RPTR KERR

EDTR HOFSTAD

DISRUPTER SERIES: WEARABLE DEVICES

THURSDAY, MARCH 3, 2016

House of Representatives,

Subcommittee on Commerce, Manufacturing, and Trade,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 2123, Rayburn House Office Building, Hon. Michael C. Burgess, M.D., [chairman of the subcommittee] presiding.

Present: Representatives Burgess, Lance, Harper, Guthrie, Schakowsky, Kennedy, and Pallone (ex officio).

Staff Present: Leighton Brown, Deputy Press Secretary; Rebecca Card, Assistant Press Secretary; James Decked, Policy Coordinator, CMT; Graham Dufault, Counsel, CMT; Melissa Froelich, Counsel, CMT; Giulia Giannangeli, Legislative Clerk, CMT; Paul Nagle, Chief Counsel,

CMT; Olivia Trusty, Professional Staff, CMT; Dylan Vorbach, Deputy Press Secretary; Michelle Ash, Minority Chief Counsel, CMT; Christine Brennan, Minority Press Secretary; Lisa Goldman, Minority Counsel, CMT; Caroline Paris-Behr, Minority Policy Analyst; Diana Rudd, Minority Legal Fellow; and Matt Schumacher, Minority Press Assistant.

Mr. Burgess. The Subcommittee on Commerce, Manufacturing, and Trade will now come to order.

I will recognize myself for 5 minutes for an opening statement.

And I do want to welcome all of our witnesses here today and welcome everyone to another installment of our disrupter series hearings. Today, we will examine wearable technologies and how they are disrupting traditional business processes and transforming ways that consumers can engage in commerce.

Last year, we held a hearing to examine the Internet of Things, a network of Internet-connected physical objects that gather information in realtime to predict circumstances, prevent problems, and create opportunities. That market has now matured, and wearable technologies have come to represent a growing segment within that digital ecosystem of interconnected devices and their applications and platforms.

The defining characteristic of wearables is that they offer consumers and businesses access to realtime, highly personalized information through products and devices that are physically worn by the user. Many of us are familiar with fitness tracking bands on the market today. They gather information about an individual's physical activity, or lack thereof, and are intended to motivate users to improve their fitness, wellness, and health regimens.

While inspiring better fitness habits is a positive use of wearable technology, the societal and economic benefits of these products extends far beyond those applications. We are just beginning

to see the potential of wearable technology across multiple economic sectors and industries, such as energy, health care, transportation, retail, professional sports, manufacturing, education, and others.

In manufacturing, for example, wearables can provide businesses with greater insight into the daily operations of their production practices, their workflows, their supply chain processes.

In sports, coaches and athletic trainers can use wearables to better assess player recovery time and inform return-to-play considerations to reduce the risk of further injury. I just think back to my own brief high school sports career. The coach would know if I was dogging it realtime. He wouldn't have to accuse me; he would have the data.

In the automotive sector, wearable technology can sense early signs of driver fatigue, prompting the wearable device or vehicle to send alerts or another type of warning to the driver.

And in the retail industry, retailers can use wearable technology to customize product offerings and better meet consumer preferences and demand.

The appeal of this technology is pervasive because of what it can offer in terms of operational efficiencies, public safety, improved performance, and cost savings for every business type and size. The potential for wearable technology is virtually limitless.

Much of the excitement surrounding wearables is rooted in the promise to create new opportunities for economic growth, economic development, and job creation. Wearables create economic

opportunities by providing insights into an individual's behavior and driving changes to that behavior to improve job performance and job execution. This can lead to increased productivity and efficiency, helping a business reduce waste and optimize resources.

The technology also facilitates smarter decisionmaking, increased information-sharing, and augmented interactions amongst workers. The productivity gains achieved through these operational advances are fundamental to a stronger and more prosperous economy.

As with all connected technologies, there are important privacy and security considerations that should be part of today's discussions. Unlike other connected things within the Internet of Things, such as connected thermostats, streetlights, and refrigerators, wearables are physically worn by users and capable of extracting highly personalized information about an individual's activities or whereabouts.

In our examination of these issues, it will be important to understand how consumers are using these technologies and how they will be protected while preserving the flexibility and the ingenuity of the innovators that are driving this market forward.

Once again, I want to thank our witnesses for taking the time to inform us about the applications and future potential.

I recognize the gentleman from New Jersey, 5 minutes for an opening statement, please.

[The prepared statement of Mr. Burgess follows:]

******** COMMITTEE INSERT ********

Mr. Pallone. Thank you, Mr. Chairman.

Today's hearing gives us an opportunity to look at a diverse and quickly developing field. Wearable technology, part of the broader Internet of Things, provides consumers with capabilities that would have seemed more like science fiction than reality only a decade ago.

Today, you can buy a wristband that measures UV exposure, helping you avoid sun damage, or a sensor that sticks to skin and teaches you how to stretch to alleviate back pain or smart shoes that give you directions through buzzes to their feet.

Researchers from WINLAB, the Wireless Information Network Laboratory at Rutgers University in my district, collaborated to design a wearable that could replace passwords for head-worn devices by authenticating the user by measuring the unique movements of the head in response to audio stimulus. WINLAB reports that the device can accurately tell that the right person is wearing it at a rate of over 95 percent through tiny movements of the head alone.

Many wearables measure biometric data, giving consumers access to a wealth of personal information. Not long ago, if someone wanted to know their heart rate, quality of sleep, and calories burned, they would have had to be hooked up to a roomful of equipment. Today, they can simply put on a small bracelet and have all of that information at their fingertips.

And these are amazing advancements, but with these new innovations come new vulnerabilities. For example, when a doctor measures your heart rate, that information is protected from

unauthorized disclosure. Those privacy protections do not apply to the same information collected through most wearable devices. And there are no standards for encryption or other security measures to protect the data wearables collect.

Long and complicated user terms and agreements have further compounded the problem. Some include clauses saying that the data they collect belongs to the company, not to the user. Most of us do not read every online user agreement word for word, so many wearable users are surprised when they learn that they may not own their own data.

Whether by sale or by data breach, the release of personal information from wearables can have serious implications. Employers, credit agencies, and health insurers can all use the data collected from wearables to draw inferences that may have a negative effect on the user.

As with other Internet of Things products, by building in security from the beginning, manufacturers of wearables can more effectively prevent hackers from gaining access to a device or the data it collects. By building in privacy, consumers can have confidence in these products and buy them knowing that highly personal information will not be shared without their consent.

So I look forward to discussing the many great innovations in wearable technology today, but with these innovations we must also devote serious attention to how we can better protect consumers and their personal information in this space. When privacy and security are made a priority, both businesses and consumers benefit.

I yield back, Mr. Chairman.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

Mr. Burgess. The chair thanks the gentleman. The gentleman yields back.

The chair would inquire of the gentlelady from Illinois if she wishes to make an opening statement.

Ms. Schakowsky. I have a short statement.

Mr. Burgess. You are recognized for 5 minutes.

Ms. Schakowsky. Thank you, Mr. Chairman. And I really apologize for being late. I thank you, and I thank our panel.

