# DISRUPTER SERIES: THE INTERNET OF THINGS, MANUFACTURING AND INNOVATION

## 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

JANUARY 18, 2018

**Serial No. 115–91**

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

U.S. GOVERNMENT PUBLISHING OFFICE
29–593 WASHINGTON : 2018

## 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 LUJAN, 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 Virgina
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 LUJAN, New Mexico
YVETTE D. CLARKE, New York
TONY CARDENAS, 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)*

# CONTENTS

# DISRUPTER SERIES: THE INTERNET OF THINGS, MANUFACTURING AND INNOVATION

**THURSDAY, JANUARY 18, 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 10:04 a.m., in room 2123 Rayburn House Office Building, Hon. Robert Latta (chairman of the subcommittee) presiding.

Members present: Representatives Latta, Kinzinger, Burgess, Upton, Lance, Guthrie, Bilirakis, Bucshon, Walters, Costello, Duncan, Schakowsky, Clarke, Cárdenas, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Staff present: Karen Christian, General Counsel; Margaret Tucker Fogarty, Staff Assistant; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight & Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Katie McKeogh, Press Assistant; Alex Miller, Video Production Aide and Press Assistant; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Hamlin Wade, Special Advisor, External Affairs; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Evan Gilbert, Minority Press Assistant; 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. The chair now recognizes himself for 5 minutes for an opening statement.

And, again, good morning and welcome to the first Disrupter Series hearing in 2018. Today, we are continuing the subcommittee's efforts to examine new and innovative technologies while learning directly from companies about what opportunities they see 5 to 10 years in the future.

I'd like to thank all of our witnesses for being with us today and highlight that Owens-Illinois is headquartered in my district in Perrysburg, Ohio and I've been—we have held two roundtables on IoT and cybersecurity issues with local businesses at your headquarters and I appreciate that.

Last summer, this subcommittee hosted a showcase with IoT companies for many of our member districts. We also held a hearing about how the IoT and interconnected network of physical objects embedded with sensors and communication devices that exchange information can improve productivity, increase response times, drive down costs, and benefit consumers. Today, we will discuss how IoT is making American manufacturing more competitive and how innovation is improving the lives of Americans. We will also learn about barriers to the continued expansion of IoT and what policy makers should keep in mind as the use of IoT expands.

The ability of devices to communicate with other devices is revolutionizing industrial practices both in the United States and abroad. Already there are examples of smart components sending data about their performance and condition to workers who can monitor the equipment and if necessary replace it before it breaks down. Municipal water systems embedded with sensors can relay information about blockages or leaks that would help ensure that the water keeps flowing. Another example is how electricity providers can monitor electrical grids embedded with sensors and relays that can identify outages or surges, locate alternative pathways, and ensure that electrons keep flowing.

Looking forward, the potential to further improve manufacturing processes through the combination of new technologies stretches the imagination. Utilizing IoT and other emerging technologies like augmented reality, workers will be able to virtually make adjustments to industrial systems to understand how to improve efficiency and then implement necessary changes without interrupting the manufacturing processes. IoT-connected factories will be able to monitor their need for raw materials and then order those materials from IoT-connected warehouses. IoT-connected transportation service providers will then deliver necessary products without the intervention of the human. These and other opportunities allow IoT-connected manufacturing centers the ability to devise their own ways to run more smoothly.

Expansion-smart industrial processes will continue to create historic changes in how American companies build and deliver products. More efficient factories means that consumers will have more choices for the goods they purchase while being able to retain them at a lower cost. At the same time, like all new technologies, IoT will create disruption in the manufacturing economy. This disruption will create the need for new ways of educating and preparing our workforce both now and in the future.

In addition, cybersecurity issues remain an ever present concern for an internet-connected service and the IoT is no different. Constant vigilance and improved coordination will be required to ensure that bad actors don't take advantage of the weaknesses in IT security policies.

Today, we look forward to our witnesses describing how IoT is being leveraged in their facilities to improve manufacturing proc-

esses, how to address concerns around cybersecurity, how this technology is likely to develop in the future, and what policymakers can do to help promote continued innovation in American manufacturing.

And with that, I will yield back the balance of my time and now 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:]

OPENING STATEMENT OF HON. ROBERT E. LATTA

Good Morning, and welcome to the first Disrupter Series hearing in 2018. Today, we are continuing this Subcommittee's efforts to examine new and innovative technologies, while learning directly from companies about what opportunities they see 5 to 10 years in the future.

Last summer, this subcommittee hosted a showcase with IoT companies from many of our Members' districts. We also held a hearing about how the IoT, an interconnected network of physical objects embedded with sensors and communications devices that exchange information, can improve productivity, increase response times, drive down costs, and benefit consumers. Today, we will discuss how the IoT has made American manufacturing more competitive and how innovation is improving the lives of Americans. We will also hear about barriers to continued expansion of the IoT, and what policymakers should keep in mind as use of the IoT expands.

The ability of devices to communicate with other devices is revolutionizing industrial practices both in the U.S. and abroad. Already there are examples of smart components sending data about their performance and condition to workers, who can monitor the equipment and if necessary, replace it before it breaks down. Oil and gas pipelines, embedded with sensors, can relay information about bottlenecks or low pressure that will help ensure energy keeps flowing. Inventory and product is monitored in real time, finding more efficient routes and ensuring goods are delivered when and where they are needed.

Looking forward, the potential to further improve manufacturing processes through the combination of new technologies stretches the imagination. Utilizing the IoT and other emerging technologies like augmented reality, workers will be able to virtually make adjustments to industrial systems to understand how to improve efficiency, and then implement necessary changes, without interrupting the manufacturing process. IoT connected factories will be able to monitor their need for raw materials, and then order those materials from IoT connected warehouses, which will communicate with IoT connected transportation service providers to deliver necessary products without the intervention of a human. IoT connected manufacturing centers will be able to devise their own ways to run more smoothly.

The expansion of smart industrial processes will continue to create historic changes in how American companies build and deliver products. More efficient factories mean that consumers will have more choices for the goods they purchase, while being able to obtain them at lower cost. At the same time, like all new technologies the IoT will create disruption in the manufacturing economy. This disruption will create the need for new ways of educating and preparing our workforce, both now and for the future.

In addition, cybersecurity issues will remain an ever present concern for any internet connected service, and the IoT is no different. Constant vigilance and improved coordination will be required to ensure that bad actors don't take advantage of weaknesses in IT security policies.

Today we look forward to our witnesses describing how the IoT is being leveraged at their companies to improve manufacturing processes, how to address concerns around cybersecurity, how this technology is likely to develop in the future, and what policymakers can do help promote continued innovation in American manufacturing.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

The Internet of Things, of course, has tremendous potential to change manufacturing in the United States. Smart manufacturing can help businesses save resources, improve performance, and expand consumer choice. For example, a senior can remove the need for a human worker to physically check a machine. I didn't mean a senior. I meant a sensor. A sensor can remove the need for a human worker to physical check a machine, assuming everything works correctly. That sensor makes the worker's job easier and reduces the opportunity for human error.

As the Internet of Things evolves, even more and more processes can be automated and this raises some familiar issues for subcommittee—privacy, cybersecurity, safety, and labor market impacts. Advanced manufacturing requires a different set of skills than the production line of previous generations and workers must be trained for these jobs, and we need to be responsive to the needs of workers who may be displaced by changes in manufacturing.

We must also be mindful of accessibility. I think back to the autonomous vehicle legislation that the House passed last year that this committee worked on. Self-driving cars promise to open up new opportunities to those with disabilities. That's great. But some of those vehicles need to be accessible for people in wheelchairs, for instance, so that we can fully realize the potential to improve mobility. The same goes for manufacturing workers. Depending on how the technology is designed and integrated, bringing the Internet of Things into manufacturing could either expand or limit job opportunities for those, for example, with visual impairments or physical disabilities. In addition, we must ensure that businesses can get the full benefit of smart manufacturing. Often, a prerequisite for businesses to integrate new technologies is the broadband to support it.

Last year, Democrats on the Energy and Commerce Committee unveiled a comprehensive infrastructure package—the LIFT America Act, which included a $40 billion investment in secure and reliable broadband. A serious infrastructure bill takes real dollars and I hope that we can work together to advance that type of job-creating legislation.

I would also note that some of the advances we see in the manufacturing stem for research supported by the federal government. For example, President Obama established a national network for manufacturing innovation which included the Digital Manufacturing and Design Innovation Institute in Chicago, which I have visited. The Trump budget eliminates funding for the Manufacturing Institutes. The U.S. can only lead in research if we invest in research.

We need a bipartisan deal to raise the budget caps on both the defense and non-defense side so that important investments in infrastructure and innovation can continue.

I thank you, and I yield back, unless there is anybody who wants my remaining time. OK. I yield back.

Thank you.

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

The chairman of the full committee has not arrived yet. But is there anyone on the Republican side wishing to claim that time?

Not hearing anyone, the chair now recognizes the ranking member of the full committee, the gentleman from New Jersey, 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.

Since 2015, this subcommittee has been examining the opportunities and challenges of the Internet of Things, from autonomous vehicles to wearable technology. But the Internet of Things extends beyond consumer products. It can be found across industries including in the energy, healthcare, and transportation sectors, and today we will discuss how it can help make manufacturing more efficient, more productive, and more safe.

The Internet of Things is used in smart manufacturing to make real-time control of production possible. Companies report that using smart manufacturing technologies lowers their energy use, reduces waste, improves product quality, and saves money, and with more efficient manufacturing we see less pollution, fewer health issues for our work force, and more opportunities for good technology-based jobs.

As with all connected technologies, strong cybersecurity is essential to successful smart manufacturing. While the Internet of Things helps ensure that a manufacturer is monitoring, measuring, and sensing control systems work together, one weak point can affect the whole network. Imagine the potential consequences if a malicious actor brought down automated manufacturing at a pharmaceutical plant that makes vaccines or if network disruptions affect the quality control monitoring for seatbelts at an auto plant.

Experts have found that companies in the U.S. are not doing enough to address these risks and that a strong comprehensive framework for cybersecurity in manufacturing is urgently needed. And also, unlike our smart phones, which seem to be replaced every few years, large machinery is used for decades, adding to the difficulty of ensuring they are consistently and properly updated for security vulnerabilities. And I have said at previous hearings on automation that we should not be scared of these new technologies but we must realize their potential effect on jobs. To stay competitive, we must ensure that employers are prepared for the changing workplace and we need to invest more in research and development so that the U.S. continues to lead the world in innovation.

For years, we have listened to experienced witnesses in industry, academia, and government tell us that federal investment is vital if you want to keep making things in America. Unfortunately, the Trump administration proposed a budget last year that eliminates dozens of essential successful programs that make manufacturing innovation possible and provides support for U.S. factory workers. Moreover, industry witnesses repeatedly tell us what they really need is stability. Yet, Republicans have repeatedly failed to pass final appropriation bills for the fiscal year that began on October 1st and we are once again at a deadline tomorrow. It appears that Republicans are going to try once again to kick the can down the road. And with this delay, Republicans are adding even more insta-

bility, ultimately hurting American manufacturers and workers. I think those delays must end, but we will see.

And I would like to yield the remainder of my time to the gentlewoman from California.

Ms. MATSUI. Thank you, Ranking Member Pallone.

The Internet of Things and the industrial Internet of Things represents a shift in how companies and manufacturers interact with data. Smart manufacturing enables real-time monitoring and tracking of a company's assets through the manufacturing process. New technologies and tools can be critical to the means of facilitating the efficiencies promised by Industry 4.0. Of course, connectivity is a cornerstone of the next industrial revolution and wireless connectivity depends on the availability of spectrum.

I believe that technologies like block chain could play an interesting role in both spectrum sharing to potentially maximize efficient use of spectrum bands and as a means of tracking digital records in real time.

Thank you, and I look forward to the witnesses, and I yield back.

Mr. PALLONE. And I yield back, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman yields back the balance of this time. This concludes member opening statements.

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

Again, I want to thank all of our witnesses for being with us today. We appreciate you taking time to testify before us and it's very important to hear from you and your testimony.

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

Our witness panel for today's hearing will include Mr. Rodney Masney, the Vice President of Technology and Service Delivery Information of Technology at Owens-Illinois; Mr. Thomas Bianculli, Chief Technology Officer at Zebra Technologies Corporation; Dr. Thomas R. Kurfess, Professor and HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control at the George W. Woodruff School of Mechanical Engineering at Georgia Institute of Technology; and Mr. Sanjay Poonen, the Chief Operating Officer at VMWare.

So we really appreciate you all being with us today and, Mr. Masney, you are recognized for your opening statement for 5 minutes.

Thanks again for being with us.

**STATEMENTS OF RODNEY MASNEY, VICE PRESIDENT, TECHNOLOGY SERVICE DELIVERY, INFORMATION TECHNOLOGY, OWENS-ILLINOIS; THOMAS D. BIANCULLI, CHIEF TECHNOLOGY OFFICER, ZEBRA TECHNOLOGIES CORPORATION; DR. THOMAS R. KURFESS, PROFESSOR AND CHAIR IN FLUID POWER AND MOTION CONTROL, GEORGE W. WOODRUFF SCHOOL OF MECHANICAL ENGINEERING, GEORGIA INSTITUTE OF TECHNOLOGY; SANJAY POONEN, CHIEF OPERATING OFFICER, VMWARE**

**STATEMENT OF MR. MASNEY**

Mr. MASNEY. Good morning to the members of the committee and to my colleagues who have travelled to Washington today to discuss the importance of the Internet of Things.

Before I begin, I would like to thank Congressman Latta for his continued leadership and engagement on the issue. I also want to thank the committee for the opportunity to discuss IoT, which is important to U.S. manufacturing and my company specifically.

Owens-Illinois, headquartered in Perrysburg, Ohio, is the world's largest manufacturer of glass containers, serving globally recognized brands throughout the world. Our company operates 79 manufacturing plants throughout the world, 17 of which are located in the United States. Glass making has historically been a trade where craftspersons and apprentices would develop expertise in the art of glass making.

At the turn of the century, Michael Owens invented automated glass manufacturing, which was a huge step change in productivity and worker safety. While the glass making process is highly automated today, the industry is poised for the next step change, which will come from the factory becoming increasingly connected with IoT technologies throughout the end-to-end process. The information collected through IoT technology will be used to transform the craft of glass making to that of data-driven science which will enhance the competitive position of glass in the global packaging industry.

Glass containers are the most sustainable option in the competitive packaging landscape with a life cycle that goes from cradle to cradle, reusable in many markets and infinitely recyclable into either new glass containers or other products. Glass is truly the sustainable packaging option. Owens-Illinois is on an IoT journey, which will transform our manufacturing process and add value to the products and services that we sell our customers.

There are several IoT areas of focus for OI. Improve manufacturing performance through higher yields, increase quality, and reduce costs. IoT will deliver deeper insights into our end-to-end manufacturing process. The data generated from sensors in the plant will provide insights into environmental conditions, process settings, and control variances, enhancing our ability to increase first-time yields and improve quality. This work will require skilled engineers, information technology professionals, and data scientists. The data required through IoT will be used to reduce reaction time in the plants and allow us to adjust the process if controls are slipping out of tolerance.

Addressing the variations in manufacturing process will be realized in a more proactive manner. The IoT platform will transform the glass manufacturing process from one of reactivity to one that is proactive and highly automated. The information generated by new sensor technology, data science, and information automation will increase yields and improve quality while achieving reduced costs and enhancing OI's ability to compete in the U.S. and global markets.

Energy management and predictive maintenance are the second area of IoT development OI is pursuing. It takes a great deal of energy to melt and form glass and to operate a glass container manufacturing facility. Developing sensor technology can help glass containers maintain the status of the most sustainable packaging solution and reduce energy used to operate our furnaces. Advanced sensor technologies can also be used to collect information while monitoring equipment throughout the manufacturing facility and could be critical to seeking new ways to maintain equipment.

IoT technologies and the concepts around IoT is enabling OI to also create and develop new and differentiated products and services for our customers with the goal to ensure the integrity, safety, and authenticity of its contents.

I would like to highlight the several concerns regarding successful deployment and sustainability of IoT. Because the achievable deployment of IoT throughout an enterprise can be quite daunting, a successful deployment of IoT requires sensors, PLCs, IT systems, networking, massive amounts of storage and software to achieve the desired business outcomes.

