FEDERAL TRADE COMMISSION

INTERNET OF THINGS WORKSHOP

NOVEMBER 19, 2013

Federal Trade Commission
601 New Jersey Avenue, N.W., Conference Center
Washington, DC

Reported By: Stephanie Gilley

FEDERAL TRADE COMMISSION

I N D E X

W E L C O M E

MS. JAGIELSKI: Good morning. I'm Karen Jagielski and I'd like to welcome you to the FTC workshop on the Internet of Things. And I have to note that it is the 150th anniversary of Lincoln's Gettysburg Address.

So I have to go through a few housekeeping details. Anyone that goes outside the building -- and I have to read this, because it's specific language. Anyone that goes outside the building without an FTC badge will be required to go through the magnetometer and x-ray machine prior to reentry into the conference center.

In the event of a fire or evacuation of the building, please leave the building in an orderly fashion. Once outside the building, you need to orient yourself to New Jersey Avenue, which is this street right here. Across from the FTC is the Georgetown Law Center. Look to the front sidewalk, that is our rallying point. Everyone will rally by floors and you need to check in with me or another one of the workshop organizers, who I will now ask to stand up so that you can recognize them. Hopefully they are in the room. Okay. And so you need to check-in with us.

In the event that it is safer to remain inside, you will be told where to go inside the building. If you spot suspicious activity, please alert security.

This event will be photographed, videotaped, webcast, and otherwise recorded. By participating in this event, you are agreeing that your image and anything you say or submit may be posted indefinitely at FTC.gov or on one of the Commission's publically available social media sites.

We would ask people to take seats, rather than standing, as it is against fire code, and that people not place their belongings on the seats next to them. Please also turn your cell to vibrate or off while in the room.

Question cards are available in the hallway, immediately outside of the conference room, on the table with FTC materials. If you have a question, fill out your card, raise your hand, and someone will come get it.

For those of you participating by webcast, you can tweet your question to #FTCIOT, email it to iot@ftc.gov, or post it to the FTC's Facebook page in the workshop status thread. Please understand that we may not be able to get to all of the questions.

So without further ado, I would like to introduce Edith Ramirez, Chairwoman of the FTC.

OPENING REMARKS

MS. RAMIREZ: Thank you, Karen. I want to say good morning to everyone and welcome you all to the Federal Trade Commission's Internet of Things workshop.

Before I start, I just want to extend my appreciation and gratitude to the FTC staff who organized this workshop and also to all of the speakers who are going to be joining us today in lending their expertise and experience in this very interesting topic. So thank you again and thank all of you for being here early this morning.

The Internet of Things has already entered the daily lives of many consumers. We can now rely on home security systems that show us who is at the front door on a screen on our tablets, even if we are across the country. We wear wireless medical and fitness devices that share our blood glucose readings with our doctors or tweet our race time to our followers. Sensors in our plants can send us a message to remind us that they need watering.

But we are on the cusp of even more change. Today's workshop examines the next technological leap when many, if not most, everyday physical objects will be able to communicate with other objects, as well as with ourselves. Almost anything to which a sensor can be attached can become a node in a ubiquitous network, continuously transmitting data in real time. It's estimated there are already 3.5 billion such sensors and some experts expect the number to increase to trillions within the next decade.

Now, it is still early when it comes to the Internet of Things, but it is clear that change is afoot. Five years ago, for the first time, more things than people connected to the internet. By 2020, an estimated 90 percent of consumer cars will have some sort of vehicle platform, up from 10 percent today. And it is estimated that, by 2015, there will be 25 billion things hooked up to the internet. By 2020, we are told the number will rise to 50 billion.

The Internet of Things is poised to transform manufacturing, business, and agriculture. Much of this can occur without collecting data about individuals, but in the consumer market smart devices will track our health, help us remotely monitor an aging family member, reduce our monthly utility bills, and alert us that we are out of milk.

The benefits to consumers will, no doubt, be great but these benefits come with undeniable privacy risks. The very technology that allows you to stream your favorite movie or send for help when your car breaks down can also collect, transmit, and compile information about your actions.