So wearable devices have taken off in the last couple of years. I am sure there are a lot of people in this room who are wearing a Fitbit or some similar device. I happen to have lost mine. It fell off the first week I got it, and I haven't replaced it.

Companies have developed numerous applications in medical testing and health monitoring. For consumers, wearables mean convenient collection of detailed data. There is clearly great potential here, but as I am sure has been said before -- and I know Chairman Pallone did -- we need to make sure the consumers fully understand what they are getting into.

Let's talk about health applications. When a hospital collects your health information, that personal data is protected by HIPAA. Your healthcare provider is not allowed the share that information with marketers or send it to your employers without your consent. However, those privacy protections don't apply to most wearable devices.

In addition, consumers have been surprised to find that they don't own the data collected through their devices. Last year, Lark, a

company that created a sleep coaching wristband, stopped supporting its device and the related app. Lark's customers lost easy access to their data. At the same time, Lark's privacy policy stated that it could sell this personal information if it is acquired or goes bankrupt.

This matters to consumers, because some of the data they collect through wearable devices is very valuable. Minute-by-minute data from a fitness tracker can be enough to determine your gender, age, stress level. That is why it is vital for wearable device companies to adequately protect consumer information.

Last year, the Federal Trade Commission issued a report concluding that companies making these devices must adopt reasonable security measures. The FTC also recommended that Congress enact baseline consumer privacy legislation for such devices. In today's hearing, I would like to delve deeper into these privacy concerns as we consider how today's laws must evolve to fit tomorrow's technology.

Here are some basic principles that I think we should start from. Consumers should be able to expect that a company collecting their personal data is protecting this personal data. Consumers need to be informed what, how, and when data is shared. In addition, they need to know if they may lose access to information they have collected through a wearable device. Technology is developing rapidly. We need to ensure consumer protection keeps pace.

With that in mind, I would like to welcome our panelists. Your testimony is important to informing this discussion.

I yield back.

[The prepared statement of Ms. Schakowsky follows:]

******** COMMITTEE INSERT ********

Mr. Burgess. The chair thanks the gentlelady. The gentlelady yields back.

This concludes member opening statements. And the chair would remind members that, pursuant to committee rules, all members' opening statements will be made part of the record.

We do again want to thank our witnesses for being here, for taking their time to testify before the subcommittee.

Today's witnesses will have the opportunity to give opening statements, followed by a round of questions from members. Our witness panel for today's hearing will include Mr. Thomas Bianculli, vice president for enterprise technologies at Zebra Technologies -- you guys got out of order -- Meg Burich, director of commercial development and marketing for Adidas Digital Sports; Suresh -- help me pronounce your last name.

Mr. Palliparambil. Palliparambil.

Mr. Burgess. Turn your microphone on, please.

Mr. Palliparambil. Palliparambil.

Mr. Burgess. Suresh, welcome to the hearing.

Mr. Palliparambil. No problem.

Mr. Burgess. -- the director of sales and business development for NXP; Mr. Scott Peppet, professor of law at the University of Colorado School of Law; and Mr. Doug Webster, vice president for service provider marketing at Cisco.

We do appreciate you all being here with us today.

We are in the middle of a vote on the floor, but, Mr. Bianculli,

I think we have time if you would like to give your opening statement. Then we will take a brief recess and come back and resume.

You are recognized for 5 minutes, please.

STATEMENTS OF THOMAS D. BIANCULLI, VICE PRESIDENT, ENTERPRISE TECHNOLOGIES OFFICE, ZEBRA TECHNOLOGIES; MEG BURICH, DIRECTOR OF COMMERCIAL DEVELOPMENT AND MARKETING, ADIDAS DIGITAL SPORTS; SURESH PALLIPARAMBIL, DIRECTOR OF AMERICAN SALES AND BUSINESS DEVELOPMENT, NXP; SCOTT R. PEPPET, PROFESSOR OF LAW, UNIVERSITY OF COLORADO LAW SCHOOL; AND DOUG WEBSTER, VICE PRESIDENT, SERVICE PROVIDER MARKETING, CISCO

STATEMENT OF THOMAS D. BIANCULLI

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

I am the vice president of the Emerging Technology Office at Zebra Technologies Corporation in Lincolnshire, Illinois. With nearly $4 billion in annual revenue, Zebra is a global market leader in a number of advanced technologies, including the Internet of Things and the related area of wearable technology.

While many Americans may not recognize Zebra by name, 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 Zebra scanners, mobile computers, and wireless infrastructure.

Our pioneering technology vision and trusted enterprise solutions, particularly our wearables that are the focus of today's hearing, are dedicated to helping business, government, and nonprofits make smarter decisions and take smarter actions by providing them with realtime visibility and mission-critical information in an ever-more-efficient manner.

Zebra commends the subcommittee for hosting this series of hearings on technological disrupters. Mr. Chairman, I will stress five key points.

First, let me begin with Zebra's role in the wearable market. Zebra's leadership in this market derives from our recreation of the overall wearables product category nearly 25 years ago. With the launch of our wrist-mounted terminal and ring scanner in 1992, we invented the first handheld laser barcode scanner, the first barcode printer, and the first WiFi-enabled mobile computer. We remain at the very forefront of breakthrough innovation as we continue to create wearables that go from the wrist and hand, as you see before me, to lanyards and heads-up computing solutions.

Second, we commend the subcommittee for its recognition of the wearable category as a disrupter. Wearables earn this status because they empower workers with total hands-free mobility in a manner that also provides instant access to business-critical information.

Instead of needing multiple devices that are all directed by hand, wearables enable new levels of productivity by providing employees with tools that marry natural language interaction with immediately

available information, be it visual, verbal, or augmenting the user's physical reality.

Imagine, Mr. Chairman, a simple verbal command that provides a worker with full access to data and subject matter expertise in realtime. Imagine, further, the same worker using another verbal command to respond back and transmit data or pictures to a main office, a remotely located colleague, or to another machine. Now imagine having that ability while suspended high above the ground repairing the electrical grid or working inside an aircraft, no hands required. Wearable technology makes it happen.

Third, I would like to offer a quick look into the future. Awareness and acceptance of smartphone technology has grown at a tremendous pace and has built the foundation for wearable device adoption. Current technologies will continue to evolve and revolutionize the way people instinctively work with computers and intuitively interact with their virtual or augmented reality environments. It is not an overstatement to say that the possibilities of these devices are limitless.

Over the next few years, they will get smaller with technological improvements in computing, analytics, power, and display optics. As part of this trend, we will continue to advance our portfolio of wearables. We are presently focused on developing an augmented reality wearable system for true hands-free application, providing a future solutions approach for uninterrupted workflow and opening up the possibilities of what realtime, eye-level information can do.

Fourth, the economic benefits of wearables come from its significant impact on productivity across virtually every industry and economic sector. This is because visual computing or the ability to work hands-free while receiving eye-level information will drive a major paradigm shift in how we, as humans, directly interface with computers. Visual or hands-free computing will enable this kind of frictionless, uninterrupted workflow. Even a small increase in the efficiency of manufacturing or warehouse workers through wearables could bring a profound economic benefit to our economy.