Seeking ways to make these investments more affordable can be a way to help U.S. manufacturing accelerate its investments in IoT technologies. Protecting against cybersecurity risks will become more critical while manufacturers deploy IoT in facilities. Manufacturing equipment devices, sensors, and control systems that previously may have been standalone, maybe exposed, not just within a plant location but also potentially throughout an enterprise.

Cybersecurity-related disruptions could cause unplanned down time or impair productivity. Cybersecurity attacks could also put health and safety of employees at risk.

Data scientists are in short supply and high demand. Transformation of the workforce becomes more critical. Tomorrow's manufacturing workforce must be increasingly knowledgeable about the use of information technology. Engineering disciplines and information technology skills will be needed to deliver and sustain these solutions.

The use of business intelligence analytics and the role of data scientists will be critical to success of IoT.

In conclusion, as manufacturers continue on the IoT journey, Congress may want to look into the following ways to help foster growth of IoT technology and its use, assist manufacturers and making IoT technologies more affordable by encouraging research and investment in these capabilities or in programs which encourage manufacturing companies to deploy IoT or programs and resources that address cybersecurity in U.S. businesses and encourage more research in the IoT data science discipline and seek ways

to encourage a supporting pipeline of skilled workers through universities and manufacturing and related technical schools.

Thank you for your time and attention.

[The prepared statement of Mr. Masney follows:]

Disrupter Series: The Internet of Things, Manufacturing and Innovation

Rodney Masney

Vice President, Technology Service Delivery, Information Technology

Owens-Illinois, Inc.

Good morning to the members of the Committee and to my colleagues who have come to Washington to discuss the importance of the Internet of Things (IOT). Before I begin, I would like to thank Congressman Latta for his continued leadership and engagement on this issue. I also want to thank the committee for the opportunity to discuss why IOT is important to US manufacturing companies and my company, Owens-Illinois.

Owens-Illinois, headquartered in Perrysburg, Ohio, is the world's largest manufacturer of glass containers serving globally recognized brands. Our company operates 79 manufacturing plants throughout the world, 17 of which are located in the United States.

Glassmaking has historically been a trade where master craft-persons and apprentices would develop expertise on the art of glassmaking. At the turn

of the century, Michael Owens invented automated glass manufacturing which was a huge step change in productivity and worker safety. While the glassmaking process is highly automated, the industry is poised for the next step change, which will come from the factory becoming increasingly connected with IOT technologies throughout the end-to-end processes.

The information collected through IOT technology will be used to transform the "craft" of glass making to that of a data driven science, which will enhance the competitive position of glass in the global packaging industry.

Glass containers are the most sustainable option in the competitive packaging landscape with a lifecycle that goes from "cradle to cradle." Reusable in many markets and infinitely recyclable into new glass containers or other products, glass is the true sustainable packaging option.

Owens-Illinois is on an IOT journey, which will transform our manufacturing process and add value to the products and services that we sell our customers.

There are several IOT areas of focus for O-I:

1. Improved manufacturing performance through higher yields, increased quality, and reduced costs.
    a. IOT will deliver deeper insights into our end-to-end manufacturing process. The data generated from sensors in the plants will provide insights into environmental conditions, process settings, and control variances enhancing our ability to increase first-time yields and improve quality. This work will require skilled engineers, information technology professionals and data scientists.
    b. The data acquired through IOT will be used to reduce reaction time in the plants and allow us to adjust the process if the controls are slipping out of tolerance. Addressing the variations in the manufacturing process will be realized in a more proactive manner.
    c. The IOT platform will transform the glass manufacturing process from one of reactivity to one that that is proactive and highly automated. The information generated by new sensor technology, data science, and manufacturing automation will increase yields, and improve quality while achieving reduced

costs and enhancing O-I's ability to compete in the US and global markets.

2. Energy management and predictive maintenance are the second area of IOT development O-I is pursuing.
    a. It takes a great deal of energy to melt and form glass and to operate a glass container manufacturing facility. Developing sensor technology can help glass containers maintain the status of the most sustainable packaging solution and reduce energy used to operate a furnace.
    b. Advanced sensor technologies can also be used to collect information while monitoring equipment throughout the manufacturing facility and could be critical to seeking new ways to maintain equipment.
3. IOT technologies and technological adjacencies is enabling O-I to develop new and differentiated products and services for our customers with the goal to ensure the integrity, safety and authenticity of the contents.

I would like to highlight several concerns regarding the successful deployment, and sustainability, of IOT.

1. The cost to achieve a full deployment of IOT throughout an enterprise can be quite daunting. A successful deployment of IOT requires sensors, PLC's, IT systems, networking, massive amounts of storage, and software to achieve the desired business outcomes. Seeking ways to make these investments more affordable can be a way to help US manufacturing accelerate its investment in IOT technologies.
2. Protecting against cybersecurity risks will become more critical while manufacturers deploy IOT in facilities. Manufacturing equipment, devices, sensors and control systems that previously may have been standalone may be exposed not just within a plant location but also potentially throughout an enterprise. Cybersecurity related disruptions could cause unplanned downtime or impair productivity. Cybersecurity attacks could also put the health and safety of people at risk.
3. Data scientists are in short supply and high demand and transformation of the work force becomes more critical. Tomorrow's manufacturing workforce must be increasingly knowledgeable about the use of information technology. Engineering disciplines and information technology skills will be needed to deliver and sustain

these solutions. The use of business intelligence, analytics and the role of the data scientist will be critical to the success of IOT.

In conclusion, as manufacturers continue on the IOT journey, Congress may want to look into the following areas to help foster the growth of IOT technology and use in the years ahead:

1. Assist manufacturers in making IOT technologies more affordable by encouraging research and investment in these capabilities or in programs which encourage manufacturing companies to deploy IOT solutions.
2. Support programs or resources that address cybersecurity in US businesses.
3. Encourage more research in the IOT data science discipline and seek ways to encourage a supporting pipeline of skilled workers through universities and manufacturing related technical schools.

Thank for your time and attention.

Mr. LATTA. Well, thank you very much.

And Mr. Bianculli, you are recognized for 5 minutes. Thank you very much for being with us.

**STATEMENT OF MR. BIANCULLI**

Mr. BIANCULLI. Thank you, Chairman Latta, Ranking Member Schakowsky, and members of the subcommittee for the opportunity to testify before you today.

I am Thomas Bianculli, the Chief Technology Officer of Zebra Technologies Corporation, and we are a global leader in bringing Internet of Things solutions to business-to-business and business-to-government markets.

With approximately $3.7 billion in revenue, nearly 7,000 employees, and doing business in more than 40 countries, Zebra is a trusted partner to more than 95 percent of all Fortune 500 companies.

And while many Americans may not know us by name, I am sure they come into contact with our solutions every day. For example, the bar code labels that are printed and applied to airline baggage tags or express delivery packages and pharmaceutical prescription bottles are often generated by a Zebra bar code label printer and tracked and managed by Zebra bar code scanning technology and mobile computers.

Similarly, manufacturing, warehouse, and delivery workers as well as countless healthcare workers across the globe employ our mobile computing devices in their daily work to increase efficiency, reduce errors, and drive a better customer experience.

Overall, what we see in the marketplace every day tells us that manufacturers and their supply chain partners are increasingly recognizing the transformational role of industrial IoT. Solutions in driving growth and improving performance in several key areas of business activity including increased total production and through put, improved ability to adjust to fluctuating market demand, and increased ability to produce a greater number of product variance, and increased visibility into operations across a given business enterprise, and a decreasing cost of production. All of these advances reflect the fact that, at its heart, the IoT revolution is a dramatic change in advancement in the way companies capture and ultimately share data.

The ability to have data about inventory that's immediately available to both plant floor managers and suppliers is providing new levels of visibility that heightens operational performance and from the greater visibility comes the great advances we are seeing in manufacturing across a wide array of industries.

In the opening comments from Chairman Latta, I heard mention of augmented reality and wearable technology. I think we should really keep that in mind as we see industrial Internet of Things creating more and more data. There is the opportunity to collect that data, analyze that data, and then use that information to inform a worker. And as we are starting to see that occur, we are seeing that mobile and computing technologies migrate from an interface that is handheld to interfaces that become heads up and are able to augment our physical reality with digital information that helps U.S. citizens and U.S. workers just get the job done. And I think that's an incredible opportunity for competitive advantage

for us to help drive efficiency and to lead the world by way of example in that regard.

Whirlpool Corporation wanted to optimize mobile device management at its distribution centers as a way of enhancing productivity. They were experiencing problems with misplaced devices, battery life, the inability to update devices in a systemic way, and a lack of data metrics around device performance. It needed a centralized management system to track device health, productivity, location, and ensure proper deployment. To solve their problem, Zebra worked with Whirlpool to employ an IoT-based solution which uses our mobile computers connected to their vehicle-mount computers and our handheld devices.

We connected all of their devices back to the cloud across all of their facilities. We are able to manage to predictably detect when batteries may need replacing, when the performance and health of applications on the device, the resiliency and security of the network, and by monitoring all that information in near real time we can detect and proactively intercede if we see that a device is going to have a problem, thereby driving up the overall worker efficiency and uptime of their operations.

Congress can play an important role in helping to ensure that all companies across America can successfully employ industrial IoT-based solutions. Specifically, we urge you and your colleagues to support infrastructure legislation that promotes the deployment of mobile broadband networks as well as directs the NTIA and FCC to allocate more commercial licensed and unlicensed spectrum in a technology-neutral way. Additionally, we urge Congress to advance policies that will help assure coordination among government agencies so that regulation of IoT does not needlessly impede innovation.

In sum, Mr. Chairman, we commend the subcommittee for holding this hearing, for your ongoing efforts to ensure that American industry has the ability to continue to roll out new technologies that will improve the lives of both our workers and our citizens.

IoT presents a transformative opportunity, some calling it the fourth industrial revolution, the advent of cyber physical systems that will create opportunity for jobs of all types and sizes across the United States to work smarter, be more productive, and help improve the overall American economy.

At Zebra, we are committed to bringing IoT solutions to companies to help them achieve their goals. We look forward to continuing to work with the subcommittee and I thank you for the opportunity to share a Zebra story, and I am happy to answer any questions you and your colleagues may have.

Thank you.

[The prepared statement of Mr. Bianculli follows:]

Testimony of

Mr. Thomas D. Bianculli
Chief Technology Officer
Zebra Technologies Corporation

Before the
Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy & Commerce
U.S. House of Representatives

"Disrupter Series: The Internet of Things, Manufacturing and Innovation"

January 18, 2018

## Introduction

Thank you, Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, for the opportunity to testify before you today. My name is Tom Bianculli and I am the Chief Technology Officer for Zebra Technologies Corporation. Zebra is a global leader in bringing Internet of Things (IoT) solutions to Business-to-Business (B2B) and Business-to-Government (B2G) markets.

With revenues of approximately $3.7 billion and almost 7,000 employees in more than 40 countries, Zebra is a trusted business partner to more than 95 percent of all Fortune 500 companies. However, Mr. Chairman, I recognize that many Americans may not know Zebra by name but I am sure they come into contact with our solutions every day. For example, the barcode labels that are prominently featured on airline bag tags, express delivery packages, and pharmaceutical prescription bottles are often generated by a Zebra barcode label printer and tracked and managed by a Zebra scanner. Factory, warehouse and delivery workers as well as countless healthcare workers across the globe employ our mobile computing devices daily in their work.

## Overview

My testimony today reflects the contents of a soon-to-be-released White Paper entitled the "2017 Manufacturing Vision Study"[1] and provides Zebra's views on how the Internet of Things (IoT) – or, more specifically, the Industrial Internet of Things (IIoT) – will impact manufacturing and innovation.

[1] The Zebra 2017 Manufacturing Vision Study is the result of a global study Zebra commissioned last year to analyze the trends, opportunities, and challenges related to IIoT solutions in manufacturing. It includes the insights of 1,100 executives from automotive, high tech, food, beverage, tobacco, and pharmaceutical companies on the role and importance of adopting technology on the plant floor that increases overall company competitiveness.

As a starting point for my testimony and to assure a common definition, Zebra describes IIoT as those technologies which enable businesses to track critical assets and events within their operations and know exactly what they are, where they are and their condition so they can make smarter, faster decisions that improve the bottom line. IIoT leverages and recognizes the fact that people, assets and devices – especially mobile devices – are becoming increasingly connected and that this trend is advancing quickly. A few key facts help illustrate this point:

- By 2020, there will be 1.75 billion global mobile workers accounting for 42% of the global workforce.[2]

- By 2020, there will be 21 billion connected devices in a global Internet of Things.[3]

- By 2020, there will be 44 zettabytes of data with 10% of it coming from the Internet of Things.[4]

As a result of these trends, Zebra is working with companies around the world to provide solutions which yield real-time visibility into their processes, assets and people. The key elements which enable this work include:[5]

- Sense. The employment of unrivaled expertise in sensor and device connectivity enables companies to inter-connect devices to software and to mobile workers so that decision makers and workers alike have substantially more real-time visibility into operations.

- Analyze. Equally important, the provision of easy access to an unprecedented amount of data that IIoT enables allows companies to plan more effective short- and long-term

---

2 Source: Strategy Analytics as cited in *Visibility That's Visionary*, Zebra Technologies Corporation (May 31, 2016, 11:15 AM), https://www.zebra.com/content/dam/zebra_new_ia/en-us/campaigns/brand-campaign/zebra-visibility-vision-report-en-us.pdf.

3 Source: Gartner Group as cited in *Visibility That's Visionary*, Zebra Technologies Corporation (May 31, 2016, 11:15 AM), https://www.zebra.com/content/dam/zebra_new_ia/en-us/campaigns/brand-campaign/zebra-visibility-vision-report-en-us.pdf.

4 Source: Digital Universe Study as cited in *Visibility That's Visionary*, Zebra Technologies Corporation (May 31, 2016, 11:15 AM), https://www.zebra.com/content/dam/zebra_new_ia/en-us/campaigns/brand-campaign/zebra-visibility-vision-report-en-us.pdf.

5 Source: Zebra Technologies Corporation, *Visibility That's Visionary*, (May 31, 2016, 11:15 AM), https://www.zebra.com/us/en/cpn/visibility.html.

strategies by delivering real-time insights into the critical data captured by the sensors in connected devices.

- Act. The explosive growth of mobile devices across the private, public and non-profit sectors enables management and workers at all levels to act on these visibility-driven insights in real-time, anytime and everywhere.

Both our experience and the findings of our 2017 Manufacturing Vision Study tell us that manufacturers and their supply chain partners are increasingly recognizing the transformational role of IIoT solutions in driving growth and improving performance in several areas including:

- Increasing total production and throughput.
- Improving the ability to adjust to fluctuating market demand.
- Increasing the number of product variants.
- Increasing visibility across a given business enterprise.
- Decreasing the cost of production.

The balance of my statement examines these issues in greater detail by discussing the elements and application of IIoT to manufacturing, including:

- The State of the Manufacturing Industry.
- The Benefits and Rising Importance of IIoT.
- The Challenges of Fully Deploying IIoT.
- IIoT Deployment Drivers:
    - Quality Management.
    - Creating Increasing Tracking Points in Manufacturing.
    - The Demands of Industry 4.0.
    - The Importance of Expanding Functionality.
    - The Value of Leveraging Technology to Realize Greater Growth.
- IIoT in American Manufacturing.
- Policy Recommendations.

**State of the Industry**

The global manufacturing industry is in the midst of a dramatic transformation that will profoundly alter plant floor operations. With a desire to connect every stage of the manufacturing process – including end-to-end supply chain fulfillment – manufacturers are turning to automation to improve quality and gain unprecedented visibility. Driven in large measure by globalization, intensifying competition and, perhaps most importantly, increasingly complex bills of materials due to rising customer demands for product variety, a connected plant floor has become a necessity to ensuring high-quality products.

Moreover, and for the first time in decades, investment decisions are no longer being driven primarily by short-term Return on Investment (ROI) calculations but also, increasingly, by long-term quality performance metrics. Companies simply can't afford to produce defective or sub-

standard products and maintain their competitive edge. The cost of poor quality in terms of scrap, reworks, returns, and defects is simply too high.