As I see it, the expansion of the Internet of Things presents three main challenges to consumer privacy. First, it facilitates the collection of vastly greater amounts of consumer data. Second, it opens that data to uses that are unexpected by consumers, and third it puts the security of that data at greater risk. I'd like to offer my perspective on each of these challenges and I know that others are going to be addressing them throughout the course of the day as well.

Let me turn to the ubiquitous collection of consumer data that the Internet of Things will enable. We are told to expect that, in the not too distant future, many if not most aspects of our everyday lives will be digitally observed and stored. The enormous data trove that will result will contain a wealth of revealing bits of information that, when patched together, may present a deeply personal and startlingly complete picture of each of us --our health, our religious preferences, our financial circumstances, and our family and friends. Our personal profiles will be parsed, augmented, and shared as they travel through an interconnected mosaic of commerce.

As one tech writer has explained, in very technical terms, "The Internet of Things will mean really, really big data." Well, with really big data comes really big responsibility. It is up to the companies that take part in this ecosystem to embrace their role as stewards of the consumer data they collect and use. That means adherence to the three core best practices espoused by the FTC: privacy by design, simplified consumer choice, and transparency.

First, privacy by design. Companies developing new products should build in consumer privacy protections from the very outset. Privacy should be integral to the innovation process with privacy hard-coded in. Companies should also consider how to shift the burden of privacy protection off of the shoulders of consumers.

For example, are there defaults or other design features that can help prevent consumers from sharing personal data in an unwanted manner? Privacy tools and settings should be as easy to use as the underlying product or service.

The second central principle is simplified consumer choice. Taking context into account, the companies that take part in the Internet of Things should give consumers control over their data. Often, this will mean just-in-time choice.

And that brings me to the third and related principle which runs through all of the FTC's privacy recommendations, transparency. Transparency is crucial. As more and more of our devices become smarter and smarter, it is essential we know as much about them as they know about us, that we understand what information the devices are collecting, and how it is being used or shared.

Now, I don't pretend these privacy practices are a panacea or that they will always be easy to implement. Privacy on the world wide web and on mobile devices is already very challenging. Even on a website on their desktop computer, consumers still often lack effective mechanisms to understand and control how their data is collected and used. On a smart phone, the smaller screen exacerbates this challenge. And the difficulties will be exponentially greater with the advent of the Internet of Things, as the boundaries between the virtual and physical worlds disappear.

Will consumers understand that previously inert, everyday objects are now collecting and sharing data about them? How can these objects provide just-in-time notice and choice if there is no user interface at all? And will we be asking consumers to make an unreasonable number of decisions about the collection and use of their data.

The answers to these and other questions may not be simple, but in my mind, the question is not whether the core principles of privacy by design, simplified choice, and transparency should apply to the Internet of Things, the question is how to adapt them to the Internet of Things.

The ubiquitous collection of data in our wired world inevitably gives rise to concerns about how all of this personal information is used. Is the data used solely to provide service to the consumer? Or will the information flowing in from our smart cars, smart devices, and smart cities just swell the ocean of big data, allowing the creation of profiles about consumers and predictions about their behavior?

Connected cars may direct emergency

responders to an accident, but will the data transmitted be shared with your insurer who may raise your rate or cancel your policy? Your smart TV may track whether you watch Masterpiece Theater or The Kardashians, but will your TV viewing habits be shared with prospective employers or schools? Or with data brokers, who will put that nugget together with information collected by your parking lot security gate, your heart monitor, and your smart phone and paint a picture of you that you won't see, but that others will. People who might make decisions about whether you are shown ads for organic food or junk food, what sale offers you received, and where your call to customer service is routed.

And finally, let me move on to security. Any device connected to the internet is potentially vulnerable to hijack and companies need to build security into their products, no exceptions. In the Internet of Things, data security will take on new importance, as it may affect the safety of our cars, medical devices, and homes.

Companies that don't pay attention to their security practice may find that the FTC will, as a company called TRENDnet recently learned. In the FTC's first enforcement foray into the Internet of Things, we alleged that TRENDnet's lax software design and testing of its IP-connected security cameras enabled a hacker to get his hands on the live feeds from 700 cameras and make them available on the internet.