Fifth and finally, we urge Congress and the administration to take a light touch where wearable technology is concerned, for the same reasons that many in industry as well as in Congress and the administration have advocated for a light regulatory approach to the Internet of Things.

The primary challenge is to allow for the rapid development, deployment, and subsequent advancement of wearables in a manner that simultaneously addresses concerns over data, security, and encryption. The goal is to encourage technologies which provide enhanced, secure, and realtime visibility and access to information in a way that empowers workers to undertake more effective and timely decisions and actions.

To this end, Mr. Chairman, Zebra stands ready work with the subcommittee in advancing policies which keep the United States at the leading edge of this exciting technology. And I again thank you for the opportunity to provide our views on wearables, and I look forward to your questions.

[The prepared statement of Mr. Bianculli follows:]

******** INSERT 1-1 ********

Mr. Burgess. The chair thanks the gentleman.

Because of the vote, we are going to go into recess.

Look, I want you all to know what you are up against with this congressional panel. Look at his notes, all stuck together and handwritten. You are down there with all of these fantastic technological devices, and we are kind of in the Stone Age.

But thank you for your forbearance. We are going to go vote. We will reassemble as soon as the last vote is over.

Mr. Bianculli. Thank you, Chairman.

[Recess.]

Mr. Burgess. I thank everyone for their forbearance. The subcommittee will resume.

We will resume with the testimony of Ms. Meg Burich from Adidas Digital Sports.

EDTR ROSEN

STATEMENT OF MEG BURICH

Ms. Burich. Good morning, Chairman and members of the subcommittee. Thank you for having me.

Mr. Burgess. If I could just ask you if your microphone is on?

Ms. Burich. It is on.

Ms. Schakowsky. Pull it a little more closer.

Ms. Burich. Yeah. Okay. I am Meg Burich here on behalf of Adidas Digital Sports, and I am director of marketing and commercial development.

Adidas Digital Sports is the business unit within Adidas that drives the development of wearable technology. Our team consists of technology experts in the fields of data science, experience design, industrial design, algorithm development, software and hardware engineering. We have centers of excellence located in Portland, Oregon, Chadds Ford, PA, and Herzogenaurach, Germany where our headquarters is.

We have been active in the wearable space for over 15 years, with the first commercial launch of sensor-enabled footwear in 2001, and the introduction of real-time coaching under the Adidas miCoach brand in 2008. MiCoach offers real-time coaching to users, enabling them to achieve their goals by training with heart rate, speed, and distance

to run faster and further.

Today, we are repositioning our wearables offering to address the growing opportunity for the larger population to benefit from this technology. All these products are enabled by companion software applications designed for mobile or desktop.

I am going to go through three examples to demonstrate the range of applications for wearables in sports, fitness, and health, and the first one will be related to schools and school children.

Adidas is partnering with Interactive Health Technologies to make fitness personal for kids in phys ed classes. Instead of competing with each other, kids can wear an Adidas heart rate monitor that uses simple color zones to guide them through a fitness challenge. Wearable technology gives every kid the chance to know the good feeling that comes from a successful workout.

Next, I would like to cover the use of wearables in competitive and professional sports. We have a system. This is the jersey that athletes wear on the training field. Coaching software is coupled with this system, and coaches can see in real time what results are coming from the athletes on the field. So instead of just driving them to train as hard as they can, they are really trying to train them in a smarter way, and in professional sports, there is kind of a fine line between peak performance and injury, so you want to really have this data to help you tell when you are really stressing an athlete versus when you are coaching him to the level where he can perform better.

Adidas uses in-depth experience with professional athletes and

coaches to understand the cutting edge of performance. We also believe that all athletes and fitness participants deserve the best coaching, so we take what we learn working with the elite athletes, and then we translate that to smart systems for consumers, because consumers don't always have the option to hire a professional trainer. So we are making those consumer systems smart systems based on what we know about the cutting edge of coaching.

The third use case that I am going to go into focuses on women, and this is kind of a pivot for us in terms of how we see the market and the opportunity. Today, we know that women are managing their own health, and they have multi-generational influence. They are supporting healthcare decisions of their families and of their parents sometimes, so they are really kind of that officer of health.

These women are also the main users of fitness apps and devices. They are participating in digital social communities that help them stay engaged in their fitness routine. They may be going for a daily walk, getting ready for a 5K, or training for a marathon, but we have coaching solutions that will help them achieve their goal.

We have been talking a lot to women and researching their needs to understand what they are looking for, and basically, women are saying step counting is not enough. When they have a step counter, they either lose it or they drop it within 3 to 6 months. In fact, nearly 40 percent stop using it after 6 months. So we know they are looking for insights beyond how many steps they took. They really want the picture of their whole health, and managing it in a proactive way is important to them,

so they are looking for tips on nutrition, they are looking for exercise tips, they are looking for guidance for how much to move during the day, how much they should sleep, and how that connects to their whole health and wellness.

So we know it is hard to stick to an exercise routine, and we are looking at how we can help women through digital wearables and digital experiences to stick with their exercise routine throughout their life, because we know that has an overall impact on health, disease prevention, and keeping people well. So we really believe that wearables is in its infancy, and wearables 2.0 is where we need to go, connecting consumers to health care and keeping them kind of on the wellness side. Thank you.

[The prepared statement of Ms. Burich follows:]

******** INSERT 1A-1 ********

Mr. Burgess. The chair thanks the gentlelady, and the chair now recognizes Mr. -- try again, Palliparambil.

Mr. Palliparambil. You got it.

Mr. Burgess. 5 minutes.

Mr. Palliparambil. Thank you.

Mr. Burgess. Plus the 1 minute it took me to pronounce your name.

STATEMENT OF SURESH PALLIPARAMBIL

Mr. Palliparambil. Thank you. Good morning, Chairman, and members of the committee. Thank you for holding this important hearing on wearable technologies today. My name is Suresh Palliparambil, and I am the America's director of sales and business development for NXP's secure identification solutions business line.

NXP helps to make today's ideas into tomorrow's exciting reality as the supplier of end-to-end solutions that range from semiconductor ICs to infrastructure components and secure applications.

We are the inventor of MIFARE and the co-inventor of NFC, the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds. NXP powers and enriches the IoT as a high-level contributor to standards bodies, including the FIDO Alliance, whose work promises to usher in a new era of online security, making the need to remember complex passwords a thing of the past.

As a proud employer of nearly 7,000 staff members in the U.S., NXP is committed to security leading -- leading edge design and bringing

products to the domestic market that have a substantial share of domestically built content and local value add to end products in which NXP plays a role.

Our company is dedicated to leveraging all of those resources and partnering with America's leaders to invest in the country's future and safer, more convenient lives for its citizens. From rockets in the air, to cars on the road, and cards in your wallet, our innovation at NXP has been integral to America's past and the success it enjoys today. As an important legacy as that is, we at NXP are looking to the future in building a better, easier, and safer tomorrow with exciting leading-edge technologies of utmost quality.

This is no small task. The rapid expansion of public and private data networks, the rise of social media, and the mass deployment of smart objects across the Internet of Things, IoT, have connected us in ways we didn't think possible two decades ago. They have also left us open, vulnerable, and exposed.