Add to these challenges the adverse impact of customer complaints, a lack of customer confidence and, ultimately, the loss of brand loyalty, and it's evident that poor quality products can cause irreparable damage to a company's reputation. As a result, manufacturers and their suppliers are making changes to their plant floor operations and moving toward a fully connected, smart factory as a way of achieving the goal of error-free production. Zebra views IIoT-based solutions as an essential component of this effort.

**The Benefits of IIoT**

At the heart of IIoT is the way companies capture and share data. The ability to have data about inventory needs immediately available in the cloud and available to both plant floor managers and suppliers provides unheard-of visibility that heightens operational performance. It is for this reason that technologies which connect assets, inventory and equipment are essential pieces of the IIoT puzzle.

Zebra believes that manufacturers are beginning to see the many benefits of having fully connected operations that include both internal plant operations and the supply chain. The factory of the future needs end-to-end supply chain visibility on the plant floor to improve productivity and increase quality, which is precisely what IIoT delivers. Zebra's 2017 Manufacturing Vision Study indicates that the number of companies supporting a fully connected factory is expected to double by 2022 as over one-third of those surveyed anticipate having this capability.

**The Rising Importance of IIoT**

Manufacturers are adopting Industry 4.0 to create "smart factories" in which workers use a combination of RFID, wearables, automated systems, and other emerging technologies to monitor the physical processes of the plant and enable companies to make faster and more decentralized decisions.[6]

With automation comes instant access to data which is essential to ensuring that the production process operates smoothly and efficiently. Importantly, data gives suppliers the ability to anticipate the needs of their customers. It also enables manufacturers to keep less inventory on hand and eliminate points-of-failure. In fact, 50 percent of the respondents to Zebra's 2017 Manufacturing Vision Study stated that improving their ability to adjust to fluctuating market demands is a top business growth strategy.

To this end, I am pleased to inform the Subcommittee that, from Zebra's perspective, manufacturers – and the U.S. economy – are already realizing the very real benefits of data connectivity through such things as:

---

[6] Source: Bernard Marr, *What Everyone Must Know About Industry 4.0*, Forbes Magazine, June 20, 2016. Web. 10 Apr. 2017, https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#1f25bf89795f.

- Increased visibility into the entire manufacturing process.
- An accelerated pace in shipping and receiving.
- Faster identification of points-of-failure, and
- Deeper insights into the interworking of their operations.

**The Challenges to Fully Deploying IIoT**

The goal of achieving end-to-end visibility in manufacturing and across the supply chain isn't easy to attain. There are many barriers to adoption, most notably the costs and highly complex processes associated with integrating this functionality into existing systems.

Often, proprietary legacy systems require a full rip-and-replace to achieve the integration needed for optimal IIoT and this is likely a key reason why companies rank complexity of technology and availability of IT resources among the top reasons why businesses are not yet achieving a fully connected factory. Fortunately, new advancements in technology are both making it possible to integrate these legacy systems and simplifying the process for doing so.

Currently, 27 percent of those surveyed in the Zebra 2017 Manufacturing Vision Study indicate that they are collecting data from production, supply chain, and workers. It is worth noting, however, that the data appears to often remain in silos, rendering much of the intelligence unrealized.

While implementation may be challenging, Zebra believes manufacturers are committed to improving quality and, therefore, are focused on adopting and constantly improving these data collection processes. In fact, some 34 percent of those surveyed in the Zebra 2017 Manufacturing Vision Study expect to achieve a connected factory by 2022. IIoT deployment may occur in incremental stages, but there is little doubt that manufacturing companies will pursue the creation of fully connected factories over the next several years.

**IIoT Deployment Drivers – Quality Management**

Manufacturers are entering a new realm where quality has retaken its rightful place as a very real competitive differentiator. Producing high-quality products isn't only required for retaining and gaining customers, it also translates into incredible cost savings that ultimately impact the bottom line. This applies in particular to discrete manufacturing plants where one wrong item can affect an entire process.

Manufacturers across all industries cite supplier quality as a prominent concern, with a total of 58 percent of respondents to our 2017 Manufacturing Vision Study stating supplier quality is an issue. Improving quality overall is a top concern for manufacturers and that trickles down to the materials and components they use to produce their products. In fact, executives across North America, Europe, Asia Pacific and Latin America cite improving quality assurance as their top priority over the next five years.

Thankfully, achieving consistent quality output is increasingly attainable and affordable thanks to advancements in IIoT technology and automation. With auto ID technologies that enable track and trace, RFID tagging, and gate automation, manufacturers have greater visibility into what is happening every step of the way so they can easily identify a point-of-failure or reconcile the bill of material.

**IIoT Deployment Drivers – Creating Increasing Tracking Points in Manufacturing**

Improving quality in the manufacturing process means having multiple checkpoints and real-time monitoring along the production line. In a fully connected plant floor, every physical asset has a digital profile. Manufacturers use these profiles to track real-time location, material allocation, and condition of assets. The data can also be used to improve the overall manufacturing process by eliminating bottlenecks, communicating with suppliers, and ensuring overall process and product quality. Although only 24 percent of those surveyed in the 2017 Zebra Manufacturing Vision Study currently have technology-driven tracking capabilities in place, it is something manufacturers know they need. In five years, 63 percent of those surveyed plan to increase their tracking with more than 28 percent planning to adopt real-time monitoring.

Additionally, the 2017 Manufacturing Vision Study also notes that manufacturers are planning to install more check points or gates across the entire manufacturing process. Increasing gates gives real-time monitoring capabilities that help improve quality and throughput. In fact, 23 percent of respondents report their intentions to increase the number of gates in the production process to 10 or more within the next five years.

More check points will both help ensure a higher quality of goods produced and reduce the costs associated with recovery. These additional check points will also provide much-needed transparency, an element that's critical to growth. Forty-six percent of those surveyed acknowledge increased visibility across their operations which, in turn, indicates that a connected plant floor with the ability to collect and analyze data is imperative. Providing employees real-time access to that check point data will improve productivity, decrease unplanned downtime, ensure process compliance, and enable traceability both in internal plant production and across the supply chain.

**IIoT Deployment Drivers – The Demands of Industry 4.0**

Smart factories are the core of Industry 4.0 where real-time communication between the supply chain and the production line enable a high-level of automation and digitization. Making this possible are machines that IIoT helps self-optimize and share data in real time to deliver better quality goods, unprecedented visibility, and impressive cost efficiencies.

Increasingly, companies are focusing less on keeping materials on hand and depending more on suppliers to provide goods on-demand. Industry 4.0 brings with it a legitimate and affordable capability for mass adoption of Just in Time (JIT) shipments in which suppliers have the technology to anticipate the needs of manufacturers and deliver materials when needed to meet production cycle requirements. This trend is particularly prevalent for the high tech and

pharmaceutical industries, and these industries expect to have the greatest amount of change in this area in coming years.

**IIoT Deployment Drivers – The Importance of Expanding Functionality**

To meet the needs of customers who require JIT notification of shipments, companies expect to deploy full-featured, best-of-breed Manufacturing Execution Systems (MES) that track and document the transformation of raw materials into finished goods.

According to the Zebra study, 40 percent of respondents are currently using a full-featured MES in their factories. By 2022, this number is expected to increase to 52 percent. Surprisingly, high tech is behind the trend with only 34 percent using best-of-breed MES today. Over the next five years, this industry will likely see the largest adoption with 50 percent of respondents expecting to deploy MES.

What will help companies make this leap? Most likely, we believe it will be on-demand cloud capabilities and the growing trend toward Software as a Service (SaaS). Fifty-two percent of the respondents in the 2017 Zebra Manufacturing Vision Study expect to use these services in 2022 compared to 38 percent who use it today.

**IIoT Deployment Drivers – The Value of Leveraging Technology to Realize Greater Growth**

As the manufacturing industry moves toward more automation, IIoT-based wearable and voice solutions will play an increasingly pivotal role. Wearables and voice-driven technologies go hand-in-hand and present exciting opportunities for manufacturers to automate processes and increase efficiencies.

While still a relatively young technology, wearables offer a plethora of opportunities to improve safety and increase productivity on the plant floor. For example, some solutions can monitor a worker's physical condition and alert supervisors if issues arise that could present a health or safety hazard. Employees equipped with video camera glasses will be able to record what's happening on the line. There are many more opportunities for wearables to transform the production line, which is most likely the reason why companies plan to increase the use of wearable technology by 15 percent in the next five years.

Similarly, as manufacturers seek to eliminate the need to store excessive inventory, voice technologies will play a key role in JIT manufacturing and automating processes. Fifty-one percent of companies which participated in the Zebra 2017 Manufacturing Vision Study indicated that they are planning to expand the use of voice technology in the next five years. The most dramatic growth for voice technology will be in the largest companies (>$1 Billion) with reported use growing from 28 percent today to 55 percent in 2022.

**IIoT in American Manufacturing**

In American manufacturing, companies are working hard to adopt IIoT solutions to create smart factories and superior supply chains. The Subcommittee's hearing this morning is well timed and most appropriate as firms are capitalizing on IIoT in both factory operations and across the supply chain to achieve real-time visibility into their goods, assets, processes and places.

Through the principles of Manufacturing 4.0, the smart factory calls for providing actionable visibility to the entire operation, from inside the plant to the operations of those vendors who can help manage the supply chain. Workers use a combination of RFID, wearable technology, automated systems, and other emerging technologies – many made by Zebra – to monitor the physical processes of the plant and enable companies to make faster, smarter and more decentralized decisions.

By way of example, Whirlpool Corporation wanted to optimize mobile device management at its distribution centers as a way of enhancing productivity. Whirlpool was having problems with misplaced devices, battery life, the inability to update devices in a systematic way, and a lack of data metrics around device performance. They needed a centralized management system to track device health, productivity, location, and ensure proper deployment.

To solve their problem, Whirlpool began using Zebra XT15 mobile computers, VH10 vehicle-mounted computers, and Zebra's Operational Visibility Service (OVS). The VH10 and XT15 are extremely rugged, reliable devices that suit the distribution center well. OVS helps Whirlpool and long-time Zebra partner, Industrial Service Technology (IST) right-size equipment and understand the needs of the pool as well as site-by-site needs. This combination allows Whirlpool and IST to sense when there could be a problem, analyze what it is, and act on a solution in real-time.

This is but one example of how automation provides instant access to data which is essential to ensuring that the production process operates smoothly. Manufacturers are realizing the very real benefits of data connectivity: increased visibility into the entire manufacturing process; an accelerated pace in shipping and receiving; faster identification of points-of-failure; and deeper insights into the inner workings of their operations.

**Policy Recommendations**

For companies all across America to successfully utilize IIoT solutions, they must have unfettered access to quality high-speed broadband, both wireline and wireless. Without investment in ubiquitous broadband infrastructure, many rural communities, companies and consumers risk being left behind. Spectrum is the lifeblood of IoT, and that is no different for IIoT solutions.

We urge the Subcommittee and the full Committee to support infrastructure legislation that promotes the deployment of mobile broadband networks, as well as directs the NTIA and

FCC to allocate more commercial licensed and unlicensed spectrum in a technology neutral way. Additionally, we urge Congress to advance policies that increase broadband investment and deployment.

Zebra also supports coordination among government agencies to discourage overlapping government regulation of the Internet of Things which could impede innovation. We commend the Subcommittee for your efforts to ensure that American industry has the ability to continue to roll out new technologies that will improve the lives of both our workers and our citizens.

**Conclusion**

Industry 4.0 and IIoT may be transforming the manufacturing sector, but it is the need for quality assurance that is driving manufacturing process innovation. Change is already underway and manufacturers and suppliers are integrating visibility solutions into the plant floor operations to increase quality, expedite production, and reduce costs. Key efforts include instituting more gates along the production line, enabling automated communication between suppliers and manufacturers, and deploying advanced technologies to empower workers and decision making. All are strategic steps that companies are embracing to realize the truly smart factory of the future.

In sum, Mr. Chairman, IIoT presents a transformative opportunity for enterprises of all types and sizes across the Unites States and around the world. The benefits of IIoT-based solutions are allowing companies to work smarter, enhance productivity, create jobs and improve the overall economy. At Zebra, we are committed to bringing IIoT solutions to companies to help them work better and smarter, giving them a performance edge.

Thank you for the opportunity to share our story. I am happy to answer any questions you or your colleagues may have.

Mr. LATTA. Thank you very much.
And Dr. Kurfess, you are recognized for 5 minutes.
Thank you.

**STATEMENT OF MR. KURFESS**

Mr. KURFESS. Thank you, Chairman Latta, Vice Chairman Kinzinger, Ranking Member Schakowsky, and other members of the committee.

I do appreciate the opportunity to testify here before the subcommittee. So I am Tom Kurfess. I am at Georgia Tech. The difference between my colleagues here and myself is our product or our students. For example, mechanical engineering produces about 3% to 4% of all the mechanical engineers in the Nation and these kids are extremely capable and really moving a lot of the IoT forward.

I have spent a lot of time in manufacturing. I grew up actually in a plant in Congresswoman Schakowsky's district. I went to high school there and so forth—a small family plant. So I've been in production for over 40 years. And if you look at it, we talk about the fact that, yes, it's going to take a lot of money to sensor up, as we would say it. But there are already a lot of sensors out there and they're providing free information to us and so forth.

So there are a lot of sensors. They're generating big data. The companies know this and we are starting to track this. My team works with two major U.S. OEMs in automative, a major OEM in aerospace and several large-scale suppliers to figure out what their digital manufacturing platforms need to look like. And, basically, all the data are there for the taking and how are we going to make use of them, right. And then the question is what can we do with it.

Well, certainly, we can improve efficiency. I think we've heard about that. We could lower our energy consumption. We can lower our waste. This is very clear. It's been demonstrated time and time again. I've spent a lot of time actually over at the BMW plant in South Carolina—tremendous opportunities there in terms of moving it forward. A safer work place—certainly, the more sensors you have out there, you know what's going on. You can make sure that your employees are safe and you can make sure that those machines keep them safe and actually make their jobs easier and more reliable. But perhaps a very important point that we need to really understand is that this capability allows us to respond rapidly to the changing markets and the changing technologies that are out there, and those technologies and markets are changing rapidly.

It took about 70 years for the telephone to become ubiquitous. It took about 10 years for the mobile phone to become ubiquitous. It took about a year for the smart phone to become ubiquitous. This is how fast things are changing. So we can have a safer place, a place that responds better, and what industry doesn't want to respond better and faster?

What do we get out of the Internet of Things for manufacturing? First of all, there are better paying jobs. There's no doubt about it. But I will caution you, and I will say this again, it requires a much lower-skilled workforce and a better trained workforce. But it's not

impossible to do. I think we just saw over here, and I will wave mine around too, people are used to the smart phone. This is not something that they're afraid of. We can get them to use it and actually we are using smart phones in production operations day in and day out at a number of different corporations.

We get a stronger, more productive manufacturing base, which is always good for the Nation's economy and national security, and we basically excel in the strengths of the culture of the United States of America.

We are innovative, right. We have some of the best ideas and what this technology allow us to do, IoT for MFG, as we call it, it allows us to get these ideas out there rapidly and not just out there but to scale them in terms of the market. And you know, if somebody else wants to copy us, come get us, because by the time you copy us, we'll have our next technologies out there and we can see how fast these things are moving along.

So how do we get there? Basically, we have to look at workforce development. I heard cybersecurity a number of times. This is critical. People—and we've actually seen at companies where they say, no, we are going to not do this because of cybersecurity issues. They have now come to the realization that we have to do this if you're going to compete, and we are looking at cybersecurity. We have a lot of, for example, national apps.

NIST is doing some great work in cybersecurity analysis and so forth in conjunction with our universities and a variety of companies. So it's there. We are thinking about it. We are working on it and we are beating the bad guys in most cases. We have to develop that infrastructure to make sure that that broadband connectivity—I heard that, right—that is so important.

Again, the low-cost labor areas, yes, you see their shiny new factories but a lot of low-cost labor areas don't have that type of connectivity. We can leverage that. We could make use of that. That is where we can compete.

We also need to take a look at our universities. Right. How do we leverage our universities? How do we leverage our national labs—places like NIST and bring them together? I heard the National Network for Manufacturing Innovation, Manufacturing USA. This is where companies are coming together to really move things forward for the United States of America and this is where we can really leverage these things. So, basically, this is going to allow us to rapidly address a changing market, not just what people want but what the technology is when it comes out there.