The FTC is particularly vigilant when it comes to safeguarding sensitive consumer data, such as health information. I highlight the importance the FTC places on health information because of the numerous devices gathering this data. From wearable fitness devices that help us track and record exercise or sleep or blood pressure to smart pills that tell doctors when we are taking our medicine, these devices are poised to revolutionize healthcare. But we also have to take special care to prevent sensitive health information from falling into the wrong hands. This is among the crucial subjects that we are going to be discussing during today's program.

So in closing, let me end where I began. We are at the dawn of the Internet of Things. And like all dawns, the first light of the new day both illuminates and casts shadows. We see the promise of improved safety, health and efficiency as the items of our everyday life come alive. But we are also alert to the challenge of protecting consumer privacy in a cyber environment that breathes our personal data like oxygen.

Consumers will enthusiastically invite the Internet of Things into the homes, cars, and workplaces only if they are confident that they remain in control over their data. I know that we can find a way to reap the rewards from our connected future, while mitigating the privacy and security challenges that it brings and the purpose of today's program is to figure out how.

I want to thank you very much for joining us in that endeavor. Thank you.

MS. JAGIELSKI: Okay, our next speaker is Keith Marzullo. He's the Division Director for the Computer and Networks System Division and the Computer and Information Sciences and Engineering director at the National Science Foundation. Keith.

PAPER SESSION ONE: "What is the Internet of Things"

MR. MARZULLO: Good morning. Here's where we are. I'm very happy to be here to introduce this workshop on the Internet of Things. I've been asked to give sort of the technical framing of this. I know many of the issues we will be talking about are also sociotechnical. I will be touching very briefly on those, but my goal in my time here is to give you a basic overview of the Internet of Things from a foundational, scientific point of view, that is the National Science Foundation's point of view. So that's where I'm going with this.

I should say that, when I was flying out about ten days ago to visit some people at UC Berkeley, I was flying United and they have Hemispheres magazine and there was an article here that I looked at called, "It's All Connected: Pretty Soon, Even Your Trousers Will Have Their Own Twitter Account." I'm not sure why, but nonetheless, there it was written, right there, by Paul Ford. I don't know if you know Paul Ford, he's a good technical writer. This was clearly written rather tongue-in-cheek.

He starts off talking about the very first Internet of Things device, which was a coffeepot at the Trojan Lab at Cambridge University. In fact, I have a picture of it. It's right there. This was done in 1991. This was a camera put on a coffee pot in a lab so that you could actually see whether there was coffee in the coffee pot. So it would mean that you could either bug someone to make it if it wasn't there or go down if there was fresh coffee. The very first device. This was available until 2001, when they finally decommissioned it.

When you read this, it is actually a rather easy article to read, it's like two pages long. I recommend it just because it's rather fun. He makes many of the points we've already heard, for example Cisco has this prediction that some 25 billion devices will be connected to the internet by 2015, going to 50 billion by 2020.

He says that even the most mundane objects, watches or wallets, will have internet connection. He talks about the Songdo International Business District, which is a 40 billion dollar redevelopment project in the Inchon waterfront in South Korea. This is a model for where all of this is headed, he says. When it is completed in 2015, everything in this new district will be wired together and connected to the internet. Streetlamps will react to the number of people walking under them, for example. So it's being done, for example, in energy savings.

He also talks about Tom Coates. Tom Coates lives in San Francisco, he's a technologist, and he has wired up his house to give out tweets, depending on what's going on. When he comes home, when he leaves, what the temperature is. One tweet is that the house felt an earthquake. I went and checked on the USGS site and there was no earthquake at exactly the time, but the house thought there was one.

But the model is he is going with this is that this is information that will be sent out about things that are of interest. And he is envisioning Twitter as a kind of data feed to be used by companies that absorb this information, to be able to help you by observing what you are doing in your life.

So it's a fairly broad view of where we're going. Again, I'm not sure I want to have Twitter used as the delivery of my information, but it is clear there's a market here and this lighthearted article really is pointing out the direction we are going in terms of commercialization of the information that is being collected by all of these devices, these 25 billion devices on the internet.

I'll give you my own version of the origins of this. I think the earliest part is what was called ubiquitous computing. We heard Chairwoman Ramirez talk about ubiquitous computing or ubiquity of data. This was developed by a fellow named Mark Weiser at the Palo Alto Research Center at Xerox. He was really thinking about the Internet of Things in the context of the office place. I mean, that's what he was working on. So one of the things that they developed there, for example, is an active badge, a badge that would track where you were. This was seen as a great idea because this way people could find where you were.