To counteract these vulnerabilities, NXP is focused on, one, avoiding unauthorized access in public and private areas of the IoT, developing tamper-resistant secure element devices, and perfecting the end-to-end solution that power the new, often wearable technologies will use to improve and simplify health care, entertainment, transportation, and the rest of our everyday lives

Online security can mean different things to different people, but the task of keeping data private and ensuring cyber safety essentially comes down to one thing, access.

NXP has made authentication a top priority for more than 20 years and has continually reached new levels of performance by making algorithms more resilient, and by increasing the robustness of secure elements. We are recognized as leaders in authentication, known for our ability to deliver trusted security in many of the world's most high-profile applications.

NXP produces chips that have their own unique fingerprint based upon their crystalline structure, so no two chips are alike, preventing cloning. NXP's strength in authentication is closely tied to eGovernment and banking. With roughly 80 percent market share of the electronic passport market, our technology is trusted by more national governments to increase security while reducing wait times at international borders. We are helping governments expand the use of electronic documents, and our repeated success with large-scale implementations of electronic IDs, public transportation, and multi-application cards, which combine payment, transportation, identification, and other services on a single card make a trusted partner to municipalities, transit authorities, and banking and payment organizations worldwide.

NXP brings a comprehensive set of skills to each authentication challenge and leverage outstanding relationship with broad spectrum of security leaders to develop and deliver tailored solutions that address needs in the market. The evolution in wearable technology is all about enhancing users' lives and making everyday functions simpler and easier so we can concentrate on the things that matter.

NXP creates the security, connectivity, and circuitry solutions that enable these wearable devices their convenient applications in today's society and the innovative ways they could be used in the future.

Many applications for wrist-based wearables are in place through entertainment venues and in the healthcare industry. The most popular example include keyless entry, smartwatches for luxury cars, Disney's RFID wristband, the MagicBand, an all-in-one device that serves as a room key, a park ticket to get in line, and also the payment, too.

There are already many existing areas where smartwatches could improve users' lives. Today's keyless entry for vehicles will probably move to a wearable platform, and in the future, watches will act as the key for an entire car. In fact, most luxury car makers already offer their own wristwatches. It is a great channel to make -- to help build their brand recognition.

In the home environment, smartwatches will interact with communication protocols such as ZigBee and Bluetooth, allowing users to control the home environment. Heating, lighting, AV equipment and more, will all be controlled by simply making a gesture with an arm or using apps installed on the watch. Soon, the smartwatch will be the only key anyone needs, the technology passport that gives access and control to your entire life.

NXP is working hard to simplify lives of citizens to secure transactions in the connected world, and we currently have the following tools and accomplishments in place to enable the securely connected -- to securely connect the next generation devices. We have

a smart microcontroller platform; we have MIFARE, the world's leading contactless technology platform; Near Field Communications, which is a wireless proximity and contactless technology; and then high-level contributions to standards bodies, including the FIDO Alliance for online security.

Thank you for the opportunity to participate in today's hearing. Thank you very much.

[The prepared statement of Mr. Palliparambil follows:]

******** INSERT 1A-2 ********

Mr. Burgess. The chair thanks the gentleman. Mr. Peppet, Professor Peppet, you are recognized for 5 minutes for your opening statement, please.

STATEMENT OF SCOTT PEPPET

Mr. Peppet. Chairman Burgess, Ranking Member Schakowsky, members of the subcommittee, I appreciate the opportunity to talk to you about wearables. I am a professor of law at the University of Colorado Law School in Boulder, where I work on markets, technology, and privacy. I should say I am also a member of the board of directors of Anixter International, an Illinois-headquartered company, so my remarks today are in my own capacity, and in no way represent Anixter or anyone else

I also want to say I am involved with four entrepreneurship and innovation centers: one in Colorado, one at Kellogg in Illinois, and one at the University of Michigan, and one actually in Israel at a university called IDC. And in that, in those roles, I have worked with student teams creating startups, many of whom are interested in or working in the wearable space. So I sort of got various perspectives on this -- on this set of issues.

These are exciting technologies, and I agree with my fellow witnesses who have said how much innovation is happening in this space, and I agree with all of that and just want to focus on three things in terms of privacy and security that I think deserve attention.

The first is one that you have already mentioned, which is data

security, and I think there are two issues in data security. The first is, is the device itself secure? And that is a technical matter. Mostly, we know from research, that many of these devices have not been secured in the first wave of consumer devices, for example, and the reason is obvious: They are small, they are generally designed to be relatively inexpensive. It is hard to pack data security measures into a thing with a small processor, very limited connectivity, they are hard to update because they don't talk to the Internet that frequently.

And so it has been a challenge, and the FTC has worked with companies, continues to work to try to push companies in that space, or in the security issue, and I think we will see more innovation there to try to resolve some of those questions.

The second data security issue is actually not about the device, it is about the data. What happens to these data once they are off the device, they are stored in a company's cloud server somewhere, and someone hacks into that server. At the moment, if your credit card information is stolen from Target, for example, as you have all heard about that example, Target has to say, Hey, we were hacked, and they have to notify the public. That is our market-based response to data security in this country is to say, Listen, give consumers information, they will then choose with their dollars or their feet whether they want to go back to that store.

In all but one State, and Mr. Chairman, it is the great State of Texas, only Texas' data breach notification statute would actually apply to biometric data coming off of most of the wearables that we are talking

about in the consumer space. The rest of the States really have not yet seen the risk that these incredibly sensitive data, as you said, pose if they were to be hacked, which I think is an odd and sort of unfortunate anomaly.

To the extent that Congress ventures into the data breach notification area, that is something that it should consider. So that is security.

The second thing I will talk about is use, and I will just give a very simple example. There are lots of different devices at the moment being used in hospitals that keep track of whether a hospital worker washes his or her hands when they use the restroom. What they do is they have a lanyard on, you know, or some kind of ID badge, and there is a device at the sink and it literally just says how long did they spend standing in front of the sink? And then if they approach a hospital bed and they haven't washed their hands properly, the device -- their lanyard starts to buzz and say, hey, wait a minute, and it records that they have done that, and that is not a good thing.

That is a great idea, right? I think that is a terrific idea. I hope that every hospital I ever use has that, and employees, consumers, whoever we are talking about, need to know what those kinds of data are being used for. So for example, there might be no issue at all for a hospital or an employer using the data coming off a wearable for the obvious use that it was designed for, but I would guess that if one of the hospital employees discovered that their hand-washing habits had leaked out into data brokerages and was being used in credit decisions

or insurance decisions or any other kind of decisions in the economy, they would be both surprised and unhappy. So the use issue is a very complicated one.

And the last one I will say something about is consent. Consent is hard, particularly in the consumer space, for these little devices. A study that I did, I brought 20 of these very popular devices, I opened all the boxes, and I looked inside. There is almost never any privacy information. I have no idea -- I didn't test Adidas', but there is almost never privacy information in the box. Sometimes you get the privacy information when you download the app that pairs with the device. Often, you are sent to the Web site or you have to go to Web site of the firm, and often, when you get there and you read their privacy policy, it doesn't apply to the data coming off the device. It applies to the use of the Web site.