The bottom line is IoT for manufacturing it's going to grow. It's going to grow high in jobs. But that basically means not just workforce development and workforce training, not training the next generation workforce but training the current generation workforce. It can be done. We can't compete on the low-end jobs. We just can't, right. But we can compete on the high-end jobs and people are not afraid of the technology. It is amazing. We are doing Pokemon out in the factories right now and they're tracking things, and they love it, OK, and their reward might be to get off a couple of hours early on a Friday afternoon. But it allows to grow the national economy, to grow key sectors of the national economy—high-

tech sectors—to strengthen our national security, to make sure that we are able to move forward in a rapid a nimble way.

Thank you very much.

[The prepared statement of Mr. Kurfess follows:]

Energy and Commerce Committee Hearing

**Disrupter Series: The Internet of Things, Manufacturing and Innovation**

Testimony before the Subcommittee on Digital Commerce and Consumer Protection

United States House of Representatives

January 18, 2018

by

**Thomas R. Kurfess, Ph.D., P.E.**

Professor and
HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control
Woodruff School of Mechanical Engineering
Georgia Institute of Technology
Atlanta, Georgia USA

Chairman Latta, Vice Chairman Harper, Ranking Member Schakowsky and other committee members, I appreciate the opportunity to testify before the subcommittee. My name is Thomas Kurfess and I am a Professor and HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control in the George W. Woodruff School of Mechanical Engineering and the Georgia Institute of Technology in Atlanta, Georgia. My background is in advanced manufacturing, and I have over 40 years in manufacturing. I grew up in the Chicago area in a family machine shop working on machines tools with my father, sister and brother. I studied mechanical engineering, and electrical engineering and computer science at the Massachusetts Institute of Technology. I have been a faculty member since 1989, and have had in depth experiences with a variety of companies and organizations including small start-ups, medium sized corporations, large suppliers, and original equipment manufacturers (OEMs). I have worked at national laboratories such as the Lawrence Livermore National Laboratory and the Sandia National Laboratories, and I have participated in a wide variety of national and international organizations that are heavily involved in manufacturing.

As I have previously noted the principle area of my research and its application is in advanced manufacturing, in particular what has come to be known as digital manufacturing. Digital manufacturing relates to the use and integration of Big Data,

connectivity (*e.g.*, broadband and the Internet), and high performance computing into manufacturing. Sometimes this is described as the fourth industrial revolution, or Industry 4.0. The first industrial revolution was when water and steam were used to power production operations. The second was when electricity replaced water and steam. The third industrial revolution was when electronics, such as computers, were used to automate production. The fourth industrial revolution takes the third industrial revolution to a completely new level by leveraging high speed connectivity, Big Data, cloud computing, and cloud storage. In particular, I am here to speak about "The Internet of Things and its effect on Manufacturing and Innovation." The Internet of Things, or IoT as it has come to be known, is the network of physical devices that are all around us. For example, we have smart phones that are on line, smart watches and cars that are on line, and so forth. The same is true for the IoT and manufacturing, sometimes known as IoT4MFG, or the Industrial Internet of Things (IIOT). In particular, I will testify about IoT for manufacturing as it relates to Digital Commerce and Consumer Protection. The key points of my testimony are as follows:

1. IoT has come to manufacturing. It is here and cannot be stopped. We need to embrace it, and ensure that our use of IoT in manufacturing leverages all of our strengths in the United States.
2. While IoT for manufacturing provides a variety of significant advantages, and must be embraced by U.S. industry, we must also be aware that there are a variety of security issues that must and can be addressed. These need to be taken seriously and addressed quickly to avoid falling behind our competition in the manufacturing sector.
3. IoT within manufacturing leverages the innovation and forward thinking nature of U.S. culture, and should be used to enable innovation in the United States, allowing U.S. based companies and entrepreneurs to quickly innovate and move their ideas and concepts into large scale production before others can copy and deploy these new concepts and technologies.
4. IoT for manufacturing is a means by which an educated workforce can be highly leveraged and utilized. It can be used to make safer and more productive workplaces, but it does require a more sophisticated workforce.

I will elaborate on these points during the remainder of my testimony.

Many of our manufacturing operations are already connected one way or another to the Internet, or at least to an internal corporate network. For example, typical machine tools and robots that we see in production operations have front end PCs as user interfaces, and these PCs, like most PCs, are on line. Network connections to these front end PCs are typically how information such as the programs is loaded into a machine and/or robot. Furthermore, these machines have a variety of sensors that generate data that are useful for plant operations and maintenance. For example, just monitoring the oil level in a machine is a simple operation. Sending out an e-mail or text over the network when the oil level becomes low is a very useful and simple operation using the IoT. The oil level sensor is ultimately connected via the network to plant operations and maintenance personnel, allowing them to know when to add oil. Of course, this is a very simple concept, and one with which we are familiar, as modern automobiles also inform us when it is time to add oil, or perhaps change the oil. Furthermore, many cars are on line, and it may be that the car schedules an oil change on its own such that the driver or owner of the vehicle is not bothered with the details of an oil change. The same is true for a machine in a plant. The information from the machine may be used to automatically order more oil and oil filters for the machine, and schedule an oil top-off or change, making plant operations even more efficient. Finally, a supervisory system may track oil consumption on a particular machine. If that system notes that the machine is consuming excessive oil, it may order extra maintenance or diagnostics for the machine to determine why it is "burning" or consuming more oil than usual.

The example that I have just given is related to a single machine. However, there are plants in the U.S. where we have thousands, or maybe even tens of thousands of machines. The ability to monitor those machines to ensure that they are operating most effectively is exactly one of the capabilities that IoT for manufacturing enables. This requires significant infrastructure within plants and between plants. This infrastructure consists of, but is not limited to, broad band connectivity, large data storage capacities (e.g., cloud storage) and advanced high performance computing capabilities to process the large quantities of data. Such infrastructure is readily available in the U.S. and provides us with a significant advantage over less developed parts of the world. Indeed,

such infrastructure can offset the advantages of lower labor costs in less developed sectors of the international market. We should be leveraging this advantage, and continuing to support these critical manufacturing relevant technical infrastructures to ensure that the United States preserves and extends its advantage in this area.

With respect to security and safety, the IoT for manufacturing does provide for a safer and more secure workplace. There is no doubt that added sensors and monitoring will lead not only to enhanced productivity, but also to enhanced workplace safety for the labor force. However, with added connectivity and more computing capability comes the threat of cyber-attacks and cyber security issues. As with all sectors that are integrated tightly into the Internet, we must be vigilant with respect to cyber security. This requires that the Nation invests accordingly in cyber security initiatives and standards, and that our workforce is properly trained in best practices for cyber security.

IoT for manufacturing also enables our manufacturing operations to rapidly change and upgrade. This has two major effects. First, such rapid change capabilities enable the latest technologies to be implemented, ensuring that production operations are continuously improving and remain competitive. This capability also permits quick and effective product launch, which allows new products to be quickly produced at scale for deployment into the market. In short, IoT for manufacturing enables the innovations from the proverbial drawing board to migrate quickly to the market. Others may copy new U.S. innovations, but when that happens, we will be able to deploy even newer innovations, constantly keeping ahead of our competition. Thus, IoT for manufacturing complements the highly touted U.S. ability to innovate by rapidly and efficiently bringing those innovations to market.

Finally, as I have already stated, to fully utilize IoT for manufacturing, a strong and well trained workforce is needed. I am talking about training both the next generation workforce, as well as the current generation workforce. The reality is that most of our workforce is well aware of the Internet of Things. Many have products like Fit Bits, smart phones and tablets. Thus, I am not talking about a significant technical leap for our

workforce. Rather, I am speaking of having them apply what they are experiencing in their everyday lives to the manufacturing floor. What we need to do is ensure that our workforce understands that the diagnostic and prognostic functions that are now viable for systems, such as robots in a plant, make use of sensors that are already on board the robot. The concept is fairly straightforward. We have Fit Bits for humans. We can also have Fit Bits for robots and machines. Of course, the analogy goes much further than this; however, culturally, the general population has, for the most part, accepted the IoT in their daily lives, and transitioning the IoT to their lives at work in a manufacturing operation is a path that is easily pursued. That being said, there are a number of universities, schools and professional societies that are developing training material to aid in this transition. There is no doubt that IoT in manufacturing will help to grow our manufacturing operations and will generate new and higher paying jobs. However, those jobs will be filled by individuals that are highly trained. Furthermore, those individuals will need to be continuously trained in the latest and state-of-the-art technologies to keep U.S. manufacturing operations at the forefront of this rapidly advancing technology wave. Thus, a culture of lifelong learning must be instilled and supported in our workforce.

In conclusion, the Internet of Things for manufacturing is a technology and capability that is vast, rapidly changing, and plays well to American strengths in high tech, innovation, and a strong manufacturing infrastructure. To fully leverage the opportunities presented by the IoT for manufacturing, we must have a strong high tech industry in place with a well and continuously trained workforce. The United States has all of the elements to fully utilize and leverage the IoT in manufacturing. What is needed is a strong manufacturing infrastructure, new manufacturing technologies and capabilities, and a well trained workforce with a culture that is amenable to lifelong learning. Programs such as Manufacturing USA that bring together collaborative teams from industry, government and academe are not only bringing the Internet of Things into the manufacturing world, they strengthening U.S. manufacturing capabilities by engaging highly diverse and technically savvy teams to rapidly deploy next generation capabilities to our manufacturing operations. Such partnerships not only ensure that the United States

domination of the manufacturing sector will continue well into the future, they also ensure that U.S. manufacturing will keep pace with, and lead, our competition no matter how rapidly change occurs. IoT for manufacturing promises to provide a strong, secure and vital manufacturing base for the United States, ensuring national security and strengthening the nation's economy.

Mr. LATTA. Again, thank you for your testimony.

And Mr. Poonen, you are recognized for 5 minutes for your opening statement. Am I pronouncing your name correctly, sir?

Thank you.

**STATEMENT OF MR. POONEN**

Mr. POONEN. Dear Chairman Latta, Ranking Member Schakowsky, members of the subcommittee, and my honored colleagues from academia and the industry, it's an honor to be here to testify in front of this committee.

And by way of instruction, my name is Sanjay Poonen. I am Chief Operating Officer of VMWare. VMWare is one of the top five software companies in the world, about a $54 billion market cap company. We are headquartered in the Silicon Valley in Palo Alto. We are also part of the Dell Technologies family.

It's very clear from a lot of what you have heard already that the Internet of Things and IoT has a profound impact on the consumer economy and also in the industrial age. I will just give you two examples of how our lives have changed. One is from my past job. I worked for a German software company, SAP, and many of the meetings that I had would actually be at 1:00 p.m. in the afternoon, German time, which is 5:00 a.m. Pacific time. So mean scheduled, I go down to my home office and I find out that overnight some person had the great joy of canceling the meeting. Now, listen, wouldn't it have been nice if I could have known that before I went to bed and I could have probably woken up an extra hour later? Well, it would be nice if once the meeting is canceled it actually communicated with my alarm clock that actually set my clock up an hour later, which is very much possible today with IoT because often the alarm clock and your calendar is on the same device.

Another example—when I leave to go to ski—not a lot of snow this year in Tahoe but the years that we do have snow, we'll have a debate with my wife as to whether we turn the heating off. And I like to keep the energy down and keep the house not necessarily heated all the time. She wants to keep the house warm for our kids when we come back home. Well, now with modern thermostats you can actually turn your thermostat on or off from your phone when you get about an hour closer to NIST and many others are doing this.

So this is the practical way in which our consumer lives are being transformed for the better with IoT and this is now starting to invade the American worker. And manufacturing actually becomes enormously smart, as you heard, because of this and it has profound impact, we believe, in lots of new areas—artificial intelligence, big data machine learning that can be very positive as opposed to as much as what's also been talked about, the negative impacts. But it does have some profound security challenges and that's been a key part to VMWare's focus. VMWare's focus is to ensure that the cyber attacks that we've seen, whether it's WannaCry, Petya, many of these things that could get even more profoundly disruptive in the context of IoT is something that we can attack and we can protect ourselves from.

So we've actually been focused on aspects of cybersecurity and cyber hygiene that allow companies to protect themselves in this era of IoT.

We've got some very practical ways in which management security would be baked into the infrastructure of both technology and manufacturing.

We think that everybody today, whether you're in technology or not in technology, need to be educated in some very fundamental principles of security, like, for example, lease privilege, micro segmentation, multi factor authentication and identity management, encryption, patching. These are all very fundamental concepts that board members today are being educated on and certainly government and other professionals need to.

As we think about the notion of hardware, that's also getting more sophisticated. We heard about mobile devices and rugged devices—one of my colleagues. Edge gateways now are becoming ways by which this miniature data center could actually become micro into something like a little nano data center, protected and ready for the production line. These are the ways in which we believe that the Internet of Things and smart manufacturing can actually be secure.

In closing, the Internet of Things will have a significant and positive impact, we believe, on both American innovation and jobs. Billions of IoT devices will be in the free market for consumers, will be available to manufacturing and can have a very positive impact. But to make sure that this is actually deployed in a safe fashion, security is key. If consumers are to trust these devices and manufacturers were to trust these devices, we've got to take security seriously and we believe that this is something that both the coming together of academia, of industry and the government makes this a priority.

We look forward to working and doing our part at VMWare to make this happen. The other aspect of this that could be very positive is the way and which the data can actually help a whole new category of jobs, whether it's machine learning, big data, artificial intelligence.

This is going to be the next color of jobs, and much the same within the agrarian culture. A hundred years ago we couldn't see the coming of computing and high tech the same way the next 50 to 100 years are going to be very exciting in terms of new jobs.

Chairman Latta, Ranking Member Schakowsky, I applaud the leadership of this committee for holding this hearing today. Thank you for the opportunity to testify and I look forward to answering the committee's questions.

[The prepared statement of Mr. Poonen follows:]

**Testimony for the Record**

Sanjay Poonen

Chief Operating Officer

VMware, Inc.

Before the

U.S. House of Representatives

Energy and Commerce Subcommittee on Digital Commerce and Conumer Protection

"Disrupter Series: The Internet of Things, Manufacturing and Innovation"

January 18, 2018

Chairman Latta, Ranking Member Schakowsky, and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Sanjay Poonen, Chief Operating Officer at VMware Inc.

VMware is a leading provider of software-defined solutions that increase the operational efficiency and security of data centers within the federal government and across the globe. Currently, VMware is one of the largest software companies in the world with more than 20,000 employees. We are headquartered in Silicon Valley, California, with 140 offices throughout the world, serving more than 75,000 partners and 500,000 customers, including 100 percent of the Fortune 500. The U.S. government is a long standing critical partner and customer of VMware and we remain committed to serving all sectors of the U.S. Government – including the Department of Defense, civilian agencies, and the Intelligence Community, as well as state and local governments. VMware is a part of the Dell Technologies family of companies, which is the largest privately controlled technology company in the world.

We are committed to providing both government and commercial organizations with the ability to respond to their dynamic business needs, whether they utilize on-premise datacenters, the cloud, or personal computers and mobile devices. VMware is providing enhanced security to government and commercial customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers, and devices.

**Cybersecurity Policy**

The U.S. Government is dependent on a vast cyberworld of interconnected information technology (IT) networks, data centers, the cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission-critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber systems has immeasurably benefitted the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern-day functions of government, sophisticated and aggressive cyberattacks perpetrated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. As you know, there have been well-publicized cyberattacks, including the Office of Personnel Management (OPM) breach, which compromised the personal data and security of over 21 million current and former federal employees.

We are also experiencing an unprecedented level of cyberattacks in the private sector. As an example, the well-publicized security breach of a large credit reporting agency created the potential that the personal data of well over a hundred million of United States citizens has been potentially compromised. Over the summer several ransomware attacks including WannaCry crippled the operations of a major global shipping company, one of the largest package delivery companies, a major drug manufacturer, as well as several healthcare providers. The reality is that global technology companies, like VMware, in cooperation with our customers observe a constantly growing increase both in incidence and sophistication of cyberattack – both from and upon systems inside the U.S. and overseas.