For example, if a phone call came in, they envisioned that the phone nearest you would ring, rather than you having to go back to your office. Or if you wanted something printed, it would go to the printer nearest you.

Of course, they quickly found out that people stopped wearing their badges because they didn't like having people know where they were. Like, how long have you been in the bathroom? That kind of thing. So there was a whole sociotechnical issue that they hadn't really envisioned. This is all back in the eighties.

It was also called pervasive computing because the idea was pushing computation out into the world. Instead of having computers, it was meant to be ubiquitous around you, all the time.

Distributed sensor networks came in in the nineties, which was looking at, how can you try to decentralize all of this. This was an attempt to look at some of the issues, in terms of failures.

And then in the mid-2000s, the term Internet of Things started to appear. The earliest report I found was the ITU Internet Report from November of 2005. In this, they said that the main enablers of the Internet of Things were three things. The first one was item identification, so you could actually know what you were talking to, that was based on RFID at the time, radio frequency identification, the ability to detect changes in the physical state of things, so we are looking at sensors, and embedded intelligence, pushing things out into the environment.

Cyber-physical systems started at about the same time. This is what we called it at NSF. Dr. Helen Gill was the one who invented this term.

This is looking at the same problem, but it is turning it around and looking more at the issue of control. That is, once I have all of this information, I have the cyber world and the physical world, how do we put them together?

Let me briefly talk about our Cyber-Physical System Project, just to tell you the things we are doing in this area. We are doing this because of national priorities, there are things that we need to be doing. In transportation, there are worries of faster and safer aircraft, improved use of airspace, safer and more efficient cars, reducing the death rate on the highways, energy and industrial automation, healthcare and biomedical. There are clearly needs for effective at-home care, as well as being able to worry about all of these devices we are putting in ourselves, critical infrastructure of the power grid, more dense highways.

And so the idea here, what is driving this is can we use the fact that we can gather this information to have more efficient control of the environment?

This is the way we like to describe our CPS program. We call this the daisy diagram because it looks a little bit like a flower. The idea here is that these various application sectors that are working in the space, energy, agriculture, vertical farming, for example, is an issue that is now instrumenting to be able to worry about growing crops on the tops of buildings, several materials, chemicals, medical, and so on.

And what we are doing in our CPS program is looking at the core sciences common across all of these application sectors. These include control, of course, verification, certification, so you know it is doing what it is supposed to be doing, safety, real-time systems, networking, security, and privacy. These are all issues that come up in our problems of CPS, or Cyber-Physical Systems.

So the goals that we've been doing are to overcome the complex technical challenge of systems that interface the cyber with the physical. Much of this, these systems often have to be certified and so we have to be able to find ways to prove that they do what they are supposed to be doing. That's a technical problem.

We have -- we are working on discovering the principles that bridge across all of these different sectors. A large part of this is enabling societal acceptance and reliance of these systems. These cyber-physical systems are systems that often people have to bet their lives on, they can bet their lives on. Not only that, they have to be willing to bet their lives on it as well. There is an issue, in terms of being transparent in terms of what they do. And part of this, what we've been doing is trying to fund a whole group of new researchers in this area of education to try to build this as a discipline.

So having told you what we are doing at cyber-physical systems and how it relates to the Internet of Things, I'm just going to give you four projects of the many that we fund to try to show you how this all works together.

The first one is what is called Actionwebs. Actionwebs is a project that is being done, it is being led out of Berkeley and Claire Tomlin is the lead on this, but they also have people from -- namely Hamsa Balakrishnan from MIT on this. And the idea of this is to try to come up with an architecture, what they call theory of ActionWebs.

ActionWebs are network-embedded sensor-rich systems that are taskable for coordination of multiple decision makers. Their approach in this research is to identify models of action webs using stochastic hybrid systems and interlinking of continuous dynamic or physical models with the discrete state representations, interconnection, and computation. Those are fairly high words for what they are trying to do. But if you go and see what they are doing, it's delightful.