So at the moment, we are in a bit of a backward situation on how to give users and consumers, in particular, good information about these devices. Is the device information protected? Who owns the data? Can users go in and delete their data? Many have discovered that they can't, so their fitness data is being stored in the cloud somewhere and they say, I don't want to use this device anymore. They didn't just lose it. They affirmatively decided they don't like it anymore, and they say, I want to get my data back. I don't want you to have it anymore.

Many companies actually will not permit that or permit editing of this data. And most important, who is the data being shared with? Can it be sold in a bankruptcy, in an acquisition, or just in general?

So again, the FTC has been giving -- working with industry to try to come up with some guidance on those issues, but that -- those consent questions are very difficult at the moment.

I will stop there. Thank you for allowing me to testify.

[The statement of Mr. Peppet follows:]

******** INSERT 1A-3 ********

Mr. Burgess. The chair thanks the gentleman. Mr. Webster is recognized for 5 minutes for your testimony, please.

STATEMENT OF DOUG WEBSTER

Mr. Webster. Thank you, Mr. Chairman and members of subcommittee. The Internet has revolutionized the world around us, transforming the way we use and share data to communicate, to collaborate, and consume entertainment and information. Yet, the next wave of technology isn't about moving data from one place to another, it is about connecting physical objects to the Internet on an unprecedented scale.

Now, increasingly, the things connected are the shirts on our backs, the glasses on our foreheads, the watches on our wrists, and the jewelry around our necks, and collectively, these emerging devices are referred to as wearables.

To be sure, some wearables are mere novelties. However, many others, like the Fitbit or Apple watch, are improving our health and wellness by tracking our daily activities, and the most advanced wearables have the power to save lives and improve patient outcomes. For example, there is an FDA-approved heart rate monitor that provides precise information from cardiac patients to their physicians between visits to the doctor's office.

Another device looks like a typical smartwatch, but in reality, it helps epileptic patients manage their stress and alert family members and physicians when a convulsive seizure happens.

And a third, a prototype in development, is a glucose-monitoring contact lens that allows diabetics to monitor their blood sugar continuously, and the possibilities are endless here. I mean, virtual reality goggles that provide for immersive education, connected football helmets to alert the team physical to a possible concussion, GPS-enabled slippers to make sure an elderly relative is getting out of bed and doesn't wander off, and accessories that make mobile payments faster and easier.

Now, the one feature that unites these devices is their wireless connectivity to the Internet. Each contains a tiny radio transmitter that sends data to a receiving device, such as a WiFi router or a smartphone, and then the data is transmitted over an IP network to a server or data storage facility.

Now, once online, software allows you to visualize and analyze the data to help improve decisionmaking, whether it is information about your daily run, your average number of steps per day that gauge your fitness progress, or simply storing videos so you can decide whether to post it at a later date.

Now, at Cisco, we have been monitoring the growth of wearables for 3 years, and it is fair to say that these devices are poised to take off. Here is the forecast from our most recent Cisco mobile visual and networking index report. By 2020, we forecast approximately 600 million wearable devices globally, up from 97 million in 2015.

Now, fewer than 15 percent of these devices are expected to be directly capable of transmitting on a cellular network. Most, instead,

will use WiFi or Bluetooth to connect to the Internet. Now, the data generated by wearables represents a tiny trickle in the larger stream of mobile data, mostly because only a few of these devices are being used to transmit video.

Traffic from wearables is forecast to account for only 1 percent of total mobile data traffic by 2020, even as the amount of data generated by each device is expected to grow.

Now, North America has a 40 percent share of global connections today, and it is because we are early adopters, but that falls to 30 percent by 2020 as Europe and Asia catch up with us. By 2020, there are forecasts to be over 180 million wearable devices in use in North America, compared to about 40 million today, representing a 4-1/2-fold increase in just 5 years.

Now, given this growth, it is important for policymakers to understand the issues affecting wearables. We need to ensure that radio spectrum is available with the right set of rules to make sure these devices can connect to the network, to encourage policy that support investment in the service provider networks that are needed to transport data to the Internet.

We need policies that encourage startups and small companies by ensuring access to venture capital to tax policies that support research and development, as well as encouraging more young people to enter careers in science, technology, engineering, and math, also known as STEM. And we need to ensure that device manufacturers and applications developers understand privacy and security threats and take the steps

to protect their devices and the personal information of consumers.

Here is the bottom line: Wearables represent a measurable component of the mobile landscape, and they are projected to continue to grow. They hold incredible promise to improve our lives. Public policies that encourage the development of this category should be supported so that the United States can continue to be a leader in this next chapter of the Internet.

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

[The statement of Mr. Webster follows:]

******** INSERT 1A-4 ********

Mr. Burgess. The chair thanks the gentleman. Thanks to all of our witnesses for your testimony. We will move into the question-and-answer portion of the hearing.

I would begin the questioning this morning by recognizing Mrs. Brooks from Indiana for 5 minutes for questions.

Mrs. Brooks. Thank you, Mr. Chairman. Thanks for holding this hearing. I happen to be one of those brand new users, just acquired a couple of weeks ago. I kind of wish I had been a part of this hearing before I bought this. However, I am excited to be part of the wearable technology consumer base, and, in fact, bought several of these for my parents and in-laws for the holidays.

And so we often think about fitness trackers when we hear wearable technology, and so we are certainly learning a lot, and when, in preparing for this hearing, learning about innovations in manufacturing. In Indiana where I am from, is a heavy manufacturing State, one of the top manufacturing States in the country.

And so, Mr. Bianculli -- I am not sure I caught --

Mr. Bianculli. Bianculli, yes.

Mrs. Brooks. Bianculli, what kind of cost savings -- can you talk a little bit more about wearables with respect to manufacturing?

Mr. Bianculli. Sure.

Mrs. Brooks. What kind of cost savings can be expected in this area, and how do we achieve this in the manufacturing sector?

Mr. Bianculli. Yes. Absolutely. Thank you, Congressman.

Looking in the manufacturing sector and breaking it down really

into kind of three major components: raw materials coming into a manufacturing facility, those raw materials being processed in the outbound side of that where the goods are sorted, picked, packed, loaded, and then transported down the supply chain. Some of the early adoption we are seeing for the kinds of wearables I spoke about, which is basically being able to capture and get the right information in front of a worker in real time have been on the third category, picking, packing, sorting.

Think about an eCommerce order that is being built, think about an order that is coming from a manufacturer to a distribution center, being able to sort the goods, load those goods, be able to optimize the volumetric efficiency of those goods onto a trailer or onto a pallet for distribution. A lot of these cases, we are starting to see be adopted or using wearables to seamlessly present information in front of the user as they are going through their workflow to be able to get the right goods in the right place, to be able to optimize the way they are loaded onto vehicles, and to be able to get them down and through the supply chain faster than they have previously.

So it is really about worker productivity. I use the word in my testimony about frictionless workflow, so think about it as taking the -- literally taking the friction out of the workflow and allowing workers to simply get their job done and let the technology take a back seat and just augment their capabilities

Mrs. Brooks. Thank you. Ms. Burich, so my daughter was a college athlete and -- but many -- several years ago, and so none of

this technology. In fact, when she was in youth soccer, that is when Under Armour came to be, okay. So just talking about that type of advancement during this time period and now all of this wearable technology. What do you anticipate -- how do you anticipate it being used from the youth -- the youth sector all the way up to the professional athlete sector?