**Internet of Things (IoT) Security**

The emergence of the Internet of Things (IoT) is a technological step in which more and more aspects of the physical world, from manufacturing to banking to home monitoring to healthcare, transportation and even "smart cities" are interconnected and coupled with analytics and intelligence. The insights gained drive increased performance and efficiency of our infrastructure and bring new services to almost every aspect of our daily lives. Some consider IoT to be "the next Industrial Revolution." Unlike most traditional computing devices, many of these IoT devices will be directly connected to important physical aspects of our lives – from smart meters to factory robots, from cars to traffic lights, and even to devices in our own bodies such as insulin pumps and pacemakers.

Aspects of industrial manufacturing transition to IoT could mean an economic boost. In fact, according to a new report by the International Data Corporation (IDC), worldwide spending on the Internet of Things (IoT) will reach $772.5 billion in 2018, an increase of 14.6 percent over the $674 billion spent in 2017. The IDC report also states that "the industries that are expected to spend the most on IoT solutions in 2018 are manufacturing ($189 billion), transportation ($85 billion), and utilities ($73 billion). IoT spending among manufacturers will be largely focused on solutions that support manufacturing operations and production asset management."

This could feed into what the future holds related to IoT in manufacturing. While not in all cases, the manufacturing process in the U.S. largely consists of fairly dated manufacturing infrastructure using programmable logic controllers (PLCs) and old versions of operating systems. With the advancement in technology, manufacturers, if they have not done so already, are considering more efficient ways to revamp and retool their IT infrastructure to modernize its operational capabilities. Therefore, manufacturers are likely to absorb the most innovative technology, which is IoT based in many cases. The opportunity that IoT could bring to manufacturing holds the ability to connect and manage the supply chain, the quality of product and other aspects of manufacturing.

While IoT offers exciting opportunities for manufacturers, it also presents some challenges relating to cybersecurity. Cybersecurity will no doubt be a significant priority with all the connectivity and varying pieces of smart equipment on productions lines in a manufacturing plant. From a security point of view, it is unlikely that an individual manufacturing plant would utilize an end-to-end stack of IoT devices and other smart equipment. This means more often than not, manufacturing plants will utlize IoT devices and smart equipment from many different manufacturers. Such a likely scenario would make it more difficult to properly manage the cybersecurity considerations when there are IoT devices and other digitized equipment originating from different manufacturers themselves, all which need to be secured, but all have different application programming interfaces (API) associated with them. The other security consideration is the threat of malicious cyber attacks and hacking to the IoT devices in a

manufacturing plant. This threat has the risk of doing significant economic damage to a given company in that space. From a protection point of view one is protecting against the potential loss of the ability to produce for long periods of time, among other considerations and commitments.

To that end, we will see a significant increase in IoT Gateway devices that aggregate and manage large collections of IoT devices in close proximity to the IoT device. These IoT Gateway devices are often powerful with some datacenter-like characteristics but will be deployed well outside the safety of traditional physical datacenter boundaries – in cars, on oil rigs, as part of the power grid, in factories, on cell towers. From a security point of view, IoT gateways would be able to isolate the varying IoT devices (likely manufactured by different companies) in a production line and ensure adequate cyber hygiene as it applies to manufacturing.

This level of interconnect will lead to exciting new capabilities in our ability to manage and optimize the infrastructures of our country, from manufacturing, to transportation systems, water management systems and many others – but also makes it critical that we secure the IoT from those with malicious intentions.

- It is vital that we secure IoT infrastructure to prevent the compromise or disruption of our economy. This infrastructure, which among other things, will now form the basis of how factories and cities critical infrastructure interfaces with the real world.

- Securing these devices before they can be used as entry points or vectors to attack other parts of cyber infrastructure is paramount to overall strong cyber security.

The threat and impact of IoT based cyberattack is not theoretical; it is real. We have seen the impact and vulnerabilities from last year's distributed denial-of-service (DDoS) attack targeting outdated devices that did not correctly utilize the industry's standard best practices for cybersecurity. That attack took down major internet platforms and disrupted internet services for millions of Americans. The major wave of ransomware attacks last summer that wreaked havoc in the industrial, healthcare and logistics sectors were enabled in part by vulnerable devices that were not built securely or with patching in mind.

Importance of Cyber Hygiene

While there is certainly no silver bullet or single solution to prevent cyber-breaches generally or within IoT specifically, we believe that many of the major breaches in the last few years would have been dramatically reduced or entirely eliminated if some fundamental principles of cyber hygiene had been followed. We propose five core cyber hygiene principles (below) as a universal baseline: the most important and basic things that organizations and the federal government should be doing. The concepts are not new but are key in moving to more effective security. They are rooted in well-established frameworks such as the NIST Cybersecurity Framework (CSF) and are technology-neutral.

| | |
|---|---|
| 1. Least Privilege | If a least-privilege environment has not been effectively implemented and users are provided with higher levels of access than they need, attackers can steal these users' credentials (user name and password) and gain broad access to systems.<br><br>For example, it is understood, in the Target and Sony breaches, attackers were easily able to gain administrative-level privileges. |
| 2. Micro-segmentation | If micro-segmentation has not been effectively implemented, attackers can break into one part of the network and then easily move around to other parts.<br><br>For example, it is understood, in the Target breach, after an initial intrusion into the HVAC system, the attackers were able to move around to the payment network system. In the Sony breach, the attackers were also able to move around from one part of the network to another. In the case of the OPM breach, the attackers obtained access to OPM's local area network and then pivoted to the Interior Department's data center. |
| 3. Encryption | If encryption has not been effectively implemented, attackers can exfiltrate data in readable form.<br><br>For example, it is understood, after a data breach at Royal & Sun Alliance Insurance PLC, government investigators determined that the company had not adequately encrypted the data. |
| 4. Multi-Factor Authentication | If multi-factor authentication (MFA) is not effectively implemented, attackers can obtain passwords and use them to access systems.<br><br>For example, it is understood, in the OPM breach, if the contractor log-ons had been enforced with a risk-appropriate level of MFA, it would have limited the ability of the attackers to use the stolen credentials of the government contractor. In the case of the breach at LinkedIn, the hack exposed inadequately protected passwords of 100 million users. Since consumers often use passwords on |

| | |
|---|---|
| | multiple sites, MFA would have reduced the risk. |
| 5. Patching | If patching is not effectively implemented, attackers can exploit open holes in systems.<br><br>For example, it is understood, the ransomware attacks such as WannaCry exploited known software vulnerabilities for which patches were available. Organizations that fell victim had failed to effectively patch. |

With education firmly in place, these five pillars of cyber hygiene are key in moving to more effective security.

VMware's Vision on IoT

Because VMware is the leader in datacenter and IT infrastructure management, we have a unique perspective on ways to secure the IoT ecosystem. With the advent of the Internet of Things, as more and more connected things are added to the network, it is a natural evolution of VMware's capabilities to now go out to the edge and help IT manage this new infrastructure.

Consumers, businesses and government need to feel confident that IoT technologies are secure and their information is protected. At VMware, we have advanced IoT products and software applications that embed each of the five cyber hygiene principles laid out earlier.

A way to secure the IoT ecosystem is to ensure flexible and isolated connection points through secure manageable infrastructure, such as IoT Gateways. Whenever an IoT device connects to the internet, whether by itself or through an IoT Gateway, that system needs to be manageable, deployed responsibly with a proper initial configuration, and maintained at the current state of best-security-practices available throughout the complete lifetime of the device.

IoT Gateways are an integral part of the IoT infrastructure, including, but not limited to, a manufacturing plant. They bridge, but also decouple, the physical IoT devices from management components in data centers. This bridge allows data and control to move securely from the device to the cloud or data center. We need secure IoT Gateways to ensure that data and information are secured as it moves through the IoT pipeline.

**Summary**

The global digital ecosystem is experiencing an unprecedented level of sophisticated cyberattacks. In order to secure and adequately protect our customers, products, services, production lines, and networks against these highly sophisticated attacks, we must utilize every security tool we have in the toolbox. The IoT economy presents a significant opportunity for U.S. companies. Billions of IoT-connected devices will be on the free market for consumers, businesses, and government to consider purchasing. The U.S. has a ripe opportunity to claim global leadership in the IoT space. The IoT economy will create American jobs and could be an opportunity to boost American manufacturing across the country.

The IoT economy will also provide new efficiencies for consumers, schools, hospitals, and manufacturing, as well as federal, state and local governments. Security is the key principle that will enable and advance further adoption of IoT. If consumers, businesses and government do not feel that IoT products are secure, it will only hinder U.S. global leadership in an inevitably growing and innovative IoT economy.

Promoting good cyber hygiene should also be a key goal that helps agencies, consumers and businesses better protect their information and networks from malicious attackers. In addition, edge systems like IoT gateways offer the industrial IT environment such as manufacturers the ability to isolate their advanced IoT devices and ensure that sound security policies will be implemented on a production line.

As Congress and the Administration continue to work on policies promoting the IoT economy, we believe that it is important to seek input from industry stakeholders. Security needs to be paramount to protect sensitive data and information, as well as securing critical infrastructure. We believe that it makes sense for the relevant federal agencies to work closely with industry stakeholders in order to develop a set of standards and principles for IoT security.

I appreciate the opportunity to share my thoughts on this very important issue. We applaud the leadership and vision of Chairman Latta and Ranking Member Schakowsky for holding this hearing. VMware looks forward to continuing to work with the Committee on this and other important issues. Thank you again for the opportunity.

Mr. LATTA. Well, again, thank you all for being with us today. We really appreciate your testimony before the subcommittee.

And now we'll move into our question and answer portion of the hearing, and I will recognize myself for 5 minutes.

Mr. Masney, what are the major advantages for OI that come from using IoT? And, again, I've been through the facility in Perrysburg where you do a lot of the testing and seen a lot of what you're implementing there. But if you could maybe just walk us through what you're doing.

Mr. MASNEY. Certainly. Some of the advantages are increased productivity in our manufacturing facilities. As I said in my statement, glass is still somewhat art, and we need to transform to data-driven science manufacturing process where we can increase our yield.

Glass manufacturing yield is somewhere in the 90 to 91 percent yield rate. If we are able to do that, we are able to unlock potential and capacity out of our factories and better serve the markets and, ultimately, reduce our cost to our customers.

Mr. LATTA. What are some of the challenges that you're facing out there today in the home manufacturing process then?

Mr. MASNEY. And having enough of knowledge base in a workforce that has a demographic that is changing. The degeneration of knowing what to do, when to do it, is changing in our organization, and being able to empower people with information so that they can react faster and more nimbly is incredibly important. And cyber security—that is a concern today because many of our machines and equipment stand alone. So they're not exposed to cyber attack. And as we network them and collect more and more information to better empower our workforce it's going to be incredibly important that we protect the floor, our people, and the company.

Mr. LATTA. Thank you very much.

Mr. Bianculli, can you give us an example of how a sensor can be used to convert data from a format that allows companies to improve manufacturing efficiency?

Mr. BIANCULLI. Sure. I think a couple of examples there—one is just driving operational efficiency. I mentioned the Whirlpool example earlier, where we just have a stream of data coming from devices. Well, just like we've done that with Whirlpool on device health, we are looking at doing that with the entire manufacturing facility.

So imagine, if you will, a smart manufacturing environment. We know where goods are. We know where the capital assets are in that environment. We can know where people are located and we can bring the intersection of all those things together in an optimized way.

We think about our daily lives using a route navigation GPS system in our vehicles. The incredible amount of advantage—the ability to dynamically reroute based on whether in traffic in real time and think about going from outside the four walls to an inside the four walls factory environment and being able to bring that same level of route optimization, work flow efficiency, dynamic work flow optimization to the processes by instrumenting the environment.

I think that as we look at data coming from these environments we are moving toward a world where we no longer operate on what

we think is happening—where do I think my people are, where do I think my assets are, where do I think inventory is—we are operating in a world where we truly know that in real time.

And so we are able to close this gap between what we think is happening and what we would ideally like to be happening and that is where the benefit is—the efficiency benefit. The return on investment is being able to close that gap. And so you can run your operations in a much more precision way and in a way that's optimized from the get-go.

We are seeing the imperative to do that because of the on-demand economy. The notion that products and services are being delivered ever closer to the point of demand is a reality. We order online and the expectation is that product or good or service is delivered sometimes in an hour to our doorstep if it's a package that we ordered online and we live in an urban city, or in some cases I am standing at a street corner and I request a ride and in moments I expect that to show up.

So the production and provisioning of products and services ever closer to the point of demand dictates, mandates, it's an imperative that we have IoT solutions that are able to create real-time streams of data to enable that new reality to propel us forward.

Thank you.

Mr. LATTA. Thank you.

Mr. Poonen, I guess in my last 40 seconds—this is going to be quick—this deals with how to manufacturers manage the threat of cyber attack disrupting their operations?

Mr. POONEN. OK. Good.

Yes, I think one of the things that we have learned, Chairman, sir, is that in this world of mobile, this device is not sort of a remote control to your life.

We've learned a lot about security in the last 10 years with the mobile device. These operating systems have adapted themselves from the PC era to have even greater level of security, whether it's Apple iPhones or Android devices. Some of the security things that you saw in the early days of Windows. And even the PC operating systems, latest version of Windows 10 are better at being able to——

We respect that same innovation, and this country has got some of the best research, whether it's from academia or other places. We'll continually pour it into the operating systems that run on these IoT devices. That's one, and we expect that to just have a greater and greater level of enterprise hardening.

Secondly, the devices and the systems that they talk to, whether it's the data center or the cloud, will have the types of things that I talked about—cyber security, security infrastructure baked into it that have the types of things like segmentation, multi factor authentication, encryption. And we are learning from all of the attacks that have happened to make those also systems hardened.

And then the third and final thing is just basic hygiene, and sort of just like you have a good diet, you do your exercise, you still have to have certain hygiene principles—brushing your teeth, taking a shower, things of those kinds.

We've got to educate government, industry, academia, college students, so that as they approach the workforce there are simple things you probably want to do.

You may not want to send your password, for example, in clear text on a text message. These are the types of things that—and you may want to change your password—these are the types of things that I think are very easy for us to continue to educate that make us all a much more secure society and a secure infrastructure for IoT.

Mr. LATTA. Thank you very much.

And the chair recognizes the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

First, Owens-Illinois—are you still in Illinois at all?

Mr. MASNEY. Yes, we are. We are in Streeter, Illinois.

Ms. SCHAKOWSKY. OK. Glad to hear that, being from the Chicago area.

I think I, years ago, saw the plant. Were you over in Granite City, down in southern Illinois?

No. OK. Let me ask Dr. Kurfess some questions.

How do workers in manufacturing stand to benefit from the adoption of these technologies? Can the IoT be used to, for example, positive things—prevent workplace injuries, limit workers' exposure to hazardous materials, et cetera? And what are some of the pluses of IoT for workers?

Mr. KURFESS. Sure. It's a great question.

There are a variety of things that could be going on, for example, worker going through the factory. If you have been, for example, to an automotive factory you see the robots going on. They're moving, they're working. These are carrying sometimes in the thousands of pounds. So they're very powerful robots. And you'd never let a human get close to them. But now you have the robot area. You have the human area, and the reality is now with IoT of things, and again, one has to be careful about this issue of privacy and so forth. But I am even walking down with my phone. I know where people are. So if somebody walks into an incorrect area, we can shut it down and make sure the roadblock doesn't hurt them. But even better, we can start to localize it better—a much tighter resolution such that the robots can be working with the people.

Robots are great. But they're never going to replace people completely. They're great at lifting really heavy things but try and pick up an egg with one and so forth. We have great research on that. But again, working together is really where you leverage it and, by the way, it also allows us to get rid of a lot of the really nasty jobs. You're taking away the terrible jobs, checking cooling tanks and lubrication tanks and machines. That's all automated. In fact, this morning I was down in your cafeteria and I saw your coffee containers—the coffee urns. They have the same technology that we are using now in there. It's about 50 cents and so the only difference is ours are online and so they're reporting the information. But we are talking with companies like Chik-fil-A and McDonald's about how to do that for improving their efficiency.

So these are the types of things we see out there.

Ms. SCHAKOWSKY. Well, I am also very interested in keeping manufacturing jobs in the United States and bring them back, and you wrote in your testimony that America's infrastructure gives us an advantage there. I would like to hear more about that.

