Industry Administration (NTIA), as well as the Department of Homeland Security (DHS), are appropriate entities for such efforts. Intel participated(es) in NIST's Cyber-Physical Systems Public Working Group including the cybersecurity subgroup, as well as NTIA's multi-stakeholder processes on Cybersecurity Vulnerabilities and IoT Security Upgradability and Patching. These are examples of public-private collaboration to address important security needs, while maintaining the necessary flexibility to adapt to new threats that rigid regulatory approaches would not provide.

Congress also should urge the Federal Trade Commission, Small Business Administration and Federal Communications Commission – with input from industry – to develop complementary cybersecurity "hygiene" education and awareness outreach initiatives for consumers and small businesses.

3.   In your testimony you spoke about IoT and what it means for healthcare. As an OBGYN and Chairman of the Health Subcommittee, I am interested to learn more about Sickbay and what it is doing at Texas Children's Hospital. Can you talk a little bit about the health monitoring they are doing? I'm interested to hear how this is impacting patient care.

Intel shares your interest in the application of IoT technology to improve patient-centered care. IoT solution Sickbay, an FDA-cleared Clinical Intelligence Platform, is using Intel technology to enable real-time, data-driven medicine. The Sickbay platform continuously captures patients' bedside data from any medical device or system and transforms that data into web-based clinical applications that make data actionable -- enabling patient care teams to make better, faster decisions. This allows medical teams to predict patient health deterioration before it occurs and ultimately save lives. The solution has been implemented at six healthcare institutions to date. Texas Children's Hospital pioneered the creation of a remote consult room that enables the viewing of real-time data from cardiac monitors and vents. Texas Children's Hospital has used Sickbay to collect data on 302 beds over 4.5 years, which included 2.1 million patients. More information is available on our website at: https://solutionsdirectory.intel.com/solutions-directory/sickbay-clinical-intelligence-platform.