Ms. Burich. Yeah. We look at the market in terms of like team sports and individual sports or individual --

Mrs. Brooks. Can you turn your mike on, please.

Ms. Burich. We look at the market in terms of like team sports, organized sports, which is what you are referring to, and then individual use for fitness, so where we have our elite system, it is very sophisticated, and there is definitely an opportunity to translate it for -- for youth sports, and I would call -- say recreational team sports to high school, even colleges who can't afford the solution today. So that is a development and an opportunity for growth, and again, it is something that the technology and capability is there and it should be accessible to more -- to broader population.

And then, I think, just connecting that down, there is probably -- it turns into more of the individual use case where you want kids in phys ed to be using technology so that it is -- they are not -- so that you are giving them the right amount of exercise for their fitness condition, and you are not overstressing them.

Mrs. Brooks. And these kids at all ages are so tech savvy from a very, very young age --

Ms. Burich. They like it.

Mrs. Brooks. -- so they are going to love this.

Mr. Webster, just shifting gears very briefly, you talked about the spectrum. Are most wearable devices operating on unlicensed spectrum or licensed spectrum, if you know, and could the spectrum be an obstacle hindering widespread adoption of these devices? We are getting ready to have an auction with respect to the spectrum. Can you just talk a little bit more about the spectrum issues?

Mr. Webster. Yes, ma'am. Our forecast indicates about 15 percent of all wearables will directly be connected to the Internet that would be using a license spectrum. The vast majority or 85 percent of them will be connected via unlicensed spectrum to the respective Internet-connected device.

Now, it is important to know that wearables is just one small part of an even larger Internet of Things --

Mrs. Brooks. Right.

Mr. Webster. -- initiative, and so when you take that all in mass, then absolutely, the importance of continuing to increase the amount of license and unlicensed spectrum will be key to help really make this industry segment that is so beneficial to so many continue to prosper.

Mrs. Brooks. Thank you. Thank you all for your testimony. I yield back.

Mr. Burgess. The gentlelady yields back. The chair thanks the gentlelady. The chair recognizes the gentlelady from Illinois, 5

minutes for questions, please.

Ms. Schakowsky. Mr. Peppet, I am going to ask you some questions, but I wanted to first -- this idea of kids. To me, I am a little concerned about that. Is this going to be more anxiety-provoking, now we are measuring and another way that you have to look at an electronic device.

I am just wondering if Adidas, in marketing to children, has talked to child psychologists, to educators on whether or not, as you say, that forget the awkward, social situation, et cetera, I mean, that could be a positive. But I feel like now encouraging kids to measure their every step or their heart rate or something, I am just wondering if you have done the kind of research I think would be important before we really market this to grammar school kids, or middle school kids.

Ms. Burich. I would say in the -- in that space, we are providing a piece of a system that our partners are providing them to the schools. I don't know how much research they have done in that area. I know they have done research and they have positive findings from the use of technology related to attendance and kids' grades and other things that this is impacting.

Ms. Schakowsky. There is also, you know, a real pushback on all the testing that is going on. I kind of feel like this may be in that category. I just wanted to raise that. I don't immediately accept that this is a great thing to push to kids.

But anyway, let me just raise that and go on to Mr. Peppet, who actually -- and you have a quote at the beginning of your testimony:

Very soon we will see inside ourselves like never before with wearable, even internal sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge.

In a way, I think I am getting at that with that earlier question, but here is what I want to get more specific.

In January of last year, the Federal Trade Commission released a report entitled, quote, "Internet of Things, Privacy and Security in a Connected World." In the report, the FTC states that there is, quote, "a need for substantive data security and breach notification legislation at the Federal level, and that such legislation should, quote, 'protect against unauthorized access to both personal information and device functionality.'"

So in your testimony, Professor Peppet, you say that small sensor-based connected devices like wearables are inherently prone to security problems. Can you explain what you mean by that? What are some of the vulnerabilities specific to wearable devices?

Mr. Peppet. Sure. Thank you for the question. The -- as I said, the devices tend to be small, they tend to be designed for a low price point, and they tend to have very limited computing and even communication power, and that presents a whole set of security challenges.

When the first wave of fitness trackers came out, security -- computer science -- you know, security folks discovered very quickly how easy it was to hack into them, largely because they

hadn't secured whether it was the Bluetooth connectivity or the WiFi connectivity, whatever they were using, they hadn't secured those connections. And you know, that was several years ago, some of those studies were done.

A study came out, I think, 3 weeks ago, testing some of the most current and most popular versions of those devices and found, essentially, the same set of results. So there -- when I talk with computer scientists, these -- this is a real technical problem because they are small, and it is very hard to design security in a comprehensive way.

It will happen, but the FTC, for example, has really been pushing companies to try harder.

Ms. Schakowsky. So would you say the biggest barrier is that there are technical issues, or are these wearable manufacturers taking into account security sufficiently, or even thinking about it?

Mr. Peppet. I think it is both. Excuse me. I think it is both on the technical side, as I already described. On the are-they-trying-hard-enough side, there is at least two problems. One is a lot of these devices originally have been coming up as start-ups, and start-ups often, you know, are rushing to market with a product, may not spend enough time on data security.

The converse problem is interesting, too, which is some of these devices have come out of very big companies, very established companies that don't have much experience with the data stack. They are not IT companies. They are some other sort of firm, and so when they venture

into the tech space, they may not -- and we have seen examples of this, they may not have the either expertise or the depth to build that kind of security.

Ms. Schakowsky. Well, let me ask you this: Get to the regulatory part. You pointed out Texas. I actually have a bill, too, that would require breaches to be -- also this biometric stuff and to be -- consumers to be reported. Should we follow Texas' lead in requiring that notification as well?

Mr. Peppet. I think we should. Whether States do it or Congress does it, I think that consumers should know if their biometric data or other sensor-based biologic data has been hacked. I think you would choose between fitness -- you know, the two of you each had fitness devices. I think you might choose which one you wanted if you knew that one of them, the data had been stolen. So yeah, I think that is something that we should do for consumer --

Ms. Schakowsky. I am going to submit the rest of my questions for the record, and I really appreciate all of you. Thank you. I yield back.

Mr. Burgess. The gentlelady yields back. The chair thanks the gentlelady. The chair recognizes the gentleman from New Jersey, Mr. Lance, 5 minutes for questions.

Mr. Lance. Thank you. Mr. Webster, we have heard a lot about the benefits of this technology. Why is it more advanced, for example, than the smartphone?

Mr. Webster. Well, Congressman, I believe that these really

are -- it is one part of the broader ecosystem. The sensors can be in a number of different places and across all different industry verticals and aspects of our lives. Oftentimes, they will pair it with a smartphone or another Internet-connected device, and then that data then will go back to a cloud area or data center where analytics can be done. So while, oftentimes, the focus on these types of discussion is on the sensor itself, the reality is it is the full ecosystem and how they are all interrelated.