Mr. KURFESS. Sure. Well, if you look at everything from our roads to broadband and so forth, and again, these are things that people really use all the time. Whether it's broadband or you're wired into your factory or broadband, over here, that capability and that growing of that capability allows us to take the big data generated by all of these different sensors, and in some instances, again, it's not just well, I've have a bunch of sensors, but in some instances I've got this phone with this really nice camera and we have our workforce taking a picture.

So now we are combining the workforce who says oh, this is good, this is bad, taking the picture. That integrates the information together. But you have got to get that out streaming all of the data and it is a lot of data. And then, of course, the other infrastructure of these, the educational infrastructure. If you think about the technology from even 5 or 10 years ago, it's old. So we've got to keep that work force spun up. Lifelong learning and that infrastructure needs to be put into place so that today's worker is still viable in 5 or 10 years.

Ms. SCHAKOWSKY. Well, I was going to ask about that because, the role of government and, certainly, public education is a part of that, but there's also federally funded research, et cetera.

So government does have a role to play then, doesn't it?

Mr. KURFESS. Oh, definitely. And all the way—again, you know, from the K through 12 that we hear about education and so forth to our Bachelors students or Masters and Ph.D.s, if you take a look at National Science Foundation, I was sponsored at MIT, right, as a National Science Foundation on a project there. A good chunk of our graduates, Masters and Ph.D.s in engineering, technology, and in science are supported by the National Science Foundation.

Again, that's something that you don't really see but they're supported as research assistants and this is a very important thing to move forward, the entire infrastructure for the Nation.

Ms. SCHAKOWSKY. I appreciate that.

So I am concerned because spending plans that we've seen from Republicans make drastic cuts to many of these things and to programs that directly support manufacturing and innovation, including President Obama's Manufacturing USA initiative.

So these cuts, I am assuming, then could be a barrier to progress?

Mr. KURFESS. Yes. I think that what you have to look at is in the short term it's fairly easy to make a cut like this and so forth. But really, the Federal Government—we don't have AT&T Bell Labs anymore. We don't have really long-range thinking companies. They're focusing on the here now, and I don't blame them. The Federal Government has to step in there and really do some of the longer range thinking. I guarantee you, China's doing it. Germany's doing it. You name it, other countries are doing it. We need to do it.

So in 5 years, in 10 years, we are positioned to continue to move forward. This is really, again, what we really need to be looking at

a little bit longer term and that's what these R&D capabilities are all about that we are talking about.

Ms. SCHAKOWSKY. I appreciate that, and I yield back, Mr. Chairman.

Mr. KURFESS. Thank you.

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

The chair now recognizes the gentleman from Illinois, the vice chair of the subcommittee, for 5 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman.

And just to go off with what you were saying, sir, I agree with you. I think there's a role for the government in terms of long-term strategic planning that sometimes gets lost in the kind of momentary debates which is, as we look at world that changes, whether it's with IoT, whether as we look at autonomous vehicles, which this committee deals with and all that kind of stuff, we have to have people that are thinking long range and beginning to prepare our workforce for what that future looks like. It doesn't mean the heavy hand of government but it also means let's consolidate some of these programs we have and try to incorporate a vision which some of our competitors, unfortunately, do all too well.

I want to thank the chairman for yielding and I want to thank you all for being here. I am excited. I have two companies represented here that have a strong presence in Illinois—Zebra and Owens-Illinois.

Zebra is based in Lincolnshire, Illinois, which, now that the economy is expanding maybe you can build one in my district too because there's no presence there yet. But we'll take it in Illinois.

And Owens-Illinois, of course, does have a strong presence in Illinois. Somehow they're headquartered in Mr. Latta's state but we can talk about that, too.

And as Mr. Masney said, there's an OI facility right in Streeter, Illinois, and in my district. So proud to have you there. You provide good-paying jobs. I was able to visit a few years ago and have been very impressed by what I've seen.

I would like to ask the panel, talking about the development of IoT, does that mean that American workers will require new training and what are companies doing to obtain a skilled workforce?

I would like one or two of your to answer that with your perspectives.

Mr. BIANCULLI. Sure. So yes, absolutely, happy to have our presence in Lincolnshire and we should talk later.

Mr. KINZINGER. Yes.

Mr. BIANCULLI. So yes, with regard to that, worker training—I think the future we are talking about here isn't going to arrive evenly.

We are going to see certain areas. We are already seeing IoT drive location technology being used to control drones in site facilities to be able to—in manufacturing plants, actually, to be able to detect inventory in a more automated fashion.

The ability to have robots deployed in a distribution or fulfilment center—but what's happening in those environments today is—let me take the robot example where goods now are bringing—taken to the picker. If you have a human, at the end of the day, doing that picking for those online orders to fulfil those orders, and the

goods are being brought to them instead of them walking to the goods.

And what does that mean? There's no job taken away. There's just several less miles a day that that worker is going to walk. That means there are many more picks per hour that worker can do.

And so we are in a world now and will be for some time where humans and machines and automation, whether it be physical automation or it be artificial intelligence augmenting the worker, basically, a digital assistant——

Mr. KINZINGER. And I just want to add onto that.

If you look at the example, for instance, around Europe, the Germans are very good at manufacturing. They have a very low unemployment rate. But they are also embracing this kind of future technology.

So we don't have to be scared of the future because it's coming. We just have to figure out how to lead and innovate in that process.

I will go on. Mr. Poonen, when you talk about the Internet of Things, does that create new concerns when it comes to intellectual property?

For instance, does the data collected in IoT manufacturing reveal anything proprietary that companies might want to protect?

Mr. POONEN. Yes, sir.

I think that one of the things you have to first remember is that the first wave of IoTs being able to take away mundane tasks and make them something that could actually be done more autonomously, I will give a very simple example.

You don't want to watch me parallel park a car. I am terrible at it. That's a perfect job for a machine to do better than a human because it's a combination of cameras and geometry, and it'll probably parallel park better than you.

But my value add long term isn't parallel parking. So what we want to be able to do as the next wave of economy shows up is to ensure that you have got the appropriate privacy and security baked into many of the machines. And there's a whole dedicated work of security being focused on the devices and what's on there and we have to make sure that there's standards also because the same type of privacy that applies to peoples' homes, people are worried as to whether or Alexa or Siri is always listening to you. Those are the types of things that standards need to be applied both from the government and industry working together, and I believe that this is absolutely solvable in the same say that the industry and government work together on standards like common criteria.

This will be applied to the new world of IoT in the coming years, we believe.

Mr. KINZINGER. And Mr. Masney, what's the trend when it comes to the cost of deploying IoT? Can you envision a day when the entire manufacturing process, from the procurement of raw materials to the delivery of the finished project, is 100 percent automated without human intervention?

Mr. MASNEY. No, I can't envision a day like that. It still takes human beings on the manufacturing floor to make things happen and make sure things are moving forward.

I will share with you, in Streeter, Illinois it is one of our facilities where we are delivering what we call the factory of the future for the organization and invite you to come see that at some time that make sense.

But, certainly, we are still going to need the capability to have people on the floor that can run machines, be ever present, make sure things are running safely, that productivity continues to move forward.

Our innovations are around more flexibility and making sure that we can be more responsive to our customer base. And IoT is another area where we think we can do that as well.

Mr. KINZINGER. Thank you all for being here, and I yield back.

Mr. LATTA. The gentleman yields back, and the chair now recognizes the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you very much, Mr. Chairman. I want to thank the witness panel. This is absolutely fascinating to know what's going on now and what the possibilities are too in the future.

Digitally connected supply chains have the potential to be an important component of the industrial Internet of Things. Just in time, manufacturing promises to drive down the need for storing excess inventory and allow suppliers to anticipate and deliver the materials manufacturers will need more quickly.

Decentralized ledger technologies like block train can make supply chain transactions faster and cheaper by securely connecting manufacturers and suppliers in real time.

I would like to hear from Mr. Poonen and Mr. Kurfess what are your thoughts on technology such as block chain and others and its ability to play a role in IoT manufacturing and security.

Mr. KURFESS. Sure. So it's a great set of questions and the reality is the distributed capability, whether it's block chain, or any of these other distributed capabilities.

These are going to be critical in terms of moving things forward. If I've got a supplier, only one supplier that supplies me with parts, and if I say tomorrow, oh, I was at Toyota—how is it going there, this was in Kentucky, and they said, well, great, we've got very, every 6 hours we can get parts from Denso and so forth—we are very lean. We have very small inventory. You go to Denso—how is that working for you? Well, we've got two or three months of supply back there because we don't know what they're going to ask us.

Now, they're starting to figure out how they're going to ask together. But imagine if instead of one big company, Denso, we had a bunch of smaller companies that could supply this.

So, yes, if I need 500 parts, as opposed to having one company say can you make 500 parts, I could go to a hundred companies, local companies, mom and pop shops, and say, I need five parts, or how many can you supply—five, ten.

And all of a sudden you can bring that together. You not only can get those parts there—and by the way, you could use something like an Uber to make a delivery, right. Again, back to the infrastructure, it's there to pull it off.

But now you also have a very resilient supply chain. If one goes down, you don't have to worry about it.

Turning that around as well on the educational side, you can take at what are these guys doing and, you know, where do they need more training and let's get them that training.

We could even percolate that down into our colleges and into our high school levels so we can deliver the education to the workforce and we can even start to send the right students in the right direction to really engage them.

So lots of stuff. Distributed all the way from supply chain of parts but supply chain of our workforce as well. Thank you.

Ms. MATSUI. That's great. Thank you.

Mr. Poonen.

Mr. POONEN. Yes. I think, Congresswoman, this is a very important topic. There's a lot of speculation and euphoria right now about Bitcoin and block chain.

I think the bigger story is the fact that this notion of a subledger, which is really what block chain about——

Ms. MATSUI. Yes.

Mr. POONEN [continuing]. Really transforms the way in which you do commerce at a much more miniature level and if you think about IoT it's sort of a miniaturization of this type of device.

Now, combine that with commerce now becoming even more miniature, it has profound implications that could be enormously positive, and that's really, we think, the big story.

If there are ways by which manufacturing could get smarter and even potentially more secure, and the commerce that happens—electronic data interchange—all of this would become a lot more efficient and potentially also secure because it's now distributed as opposed to one choke point—distributed actions have lots of inherent ways in which you can actually make the system a lot more secure.

At the same time, it does require us to take security and privacy even more importantly because of this distributed nature, and that's something we are beginning to do early research on, not just from industry perspective but also in academia.

But I am confident that the positive aspects, if you take away the speculative aspects of block chain, the positive aspects will have a profound implication that's actually—and we need to, as a country, be at the forefront of the research. If we don't do it, some of the other countries in the world will.

Ms. MATSUI. Oh, good. Well, I thank you very much.

That was very interesting. Let me go on to something quickly. The Clean Energy Smart Manufacturing Innovation Institute in California has been working to accelerate smart manufacturing throughout the country.

Broad collaboration on integrated tools and systems that are driving smart manufacturing will help reduce the cost of deploying these technologies. These partnerships and collaborations can also facilitate the interoperability of devices and standards.

Mr. Kurfess, how can government and industry partnerships help develop tools and practices that will drive smart manufacturing adoption?

Mr. KURFESS. That's a great question.

I think we've already heard about things like——

Ms. MATSUI. Yes. Go ahead.

Mr. KURFESS. Oh, I am sorry. Have heard about things like standards and so forth. But, really, to help move this forward.

The difficulty is, again, you get back to the distribution. Different people want different standards and different capabilities and so forth.

When you start to bring these entities together so, the smart manufacturing team that's, I think, centered in the Los Angeles area, and it's not only the big companies but it's also the so-called small- and medium-sized enterprises—the SMEs—that they're bringing together. So they're really bringing everybody together to say yes, how does this move forward—how do we do this.

And what a lot of companies are getting is, yes, I need to release this, because to become more productive, more capable, right, I need to participate in this standard.

It's like when I turn my laptop on, the wifi, I know I am going to be online. That's a standard and that's really where we need to be going with manufacturing.

And by the way, we see our competition overseas doing it in a big way. So, we have to be cognizant of that.

Thank you.

Ms. MATSUI. Well, thank you. This is all very interesting.

I know I ran out of time but thank you.

Yield back.

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. I appreciate this. My background, before I got here, was in manufacturing, and it wasn't very long ago that somebody from Ford Motor Company would make an order from a supplier—my family was a supplier—you would have a production meeting where they'd say, "We need a thousand of these parts."

A guy would walk out to the plant to look around and with the clipboard—or lady—and say, "OK, we got this much here, this much there. Let's go to the shipping dock. See how much we have there," because you couldn't always depend on the counts. So then they would call the buyer at our place and say, "I need X amount." So they would walk out on the floor and say, "How many do I have?" and with the clipboard and it would—this whole string of things.

And if you go to an assembly plant and invite anybody from Bowling Green, Kentucky to go the Corvette plant and see one of America's great cars made, well, what you look for is how phenomenal all of this stuff just comes together and how much effort and time and planning.

So if you do it now, you get a production manager who says, "I need a thousand parts," somebody uploads it on the internet, the supplier comes in the morning, downloads it, everything is barcoded—I assume Zebra—but everything is barcoded so you can depend on the counts, and all of a sudden it makes a work order. When you ship it you barcode it. When it goes out it creates a purchase order so you get paid for it and that's distributed through the internet or through the transfers—not necessarily through checks like you used to have to open checks and move forward. And that's

happened in the last—since I've been in manufacturing. It wasn't that long ago I started. And it's just a phenomenal look forward.

But I was looking at Mr. Poonen's testimony and looking at Dr. Kurfess' here, my son went to Georgia Tech so we appreciate having you here today.

But I was looking at this security and cybersecurity, because we think about data security and whether your credit card was secure. You had all these retailers come in and talk about—really, if you put everything online and everything is Internet of Things in your manufacturing facility, is there a cyber attack, could that shut down an assembly plant.

So in your testimony you talked about the importance of systems like Internet of Things, gateways, and why—you talk about securing the production lines, and not necessarily, I don't think, it's just from attack you were talking about. But just if you could throw that in as well and the importance of cyber hygiene and can you describe how this would provide a reasonable level of security?

Mr. POONEN. Happy to, and I think the focus on security is a very good one, and I think just the same way that if you thought about various different eras of computing, sir—mainframe, the client server, to mobile cloud—this notion of security has become a more and more profound because if there's one thing that's true, even though security is getting a lot of spending in software the bad guys, there's more attacks than there's actually investment even in security companies.

So we have got to take this seriously, and the good news is that countries like the United States and Israel have been on the forefront of security spending. We want to take that seriously.

So the way in which we think about IoT is as these devices get miniature, first off, you want to make sure the operating system that's on those devices are as secure as possible and I think we've learned a lot as the new operating systems that are post-PC have gotten more mature and with every generation they're getting better and better. IOS is a good example of that and the iPhone being more secure than the first examples of the PC and those will play down to the miniature devices.

Secondly, you want to have control points that dislocate just these devices into what's called a gateway. So gateway is just a consolidated form of many of these so that you have one place rather than multiple places where much of it gets consolidated. Dell manufactures some of those gateways. You got to make sure those are secure.

And then as they talk to other systems, for example, a data center or a cloud, that connection needs to be secure, and there's techniques like micro segmentation, ways in which you authenticate into those systems using multi-factor authentication. These are all technical terms but for the folks who are savvy in security we are educating more and more of them.

And then, finally, for the common person, as I described earlier, you want to be able to educate them on some very basic principles of cyber hygiene, especially as it relates to their access of systems.

Having a two-factor authentication is something that everybody should know about. It's not just your user name but some other factor. Maybe it's your birth date. Maybe it's your mother's maiden

name. And setting up your system so that you have that and are refreshing. That allows fewer possibilities that your consumer accounts will get hacked the same way that the enterprise is dealing with it.

These are just a few of the many principles of cyber security written in the white paper about this and it's a topic that all of us in the industry—there shouldn't be competing agendas here. We need to work together to make sure the security of the IoT systems.

Mr. GUTHRIE. A quick question. I appreciate Mr. Masney. He was talking about glass and going from 91 to 93 percent. I am aluminum foundry die casting and as you said it's sometimes more of an art than science, and I remember saying that in a meeting and a guy goes, "Well, all scientists were art at one time and how do you perfect it?"

So I only have a few seconds. When these first come out a whole industry is created and everybody is buying these. All of a sudden you get saturation and sustainable and improvement. But there's a whole world of people in Silicon Valley, all over America, to go in and redo these plants, redo these facilities.