They are doing energy efficient buildings, for example. They've instrumented one of -- actually, it was instrumented when it was built, a completely instrumented engineering building. And they are looking at, how can you use the sensing to be able to control things like energy in the building. So as people move in and out of rooms, can you ensure that you are only heating those rooms. This turns out to be a hard problem on the physics side. They are basically looking at Newton's law of cooling combined with a whole host of sensors that are available within the system. Basically, they are doing HVAC operating systems. It's really nice work.

They are also looking at energy efficient air transportation systems. Dr. Balakrishnan has been looking at that in terms of push-back rules.

Again, can you come up with better ways to gather information to be able to have more efficient air transportation.

So out of this, by looking at these two sectors, they are hoping to come up with a more generalized model so that it could be applied to other things.

Taking their work one step forward, they just recently -- a similar group has been funded on something called Foundations Resilience Cyber-Physical Systems. This is a wonderful project because they've introduced the term HCPS, so they've added an extra letter. CPS, you'll remember, is cyber-physical systems and H is humans. So they observe that humans are as part of the system as much as anything else.

And so they are looking at issues on resilient control, how can you build systems that are able to continue to operate, continue to have strong control, even in the face of failures, even in the face of natural disasters, even in the face of attack.

And they are doing this, in part, in the design by putting -- they are using game theory. They are looking for incentive theory to make these systems more resilient. Can you come up with economic models so that you can encourage people to drive more safely, for example, given the way you are instrumenting the system.

So I find this a really exciting problem because they are breaking out of the space of just trying to control it in a purely technical sense and bringing people into the loop.

This is the third project, this is a fun one. This is advanced transportation systems. You probably have heard of the Google car. I don't see Vint here, he'll be here later. This is NSF's version of this. This group actually won the DARPA Urban Challenge. They are developing cars that drive autonomously. This clearly has a large societal and economic impact. The reason why this is the Internet of Things is, well, cars are very complex. You have to build those systems, but also these cars have to interact with their environment. So they have been looking, for example, how you can sense bicyclists, so that you don't run into them. How can you sense what is going on with cars that are driving, that are not autonomously driven.

They just had a great demo of this in September. Their automated autonomous Cadillac, they say it goes the distance. They got the U.S. House Transportation and Infrastructure Committee Chairman Bill Shuster and the Pennsylvania Department of Transportation Secretary Barry Schoch to ride in this car safely from the airport, with traffic, and nobody died. This was a really good thing. It's actually really fun.

The fourth project, may I tell you, is something that perhaps is fairly obvious in a CPS kind of system. I've been told this mouse works. Yes, it does. I'm going to let the project speak for itself.

The whole clip is about two-and-a-half minutes long. I encourage you to go look at it, it's quite a nice project. As well as instrumenting the water, they also are instrumenting the soil and trees. For example, how fast are trees growing. So it's a wonderful tool of instrumenting the environment to be able to have dashboard control or understanding what is going on in the Suwannee River Basin.

So let me briefly turn to security and privacy, what we are doing in this. I'm going to make this fairly brief because I think I only have five more minutes. We are funding a considerable amount of research in both the security and privacy of systems, more in security than privacy, although in the last couple of years, we've been trying to increase the role in privacy by bringing in our sister director of social behavior and economic sciences.

So let me give you four quick examples. This first one is semantic security monitoring of industrial control systems. So industrial control systems, these are like SCADA, aren't like traditional IT infrastructure in an office. These are built out of hardware that typically have a 20 to 40 year lifetime as compared to, say, five years with the computer you have in your office. It has no ability to upgrade hardware or software and these don't tend to be built with security in mind.

And so we've developed, over the last 30 years, a considerable amount of technology, of varying success, to try to detect break-ins in computer systems. This turns out to be hard, as you all know. As you all know, your antivirus software, your intrusion detection systems, we can only go so far with this.

What this research is showing or is observing is that industrial control systems actually are more predictable. We know how they operate. They are running a much narrower kind of program, so this is a more tractable problem. And so you can imagine, Stuxnet from a couple of years ago, which was a break-in to a SCADA system. These people are looking at ways to see whether you could actually detect something like that to stop that kind of attack.

Programming and reprogramming a pacemaker. Pacemaker defibrillators, insulin pumps, these are all small computers that allow some level of reprogramming. The reprogramming is necessary to personalize them for the patient.