And that is why we believe, at Cisco, it is very important that there is security by design and privacy by design in each and every one of those parts so that you are able to look at it in aggregate as opposed to just looking down on one aspect of the broader ecosystem.

Mr. Lance. Thank you. My son got a -- would it be called a smartwatch for Christmas? I don't have one yet, but I am sure he will inform me about all of this as he does on so much of the technology, and thank you for the testimony of the entire panel. It is certainly the wave of the future, and I am pleased that the chairman and the ranking member have chosen to hold this hearing, and I yield back the balance of my time.

Mr. Burgess. The chair thanks the gentleman. The chair would note that there are votes on. Mr. Harper, I will recognize you for 5 minutes for questions, but I do want to point out to you the chair has not taken his time for questions yet, so govern yourself accordingly.

Mr. Harper. With that, I will be brief and respect my chairman.

Thank you all for being here. Mr. Webster, if I could ask what types of economic and workplace problems do wearables solve for business?

Mr. Webster. Congressman, wearables can solve a number of different problems. We discussed a little bit about the medical benefits that could be coming about and how it pertains to workers in hospitals. It also -- there is a great example about assembly line workers that were going through, and because they have wearables that are giving them step-by-step instructions when they are doing their quality checks, there is measurable less defects, and a much greater quality of the products that are served, and especially as you start going into more complex maintenance areas, especially safe for remote workers. They are going to be able to go and get -- create a much higher quality of step-by-step instructions,

Mr. Harper. Mr. Bianculli, can you comment on that as well?

Mr. Bianculli. Certainly. Yeah, we are seeing a host of opportunities. Something I would call -- the movement in the consumer space has really been around Fitbit and these other -- Adidas as well, around something called quantified self. So quantifying my behaviors, and what we are seeing in the enterprise markets is quantifying environments, quantifying workflow, you fundamentally can't improve what you can't measure. And so the use cases we are seeing are capturing those trapped inefficiencies that are there because we are not able to quantify what is happening in a given workflow, and basically, you could think about it as, you know, in a large tier 1

transportation company who might employ, or large retailer who might employ 300,000 people to restock shelves every evening in a retail store, understanding the workflow of each one of those 300,000 workers, which ones are performing in the best ways possible, and then helping the others to be able to achieve that level of performance by quantifying the environment.

Mr. Harper. All right. Thank you very much.

Mr. Bianculli. So lots of opportunities around quantifying the workflow.

Mr. Harper. Thank you. Mr. Palliparambil, given NXP's presence in many of the wearable devices on the market today, do we currently have the infrastructure to support the rapidly growing wearables market and accommodate multiple users?

Mr. Palliparambil. Yes, sir. Thank you for the question. Yes, we do, and as you pointed out, the Adidas products and some of the products from Zebra, so we have the sensors, we have the micro controllers and the security element that I talked about in my testimony, which allows to provide that level of security and often preferences for the consumer is available today. The technology is available. It is just a matter of choosing to use it, so --

Mr. Harper. Thank you.

Mr. Palliparambil. Thank you

Mr. Harper. In the interest of time, I am going to yield back. The chairman may want to talk. Thank you.

Mr. Burgess. The chair thanks the chairman. We have been joined

by Mr. Bilirakis of Florida. Mr. Bilirakis, I will recognize you for questions. You know we have votes on. The chair has generously allowed members to go before the chairman's time, so do bear in mind both you and I have to ask questions.

Mr. Bilirakis. Okay.

Mr. Burgess. I will recognize you for 5 minutes and hope that you don't --

Mr. Bilirakis. Well, I will yield --

Mr. Burgess. I hope that you don't use all of it.

Mr. Bilirakis. I yield to the chairman.

Mr. Burgess. No, no. I want you to go ahead.

RPTR MAAR

EDTR CRYSTAL

[11:26 a.m.]

Mr. Bilirakis. Okay. All right. I won't use all of it, promise you.

For the whole panel, what are the incentives for business and consumers who are not using wearables to start utilizing wearables and this kind of technology now? And this is for the whole panel.

Ms. Burich. I can take it.

Incentive. I think there is a lot of data that shows that when you use a wearable, it can really help you stay on your fitness journey longer. And this is related to -- I mean, there is also data that shows the more active and fit you are, it prevents disease, it keeps you out of the healthcare system. So it is a proactive way to manage your health.

Mr. Bilirakis. Very good.

Anyone else.

Mr. Palliparambil. Sure. So for a regular consumer, beyond fitness tracking and health, using a wearable for multiple applications, like payments, transit, and access into buildings, so logical and physical access. So the same wearable can, today's technology, allows you to use it for multiple applications, so beyond life and fitness. And that is the big advantage that I see, where you can have frictionless movement. So you have convenience, but you have

the security to conveniently use this in your everyday life.

Mr. Bilirakis. Thank you.

Anyone else.

Mr. Webster. Congressman, the benefits of wearables that I have seen, in general, really it comes down to a competitive issue. It is allowing people to be more productive, businesses to gain more productivity. It is going to help empower those that are using this is a way that can't be matched in other ways.

So it is very much a competitive issue, and I think it is very important that policymakers take the steps to really help propel this industry forward with the appropriate safeguards that we can maintain appropriate competitive positioning.

Mr. Bilirakis. Very good. Thank you.

Anyone else?

Mr. Bianculli. Congressman.

Mr. Bilirakis. Yes, please.

Mr. Bianculli. Congressman Bilirakis, I would say we break this down to two components. One is the input side of wearables, so being able to collect information about a particular workflow or what is happening in a given environment. So that is the input side. Think of that as Internet of Things sensor connectivity.

And then the wearable instructive part of this, which is being able to aim somebody in the right direction, being able to give them information on their wrist or a heads-up presentation of information while they are going through a workflow.

So think about the input side as being the Internet of Things of wearables, and think about the output side as being an efficient mechanism for being able to consume the data that is generated by the Internet of Things sensing technology.

Mr. Bilirakis. Very good. Thank you.

Anyone else?

Mr. Peppet. And then just very briefly, another incentive is that consumers in some contexts are being paid to use these devices. So many consumers, for example, myself, my healthcare plan at my employer gives me discounts if I use a wearable and track my fitness. We have also seen a life insurance company that has now issued a life insurance policy that gives you a discount on your premiums if you track your fitness using a wearable. So there are all sorts of actual direct incentives being used as well.

Mr. Bilirakis. Very good. Thank you.

And I will yield back, Mr. Chairman. Thanks for the opportunity.

Mr. Burgess. The gentleman yields back. The chair thanks the gentleman.

I will now recognize myself for questions.

And I do, again, want to thank you. This has been a fascinating hearing. Again, we do have a vote on, but let me see what I can get through.

Mr. Peppet, you brought up something that actually I am very interested in.

And, Mr. Webster, obviously, some of the work you do in the

healthcare space. The Affordable Care Act has brought us insurance with deductibles unlike anything anyone has ever seen.

But I guess what I am interested in is your comments, Mr. Peppet, on the monetization of the wearable or the monetization of the data and the ability to, perhaps, forgive a portion of the deductible to get the patient's buy-in to the continuation of the monitoring. So unlike Ms. Burich's population, people won't drop out of the monitoring, they will continue because they are getting something positive.