And I don't have much time left, but anybody want to talk about just what transformation and what economy that could create by people going through and refurbishing their plants?

Mr. KURFESS. I will just really quickly fire it off because we see it across the board. We work with a lot of different companies.

The opportunity is tremendous. Whether the small or the medium or the large companies because, again, the kids now they program these things, and so they're in there, hey, we can do this. This is the barcode readers now and so forth. And so they're really implementing it. And so it does allow you to do these types of implementations.

But back to Mr. Poonen's point, we've got to make sure that we are very secure about this. So, and again, in our classes whether it's high school or junior college, whatever, we now see that a lot of this type of thing, we are just doing good hygiene. For example, do not plug this into, just any old computer. I go to a machine shop. Million-dollar machine tool recharging my phone, which could have a virus on it.

And so these are the types of things that we really have to start teaching them and stuff. But the opportunity is tremendous.

Mr. GUTHRIE. Thank you. Thank you for indulging us.

Mr. BIANCULLI. Representative Guthrie, one other point, if I may.

There's a whole suite of capabilities I was starting to bring to these enterprise devices. We actually called it mobility DNA. But the idea is taking a standard operating system that we might be using Android by way of example and layering a whole host of enterprise-centric security on top.

So we are working closely actually with VMWare on this sort of thing. So as these devices—these internet end points are deployed in these manufacturing facilities, being able to make it secure all the way up the device level, so we have a network of secure devices instead of just trying to secure the network, and that's an investment we are making to basically serve enterprise in a more secure way than we might find in traditional consumer devices.

That, and the last thing—another word silos. I think there's tremendous opportunity to bring silos down across what many of my colleagues here spoke about—from farm to fork, if you will.

So for being able to share data from where that seed was planted in the farm field and be able to carry that data all the way through to optimize the harvest out to the transportation carriers for just-in-time delivery and then ultimately getting to a retail location where we can all enjoy that in a much more efficient way and in a way that allows us to, in a more cost effective way, reach more people.

So I think the data silo opportunity is tremendous as we start to collect more and more data across all the different elements of the supply chain.

Thank you.

Mr. GUTHRIE. Thank you very much. I appreciate the indulgence.

Mr. LATTA. Thank you.

The gentleman from Pennsylvania is recognized for 5 minutes.

Mr. COSTELLO. Thank you, Mr. Chair.

Dr. Kurfess, I wanted to focus on something that you had provided in your written testimony, not just ask you but ask the rest of the panel for their feedback as well.

There's no doubt IoT in manufacturing will help to grow our manufacturing operations and will generate new and higher-paying jobs. However, those jobs will be filled by individuals that are highly trained. Furthermore, those individuals will need to be continuously trained and that's what I want to focus on.

In the latest and state-of-the-art technologies to keep U.S. manufacturing operations at the forefront of this rapidly advancing technology wave, thus, a culture of lifelong learning must be instilled and supported in our workforce. If you look at our high schools and STEM schools and trade schools for 18 to 19 year olds, I am struck by the opportunities that might be available to incorporate more of this lifelong learning culture into curriculum at an earlier age so that it is not incumbent upon a company in order to do that. And when you look at company of 20, 30 people, even startups of two or three individuals, it's just simply not sustainable to offer that type of learning and sort of up-to-date type education that's required in order to keep a well-trained workforce.

I've already spoken too long. Share with me what you think the right kind of learning platforms are in order for our country to be a leader for the next 20 and 30 years so that these are not jobs that are not remaining in the U.S.

Mr. KURFESS. Sure. So really quickly, the first thing is, I can tell you, we have turbine blade production. We do a lot of work in turbine blade production. So we have turbine blade production machines. We are doing research and so forth. And typically you need about 15, 20 years of experience before we turn you loose on those in production operations.

We have developed gaming interfaces—high-performance computing that can really—it just pounds that problem to dust and there are gaming interfaces and we have high school kids who are now programming these types of machines and so forth.

So it's a whole different way of learning and as I mentioned before, we can even take a look at who is really excelling. People

think, oh, engineering—I've got to be a super genius. Well, you have to be fairly good at math and so forth. But if we can start to really identify those students early on and start to work them forward—they don't necessarily have to go into engineering. Maybe they're going to go into the shops and so forth and get the right type of training.

But it's a two-way street. So the infrastructure is coming into place. We have a number of these different—if again you look at Manufacturing USA, these centers that are working with the local and particularly the community colleges, the Associates degrees and so forth, they are saying, yes, what is the next generation that we need to be moving forward and let's work that into the curriculum. And that's not only for the 2-year degrees but for the continuous learning. And then we also see a lot of the professional societies, that they have a lot of curriculum development that's deployable whether it's on the web or interactive and so forth.

So a lot of the technology is moving out. But I agree, you have got to build it in. Universities, I think, have done a good job with life long learning. We now have to start to propagate that down into the K through 12. It's getting there, but once it's there, I think the access for those students and for that work force is available and it also does respond very quickly to the needs of the workforce and the needs of the market.

Mr. COSTELLO. Right. Mr. Poonen.

Mr. POONEN. I would just briefly add, this topic is personally very much a topic of passion for me, sir.

I came to this country as an immigrant. I am now a U.S. citizen, partly because the United States has the best universities. I studied my computer science at Dartmouth College. I did my MBA at Harvard University at Harvard Business School, and I hope that this continues to be the country with the best education in the world.

The education has now changed. Today, my kids, who live in Los Altos, California, are learning through Khan Academy. YouTube has completely transformed education and it's not just for kids. You can get a how-to or learn-to anywhere anyplace in 15-, 20-minute Ted Talk types of videos and we encourage our workers to constantly be in that learning mode and the good news is the internet makes that possible. And it's almost upending the classroom where learning is happening at home in the evenings and the classroom becomes a discussion form. That's the new fashion of what we're doing.

I think the other part that is incumbent on all of us as leaders is to mentor others. As much has been given to us, we've got to give back to the next generation. I encourage all of us—I know many of our colleagues here do the same—it's our job to mentor the next generation. As we do that, both the combination of STEM and mentoring will make the next generation ready.

Mr. COSTELLO. That's interesting. So it might be technology that enables us to teach technology.

Mr. POONEN. Exactly, sir. That's what we hope.

Mr. COSTELLO. Anyone else?

Mr. MASNEY. From a manufacturing company perspective, we are investing in our local high schools and STEM programs to help the younger generation get interested in science and technology.

We are also working with local universities to make sure there's an interest as well. So I personally believe helping workers, obviously, continuous learning—lifelong learning—there's also an aspect of company helping our employees be lifetime employable through those kinds of ideas as well.

Mr. COSTELLO. I appreciate your feedback. I yield back.

Mr. LATTA. Gentleman yields back.

The gentleman from South Carolina is recognized for 5 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman.

Siri, hey Siri. I use that as an example in that these devices are always listening, right. Whether you have an Echo in your home or some similar device, whether manufacturing has those devices that, as you say, are all interconnected, or whether you as an individual have a smart TV and internet rumors, true or not, that that TV is spying on you and sharing that information.

As we move forward with technology and we have a refrigerator that notices that my milk is low and asks me if I want to order milk, and I do, sends a signal to the grocery store—milk, bread, other things I may need delivered to my home by an autonomous vehicle, right.

So I consider myself a conservative. There's nobody in this room that would say I am not a conservative. But I would actually take it another step further. I am a conservatarian in that I have a libertarian streak in me that it's my information and I own it. But in this scenario that I laid out, who actually controls that data and who owns that data, and at some point, it's the government getting that data and what do they do with it.

Now, data sharing and by buying habits and what Amazon is sending me through e-mails or pop-ups that, because they watch my buying habits and they're recommending certain things, that benefits me. I get all that.

But I can tell you the constituents in the 3rd District of South Carolina are concerned about who has that information, what they're doing with it and ultimately does it get in the government's hands without any sort of 4th Amendment protection, so to speak.

So I would just love to—I know, Mr. Poonen, you were talking about some of that earlier. I would just like to expound on that. Who owns that data and how can I assure my constituents that that data is not going to be used wrongly.

And then I would also like to get back out on that tangent because you have got proprietary information and corporations, and we all know that China got the plans for the F-35. China has gotten plans for a lot of the military components with the best safeguards of cybersecurity in place by our government, right, who has access to all of you all to create those platforms for security.

So I would like to talk about not only individual privacy and data ownership but also how do we keep China from—or a Chinese company, and I am not just singling China out but from going to BMW or Magna or some sort of manufacturer in the 3rd District and getting proprietary information as well and creating a competing product.

Mr. POONEN. Yes. Very briefly, and then allow time for my other colleagues, too.

This is a very hard topic. I would be smug if I said we have all the answers today. This is going to require continued innovation and collaboration with the government.

I would say there's a family of problems that are related to predictive maintenance of machines that are positive. For example, if the refrigerator or the washing machine is decrepit and you need someone to come and help you in that, that's a family of problems—that people are probably less concerned. The data on that machine probably needs to be encrypted.

But as soon as you have things that are voice recognition, camera related, privacy concerns, and we encourage consumers, certainly enterprises also, to be extremely cautious. You can turn the camera off on your TV. You can certainly unplug Alexa when you need to and get appropriate cautions on how you handle these consumer devices.

Mr. DUNCAN. But that smart TV is monitoring all of your viewing habits.

Mr. POONEN. Exactly. So this is going to be one of those places where a combination of encryption, a combination of technologies, and I am with you. Consumer privacy—the consumer owns that data. The way in which they interact with enterprises—most of our focus has been on the enterprise use of this. But the consumer part of it is a huge problem that needs to be solved together and there's no easy answer for much of this because we are just beginning to scratch the surface of many of the topics that are way out there.

Mr. DUNCAN. In the essence of time, we know China took the plans for the F-35, so to speak, and government was involved. How do private industry—how can they have some assurance that their proprietary information is sheltered from their competitors?

Mr. POONEN. We are seeing the shift from assuming that we can prevent an enemy, if you will, from getting in to being able to detect that as quickly as possible.

So if you think about what is your mitigation plan if you assume a thesis of you'll prevent attack from occurring, you have a very different outcome in that strategy and that plan that if you assume that you will not be able to prevent an attack and so now your strategy is going to be to detect that as quickly as possible, to shut down that intrusion, and then to take the corrective actions from that point forward but detecting that as soon as possible.

So going from protecting to detecting and then taking a counter measure as quickly as possible in every sense of that word I think is a shift we are seeing right now. It's no longer, as you pointed out, the best resources on the planet in some instances cannot protect that attack from occurring. So let's focus more on leveraging all the technologies spoken about here—machine learning, artificial intelligence, technologies like deep packet inspection, over packets on the network, to be able to detect that if that is occurring.

With regard to in-home, I think similarly we are going to see—technology has been used for a while in the network space called deep packet inspection where why not have a single source of truth of the information that's leaving my home.

So what products are sharing what information with whom, and imagine if I had a dashboard that I could go to a portal on a web page in my home and I could see, well, I shut that TV—I don't want that camera on that TV sharing information. Is in fact that data going out over my network or not, and those kind of dashboards so that we can have—enjoy, all of us, the convenience associated with sharing the information but have the integrity and single source of truth to understand what actually is being shared, and I agree with the number of devices and the prolific nature of this that thinking that we are going to be able to control that because we were told it works a certain way is not going to be sufficient.

Mr. DUNCAN. I guess my constituents would say, is Big Brother going to call me or send me a notice and say that your thermostat was set on 72 when you left the house today and you have overutilized your allotment of electricity for the day. Do you see what I am saying?

Mr. POONEN. I do.

[Simultaneous speaking.]

Mr. DUNCAN [continuing]. Be going and that's a true concern.

Mr. POONEN. I think the best answer to that is to use all the mechanisms I just mentioned and more to come to ensure that that's your option—that you're informed enough to—it's your choice to share that information for a benefit gained.

Mr. DUNCAN. I am way over time, Mr. Chairman. Thanks for leniency.

Mr. LATTA. Thank you very much.

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

Mr. GREEN. Thank you, Mr. Chairman. I thank our witnesses for being here.

Sorry we have other committees—the Energy Committee upstairs and so I am jumping back and forth.

When I first saw the hearing, and that's why I appreciate this subcommittee—the Internet of Things—I thought, what in the devil is the Internet of Things? I cleaned up my speech after the president didn't.

But what is it? And thank goodness I have young staff to explain to me. I am glad you're having the hearing because it makes some of us who don't typically live with these things shed light on different aspects of the smart manufacturing and the Internet of Things.

One of our witnesses mentioned manufacturing as one of the sectors that is investing the most in IoT. I have a district that's predominantly petrochemical refineries, chemical plants, extraction, and I know they're looking for every way they can using technology both to produce their product safely or cleaner and doing more smart manufacturing can make operations both environmental safer and more efficient. But Congress needs to do more to prepare our workforce for those changing needs and manufacturers.

Mr. Kurfess, you mentioned in your testimony importance of instilling a culture of lifelong learning and of helping to train our manufacturing workforce in the data science and IT skills that workers need. Some people that need job training the most are the

unemployed and one of the biggest obstacles they face getting into that technical training is the cost of it.

Can you elaborate on possible ways Congress can help this technical training be made more affordable as well as help support a culture of lifelong learning broadly?

Mr. KURFESS. Sure. I would be very happy to do that, Congressman.

I know that there are a lot of initiatives that are really supporting the community colleges. These are the 2-year colleges and so forth. They're very cost effective for the training of the workforce and so forth and there's a lot of leveraging that goes on there.

We heard about some of the online courses that are available today, even via YouTube and so forth. And actually, our—at least our younger generation they learn and they think in a different way, right. So, when I was a student I might have had one book to look at or maybe two books to look at. Now they go out there and they get 10, 20, 30 different examples and so forth.

So, really, not only just saying yes, we could make sure that we can support the community colleges and some of the professional societies that have these types of courses offering technical training but also the ability to basically say yes, let's make sure that we are starting to leverage some of these new approaches to teaching and so forth and that we understand that they're out there so that it comes out there very quickly.

And by the way, these are also very important not just because they're lower cost but they're very nimble. They can respond quickly to new technology as it comes along.

So, if you have some YouTube videos out there—you can learn anything from fixing a faucet all the way to, hey, let's go do a calculus problem.

But as new technology comes along, it's amazing. You can go to YouTube. You can go to some of these different courses, even MOOCs, these massively online courses and so forth that some institutions offer for free. And so how do we promote that, once you have that, I think the next key thing is certification. Yes, you are certified in that course. So that when they go to your company—and by the way, it's interesting, when people think manufacturing, make a car. Those petrochemical plants are enormous manufacturers within the United States.

And so how do we know when that company says yes, I want to hire somebody that yes, this person has the right credentials. It's great that they have a degree from, let's say, a Georgia Tech, but what about just some of the smaller credentials that are going along. So a lot of that credentialing and getting back to some of the standards that we are looking at.

Mr. GREEN. Well, I appreciate that.

I actually have a community college in our area who partners with the petrochemical industry—San Jacinto College in east Harris County, Lee College in Baytown, because of the dominance of that industry, and I've been out there and they're doing—and a number of my other community colleges in our area developing the same thing because you just don't go get your Associate's or your Bachelor's or anything. You need to continue to look at what's new, and I was there on campus one time and a young man had about

three different certifications, and he was getting offers of over $150,000 at a Shell refinery or a LyondellBasell refinery or chemical plants.

So it's a way that someone—but you have to continue to keep up with your industry and that's what community colleges can do.

Mr. Chairman, thank you for the time.

Mr. LATTA. Well, thank you very much. The gentleman yields back. The chair now recognizes the gentleman from Indiana for 5 minutes.

Mr. BUCSHON. Thank you, Mr. Chairman.

Mr. Poonen, I am going to primarily talk with you and some of the other about security. Mostly, it seems to me, when we're talking about security we are talking about software and other—and access and things like that—passwords and all of that.

But you probably saw in the news recently that in some areas across the country there were some communities and police departments that took down their security cameras because of concerns of where that product was made, and it was made overseas and so there was some question not about that it was connected to the internet but the actual hardware itself and whether that was compromised.

There's some things I know that we do at the Federal Government level to ensure, for example, that chips that are used in Defense Department products are not compromised, so to speak, but worldwide and even in the U.S. some people estimate as many as 10 to 15 percent of computer—the hardware, like the silicon chips, are actually counterfeit.

That's an area I think we should also look at. What are we doing there?

Mr. POONEN. I think it's absolutely wise, sir.

I think that when you think about security it absolutely is in all of those layers. You need a multi-layered, whether it's the hardware or the software, whether it was the service, was the people.

And listen, capitalism works only if the entire world is a level playing field and when some countries are not necessarily playing by that I think it's absolutely the wise policy, whether it's the FBI, whether it's the appropriate agencies, to ensure that our products, whether they're bought for a foreign party, don't have embedded components, hardware or others, that could potentially compromise the security. So——

Mr. BUCSHON. I can tell you probably know and I know this myself, sometimes it takes an electron microscope and people that understand it to detect these problems with chips and stuff.

Mr. POONEN. Yes, absolutely.

Mr. BUCSHON. It's pretty sophisticated.

Mr. POONEN. Yes, and there's absolutely evidence of that happening. I am not a protectionist in terms of the way in which we think about the economy. We do believe in free market. But it has to be one with a level playing field.

So many of the governments that have been focused on this, certainly in the United States and Israel, that have had this have got a very good way of looking at the ways in which many foreign governments are building technologies, and without naming certain countries, we've got to continue that diligence, because whether it's

the camera technology, whether it's voice recognition, the types of things that could leave us vulnerable, we've got to make sure we've got the most protection. We work very closely, both the industry and the government, the agencies, to ensure that happens. That's probably a topic we haven't talked about. I am very glad that this committee is focusing a lot on security. Security is probably one of the key topics in this entire topic of IoT that needs even more and more focus.

Mr. BUCSHON. Yes, because it is a global marketplace and I am in favor of that. I am a free market person also. I think we all are.

But we also, from our jobs' perspective as members of congress we have considered national security-related risks and the biggest port of entry that we have is our people using connected devices, maybe even at their homes. For example, say they work at the NSA and they deal with classified material every day that we don't want people to know about. But when they go home they have all their devices at home are all connected and who knows who's listening.

And even though they're not supposed to—what if they're just pontificating among even themselves about the day's activities? It's hard to know.

So I have pretty significant concerns about on the hardware side, because once we are able to mitigate other things, people are smart. You're already too late when the hardware itself is compromised. Does that make any sense?

Mr. BIANCULLI. Yes. I am just going to add it absolutely does make sense, Congressman. If I could suggest, we could break the problem down to two components. One is around the counterfeit side of things. So these are counterfeit chips or, that are made overseas, copying our technology, and as you pointed out, you need somebody with sophisticated technology to check that.

But what I would say is that actually IoT is a mechanism for auditing that because if we're seeing this occur today, if I'm a semiconductor manufacturer of those chips, I can have each one of those chips report back when they connect as a—just basically a heart—pulse to say that that device is present, and if I see that coming from more devices than I have shipped, I've got an indicator that there's an alternate end around from a supply chain perspective. Someone else is injecting, if you will, these chips into the supply chain that aren't coming from my factory.

So it's sort of an IoT connected auditing mechanism. I think that represents one level of—certainly compromises economics but is a little bit lower on the threat level compared to, as you were suggesting, information that's being sent—that's actually being captured we don't know it—the example you gave around the device in the home connecting back to the network or a video camera in a municipality that's sending information back to individuals that we don't want it to go to.

And there, I think, we and a number of companies working on networking technology that can detect if information is being sent that is different than what we intended to be sent.

And I think if we can audit the network, if you will, the pipe of data that's being sent to see what's actually being sent versus what we've authorized, and at the same time we can continue to invest

and drive in IoT. So all of our devices, for instance, that are connected out in the field can connect back, we can literally count the devices we've shipped. We can count the devices we see. And if there's more devices we see than we've shipped then something else is going on.

So those, I think, are perhaps two ways to look at it. Certainly a complicated problem, as our colleagues have pointed out. But a food for thought, perhaps.

Mr. BUCSHON. OK. Thank you.

I yield back, Mr. Chairman.

Mr. LATTA. The gentleman yields back.

The gentleman from California is recognized for 5 minutes.

Mr. CÁRDENAS. Thank you, Chairman Latta and Ranking Member Schakowsky, for calling this hearing.

As a former small business owner myself, I know that a business that is not growing and evolving is a business that is not succeeding.

As an engineer, I've studied the rise and proliferation of connected devices and for the potential to help businesses and government evolve and better serve their consumers and constituents. For example, a company in my district that testified last June in this hearing on the Internet of Things, Louroe Electronics uses connected microphones and sensors to help protect property and also help law enforcement detect and rapidly respond to gunshots.

On the public service side, the Internet of Things technology has helped local governments and firefighters monitor and prevent and fight back firefighters in southern California, for example.

Recently, the House passed my amendment to study the use of drones to detect and fight wildfires. However, I also know that as with any rapid-growing technology we must encourage innovation smartly, responsibly, and with our eyes wide open.

We are constantly learning that virtually any connection can be hacked. So cyber security is an area that businesses and government will have to pay extremely close attention to and invest a lot of resources.

Another issue that we need to hold our businesses to a high standard on is workforce preparedness. As our companies evolve, our workforce must necessarily evolve as well.

Ideally, this evolution will come in the form of education and retraining. This was an important issue that I brought up during our markup of the SELF DRIVE Act and it's an important issue in every environment. For example, southern California happens to be—I was told when I got elected to Congress I was reminded that southern California is the largest manufacturing area in the entire country. I was pleased and surprised to hear that. So this is an issue that not only is important to my district but important to one of the biggest economies in the world, which is California.

My first question is to Dr. Kurfess. You have the advantage of a bird's eye view of the industrial Internet of Things through your work with a variety of companies.

So can you describe briefly what practices you've seen that help workers adapt to and learn how to better use new technologies?

Mr. KURFESS. Sure. It's relatively straightforward. Some of the practices that are out there actually get to some of the discussions

we've had about just hygiene. Don't plug your phone into the million-dollar machine tool out there because it might have a virus on it and so forth. But some of the other practices really go along the lines of understanding what people are comfortable with in terms of using and so forth and letting them make use of that technology in place.

As I said before, we actually have developed some software where you're doing a Ppkeman type of program—you're looking for the guy to try and capture. But that guy you're trying to capture is a flaw in your production cycle and so forth and you capture it.

So you actually start to bring these together. The Internet of Things—people are very comfortable in general. It just doesn't matter who you are. People have the smart phones now and they're very comfortable using it.

And so the idea really is yes, can you bring that comfort together so that they make use of it in a very easy and natural way.

So that's one of the things. The other thing, again, and we've heard from several companies here, just continuous learning, to make it easy, you make it rewarding, to provide the time so that the people in the plant can do some learning.

And we are not talking hours and hours of time. Typically, it's just yes, just take a look at this thing—we can track your progress and so forth and making sure that they're up to speed on what a company needs to have them up to speed on, whatever that might be.

Today it's going to be, and again, coming out of California you realize this—whatever's going on today may not make a whole lot of difference tomorrow in terms of technology. That's how rapidly things are changing.

Mr. CÁRDENAS. It's interesting that you describe the example of the cell phone and how that could interfere with the opportunity to, unfortunately, have an infiltration in your system.

I learned, again, through one of the subcommittees on health, is that some hospitals, and a lot of people now realize that infections—if you're going to get an infection, probably going to get it a hospital more than anywhere else—that it wasn't some incredibly expensive process to bring down the infection rate at hospitals other than having the discipline of everybody washing their hands at every opportunity. Something as simple as soap.

But what I am getting at is I think it's important for us to teach the next generation of workforce that even though they find these things to be so darn convenient and think that it's the answer to everything. It actually, if not handled properly, with simple measures you could actually cause a disaster or catastrophe that is unintended.

So I think it's important for us to realize that sometimes the answers are complicated. Sometimes the answers are really simple about basic discipline.

Thank you very much, and I yield back my time.

Mr. LATTA. Thank you very much. The gentleman yields back. The chair now recognizes the gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it, and thanks for the testimony.

I was at the joint VA Committee hearing. So I apologize for being late.

I have a couple questions. The first one for Mr. Bianculli—in your testimony you state that industrial IoT-based solutions are allowing companies to create jobs. One of the big concerns we are facing is automation replacing jobs. So can you please explain to us how these solutions help create jobs?

Mr. BIANCULLI. Sure. Yes, I think there's sort of a micro and a macro view on that. The micro one I mentioned a little bit earlier around machines working with workers to help them get their jobs done more effectively. And I think when we think about that, we have a tendency to think of the brawn side of that, meaning that the physical movement of goods and that's for sure a part of it. The other part of it is that the brain or the intelligence are an assistant that can work along with the worker. So we mentioned wearable technology, augmented reality, being able to put information right up in front of the user. And as this starts to assist you, that should create more job satisfaction, a better work environment. It also, in addition to increasing quality and having benefit to the bottom line, reduces the cost of getting that job done. And so if I shift from the micro perspective over to macro, as we reduce the cost of getting that job done, we become more competitive on a global basis, thereby bringing jobs back in.

So if we look at any one instance we could point to well, if we are reducing the cost of labor that—some might say that's reducing the number of jobs. I would say it's increasing the efficiency of an individual and thereby increasing efficiency of that individual has the macro effect of making us more competitive on a global stage.

And I think that we are starting—I mean, it's happening already. We are starting to see that bear itself out. The other thing we are starting to see with the on-demand economy that we mentioned earlier is the peaks are getting peakier, if you will. If you look at the number of shipments that are happening from manufacturing facilities or from fulfilment centers in the November to January timeframe—in some cases, you see this in the headlines—transportation carriers, retailers, are doubling or tripling their workforce to be able to handle that peak demand.

And so when you bring that influx of workers in, if it takes 2 weeks to train somebody how to do that job, you're a third of the way through that peak cycle. So leveraging this technology so that someone can be functional and up and running in an hour and be as skilled or as capable as someone that's been doing it for several weeks also becomes very important.

So I think if we view it that way and look at the bigger picture over the longer time horizon, there's early indicators that what I just described is starting to happen and I think we should lean in and accelerate to take advantage of that for the country. Thanks.

Mr. BILIRAKIS. Thank you. Good answer.

In your testimony, Mr. Masney, you note that, and I quote, "the cost to achieve a full deployment of IoT throughout an enterprise can be quite daunting," and suggest that lowering those costs would help ensure the deployment of the IoT.

What are some of the ways policy changes could help?

Mr. MASNEY. Certainly. Looking at ways to reduce the cost per unit of a sensor or technology can help spur investment into IoT, and it's not just one thing. It's sensors. It's PLCs. It's storage. It's systems. It's investment in programming and those kinds of things.

So, certainly, looking at ways that we can spur innovation, get products produced at a lower price than manufacturing companies can consume and deploy at a lower cost point, especially in a business like ours which is very capital intensive, is going to be incredibly helpful to move IoT forward.

Mr. BILIRAKIS. Very good. Thank you.

Mr. Chairman, I appreciate you holding this hearing. Very informative and I will yield back the balance of my time.

Mr. LATTA. Thank you very much. The gentleman yields back the balance of his time.

And seeing that there are no further members wishing to ask questions, I want to again thank all of our witnesses for your great testimony.

Before we conclude, I would like to include the following document to be submitted for the record by unanimous consent—a letter from the Electronic Privacy Information Center.

And hearing no objection, that letter is part of the record.

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

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

And without any objection, the committee will stand adjourned.

Thank you very much.

[Whereupon, at 11:46 a.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]

## OPENING STATEMENT OF HON. GREG WALDEN

Good morning, and thank you to our witnesses for appearing before the Subcommittee today. Chairman Latta, I'm pleased to see the Disrupter Series continue with this subcommittee's focus on innovation, and American jobs and competitiveness. The Internet of Things' impact on the manufacturing sector has been transformative. I'm looking forward to hearing from the witnesses today about how their companies think about the best ways to utilize IoT, particularly if there are applications that improve safety for their employees.

Over the last year our economy has expanded because of the efforts of entrepreneurs and American workers, and also in no small part because of the lifting of regulatory barriers. New technologies have continued to play their traditional role in driving American innovation, creating new opportunities and lowering costs for consumers.

The Internet of Things is one of these technologies. In a sense the IoT is not new-industrial processes have long sought to create efficiencies through the acquisition and use of data. But revolutions in sensor technology, communications devices and data analysis have allowed manufacturers to utilize information in ways never before possible. Now machines can play an active role in their own operation, ensuring they are functioning properly and receiving attention when needed.

That said, there is also an important conversation to continue around training and filling the workforce gaps we see in our own districts. This issue is has many facets, certainly one is the opioid crisis, and it is important to hear directly from businesses about their experience training and maintaining their workforce.

There is bipartisan agreement that we want, and need, to see American manufacturing succeed. On that front there is great news: earlier this month the Institute for Supply Management reported that in 2017 U.S. manufacturing activity was the highest it has been since 2004, and in December continued to expand at its fastest pace in three months.

The renaissance in American manufacturing, empowered by new technology that drives efficiency and lowers costs, holds the promise of continued opportunities for future generations of Americans—and to keep good jobs here at home. As policy-makers all of us share the goal of removing barriers to innovation and productivity.

I look forward to hearing our witnesses describe the role of IoT in manufacturing, and how it can further drive America's recent successes in expanding job creation. I also hope that our witnesses will share with us any areas for improvement, where Congress can help remove obstacles and promote growth.

Mr. Chairman thank you for holding this hearing, and I yield back the balance of my time.

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

January 17, 2018

Representative Bob Latta, Chairman
Representative Jan Schakowsky, Ranking Member
House Energy & Commerce Committee
Subcommittee on Digital Commerce & Consumer Protection
2125 Rayburn House Office Building
Washington, D.C. 20515

**RE: "Disrupter Series: The Internet of Things, Manufacturing and Innovation"**

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the "Disrupter Series: The Internet of Things, Manufacturing and Innovation" hearing.[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things ("IoT") 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.[2] EPIC is a leader in the field of the Internet of Things and consumer protection.[3] EPIC urged the Federal Trade Commission ("FTC") to establish strong standards to safeguard American consumers.[4] And EPIC has testified before the House Oversight and Government Reform on the risks of "The Internet of Cars."[5]

**Privacy, Security, and Physical Safety Risks of the IoT**

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[6] These "always on" devices raise numerous

[1] *Disrupter Series: The Internet of Things, Manufacturing and Innovation*, 115th Cong. (2018), H. Comm. on Energy and Commerce, Subcomm. On Digital Commerce and Consumer Protection (Jan. 18, 2018), https://energycommerce.house.gov/hearings/disrupter-series-internet-things-manufacturing-innovation/.
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] EPIC, "Internet of Things (IoT)," https://epic.org/privacy/internet/iot/
[4] *See* Comments of the Electronic Privacy Information Center ("EPIC") to the FTC on The Privacy and Security Implications of the Internet of Things," (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf; *see also* In re Google Buzz, https://epic.org/privacy/ftc/googlebuzz/; FTC Facebook Settlement, https://epic.org/privacy/ftc/facebook/.
[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 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.

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.[7] Furthermore, software and hardware vulnerabilities also harm consumers. Last year EPIC joined other consumer advocacy groups in a letter to the Consumer Product Safety Commission to urge the agency to recall Google Home Mini.[8] Due to a hardware flaw, the device was always listening to conversations and users could not disable it. Therefore, both the intentional designs and unintentional flaws 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.[9]

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.[10] 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.[11] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[12]

**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

---

[7] 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.
[8] 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.
[9] *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.
[10] *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
[11] *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/.
[12] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

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.[13] 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 memo written by majority staff for this hearing points to the FTC as the key regulator of IoT,[14] but 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.[15] Manufacturers could be liable under tort law using products liability theory, but this legal strategy has not been employed much in the courts.[16]

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 Policy Fellow

---

[13] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, Understanding the Role of Connected Devices in Recent Cyber Attacks, 114th Cong. (2016).
[14] Committee Majority Staff, Memo to Members of Subcomm. on Digital Commerce and Consumer Protection (Jan. 16, 2018), http://docs.house.gov/meetings/IF/IF17/20180118/106781/HHRG-115-IF17-20180118-SD002.pdf.
[15] *See, e.g.*, EPIC, "Consumer Groups Ask Safety Commission to Recall Google Home," (Oct. 13, 2017), https://epic.org/privacy/internet/iot/
[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.