Could either of you speak to that?

Mr. Peppet. That is a very interesting question, and it is a very interesting domain, because you are exactly right that ongoing compliance with whatever the medical prescription is difficult for doctors to get patients to follow through. And both wearables and other Internet of Things devices, there is a smart pill bottle that every time you unscrew the cap, it is connected to WiFi and sends a message to your doctor saying: They took their pills today.

Those sorts of devices do allow a medical facility, whatever it is, to extend their reach out to their patients in all sorts of environments, and that is a potential huge benefit.

Now, in terms of, I think your question precisely was about payment or how premiums --

Mr. Burgess. To actually monetize the participation in the use of a wearable.

Mr. Peppet. Yeah, I am not sure I know enough yet to know how

that is going to play out.

Mr. Burgess. But you are experiencing it as a consumer in your insurance policy. Is that correct?

Mr. Peppet. Yeah, you are seeing it in the insurance space, that is right. And I think what we are seeing is a huge number of consumers are being introduced to wearables for the first time in those wellness programs, through that insurance vehicle.

Now, again, I am actually relatively in favor of that kind of incentive. The one concern I would express is, for example, in my own experience with the program that I am involved with, it was very hard to figure out or to get information about the use that the data would be put to. So when an employee or a consumer signs up for that kind of incentive, you want to make sure they know what they are signing up for.

Mr. Burgess. Mr. Webster, just in general, is there a way to quantify the benefit from the use of some of these wearables in the healthcare space?

Mr. Webster. Congressman, I don't claim to be an expert into the healthcare industry, but, no question, it is a major vertical where IoT is being leveraged. I think if we start looking at the quality of care that is able to be delivered, to the extent of the medical reach, as was mentioned, and also just, I think, to the well-being, knowing that an elderly relative is active, for example, or being able to track them down should they wander off, say, an Alzheimer's patient, I think there are a lot of benefits there that I think could be challenging

to quantify from a monetary benefit, but all recognize that it is good from a social benefit as well.

Mr. Burgess. Thank you.

Mr. Bianculli and Ms. Burich, you both have stuff that you brought with you. Would you spend just a minute and tell us what you have brought?

Let's start you, Mr. Bianculli.

Mr. Bianculli. Yes, certainly. We had mentioned in the testimony that we developed wearable categories in the early 1990s actually, particularly for warehouse workers. And that has evolved over the last 25 years. And so one of the capabilities we have today is a wrist-mount mobile computer that is worn on the wrist of a user inside of a warehouse or a distribution center-type facility; a ring scanner that is able to image, take images, and also read machine-readable codes, like bar codes, inside of a warehouse-type environment.

And so a user as they are, for instance, loading a vehicle with goods that are coming from, say, an e-commerce order online, they are scanning those packages with that scanner that is mounted to their hand, loading them into the vehicle. Their hands are staying free -- again, back to the frictionless notion before -- allowing them to get their work done without having the technology get in the way.

And so this is a probably very early example of application of wearable inside the enterprise space. We have got the Bluetooth ring scanner connected to a mobile computer on the wrist. That mobile

computer on the wrist is connected over a WiFi network back to the IT systems of some of these major carriers.

The second example, and a more recent one, and one that we continue to invest in and we are going to see more of over the next 3 to 5 years, is this notion of eye-level information. So being able to have a device, as I am showing here, be worn on the head and then present through a screen which, if you look at the screen just a couple inches from your eye, it is going to look like a 15-inch laptop screen floating right in front of you.

So if you think about working on an aircraft, where you may have several hundred thousand pages of schematic drawings about that aircraft, being able to bring up just the right drawing at the right moment that tells me what procedure I should do. Similarly, in battlefield and government applications, where you might be working on a tank or a piece of heavy machinery out in the field, not having to deal with multiple devices, laptops competing with the sun and everything else that can get in the way, simply be able to pull that information up on the screen; or be able to, via the camera that is mounted on this, send the video that I am seeing, the particular piece of apparatus that I am looking at, back to a remote expert who can then talk me through a scenario for repair.

Thank you.

Mr. Burgess. Thank you. And thanks for bringing the peripherals today.

Ms. Burich, can you do the same with your --

Ms. Burich. Yeah, sure. And I think our coaches could wear that while their players are wearing this.

Mr. Burgess. There you go.

Ms. Burich. This the Elite jersey that professional athletes wear on the field that contains some sophisticated sensors in this pod that goes in the back of a shirt. And then there is integrated heart rate sensing.

So in terms of compliance, it is important to put it all into one wearable that they can put on and not worry about, that goes through consumer laundry or laundry without any special care. So that is the Elite.

Mr. Burgess. Wait, wait, wait. You can put that through the laundry?

Ms. Burich. Without this.

Mr. Burgess. Oh, without that. Okay.

Ms. Burich. You can put this through the laundry.

Mr. Burgess. Just in case anyone was wondering, we do have a vote on. And I have a voting card that I will go put in. I have actually laundered it twice and it seems to still work. So maybe you can work on that same kind of technology.

Ms. Burich. Yeah. And then these are some of our hardware devices for the consumer market, a high-end running watch and kind of a mainstream fitness device that also has step counting on there. And I think that is the critical thing, is that throughout the day you need to be getting intensity, frequency, and volume in terms of your

exercise. So we are learning that it is not just about your workout, it is about what you are doing all day.

And then these garments are the translation of the Elite for consumers. So you can, again, just snap in a heart rate monitor. It is directly reading your heart rate off your chest. These are FDA approved in terms of the sensors, so wearable for consumer population as well.

Mr. Burgess. Very good. Well, thank you. Thank you for that.

I will tell you this was a fascinating hearing. And I apologize that we have had votes that have kind of disrupted things. This is a disrupter series, after all. But there is a lot that has been shared today.

One of the things that we hear a lot about is on the issue of encryption. We are hearing questions about privacy and security of data. Encryption seems to be one of those ways. But there also seems to be some problems with encryption.

So I am actually going to ask each of you to respond, I realize we are really out of time and I have to go vote, but I would like a response to or at least your thoughts on that. As we develop our policies going forward, how do you balance this privacy question? Is encryption the way to go?

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Burgess. And then, as we know, we have got the FBI concerned about the makers' ability to encrypt and whether or not that is a good thing from a law enforcement standpoint.

So that is one of the questions that actually may end up before this very subcommittee when it comes down to a legislative product.

But I can't thank you all enough for being here. Wait a minute, I have got to do this. Seeing that there are no further members wishing to ask questions or for any other purpose, I would like to thank all of our witnesses for being here.

Before we conclude, I would like to submit the following documents for the record by unanimous consent: a letter from the Competitive Carriers Association, a letter from the Mercatus Center at George Mason University. Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Burgess. And pursuant to committee rules, I remind members they have 10 business days to submit additional questions for the record and I ask the witnesses to submit their responses within 10 business days upon receipt of the questions.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Burgess. So without objection, and thanking everyone once again, the subcommittee is adjourned.

[Whereupon, at 11:39 a.m., the subcommittee was adjourned.]