This attack -- this was done by Kevin Fu. He is now at the University of Michigan. They were looking at attack methods to look at the information or change the information in a pacemaker defibrillator to be able to either leak privacy or to do more damage. And they are using the techniques that are available, such as the kinds of controls that a doctor would use to be able to adjust it.

This chart here just shows you the kinds of things you could do. These are the attacks, commercial programmer, software radio eavesdropper, software radio programmer. You can see that these first issues are all privacy, whether the patient has an ICD, telemetry data from the ICD, obtain information about the patient, name, age, private telemetry.

But also, with some attacks, you could actually change the device settings, which is sort of a terrifying thing. In fact, it is so terrifying that Hollywood got into it and they picked up a news story of "Can Your Pacemaker Be Hijacked?" And this also was picked up by Washington, when Mr. Cheney was in fear that terrorists would hack his pacemaker. So clearly there are a lot of issues in terms of these devices, as you can imagine, that are necessary for security.

Reprogramming automobiles. Automobiles, you may or may not know, are also devices that contain an awful lot of computers. I have been told that the number of computers necessary on a BMW to lock the door is five, that get involved. That's because there are laws involved that, when the car is in an accident, the doors have to unlock, so they are fairly complex beasts.

Because of this, we all know about the accidental -- things that might happen with cars because of programming errors or hardware errors, but there are also attack surfaces that are created by these cars.

And so this is work done by Yoshi Kohno, who I think is going to be on the panel later, and my colleagues at UC San Diego, Stefan Savage and Ingolf Kreuger, where they looked at ways of being able to attack a car, going in through various ports. It could be something as obvious as going into the data port and something not as obvious as going to the OnStar system remotely.

They were able to successfully break into the car and change it in fairly interesting ways. This is one of their examples. If you notice here, the car is going 140 miles an hour but it is in park. That's really hard. This car actually was on blocks, it was not going anywhere. This was an attack where they are able to show how they can change it. You could also put on the brakes, deploy the airbag. It was a vector of, because of the way the system was designed, it could be attacked.

First, let me also say that NSF is not eagerly funding research to try to get people to break into cars and pacemakers, that's not our goal. Our goal here is try to understand how to make systems better. Much of the value of this research was identifying systems that were felt to be secure, but they weren't. These people have also gone on to show how to secure them. But these are the kinds of risks that come up as you start to instrument the world around you.

This project here by Hari Balakrishnan, Sam Madden, and Daniela Rus at MIT are looking at issues of security and privacy in vehicular cyber-physical systems. If you have an EZ-Pass or similar device, you are not only monitored when you are driving, but you can be monitored in many different areas. In some countries, as you know, there is pervasive monitoring and using surveillance cameras. This information is used for including insurance pricing, based on driving behavior, restricted areas and tolling, high tolls for driving in downtown London, for example, congestion pricing, and so on. But there clearly are privacy issues here as well. I mean, you may not want your cardiologist to know where you are having lunch, this could be an issue. Or you may want to not have people know which kinds of places you visit off-hours.

And so these people are looking at ways to be able to fuzz the information geographically, to be able to present the information necessary for the intended purposes, but to restrict the use outside.

Finally, as I see we have another project by Yoshi Kohno. We must like Yoshi. This is a project in secure telerobotics. Telerobotics is the process where a person in one operation operates a robot somewhere else. This is often used for telesurgery, for example operating on soldiers in the field.

And this is important, obviously, it's lifesaving things, but it -- and it avoids putting rare and expensive doctors at risk, but of course an action like this opens up several kinds of security holes. How do you ensure that the actions being done are not intercepted? Even a small change in the timing could have a large effect on what the doctor is trying to do.

So their approach on this is, again, much like the first one I was talking about, in terms of SCADA. How do you mill, roughly, what the doctor is trying to do so you can look at things that are moving outside of that envelope?

So I've given you four projects on the Internet of Things to give you an idea, and then four ideas that we've been trying to address in terms of privacy and security.

So let me summarize: The Internet of Things has been around for about 25 years in the research community, going back to the work that Mark Weiser did. Technological advances are moving very quickly, RFID, Smart Dust. Smart Dust is another term for a small computer that is used as a sensor. University of Michigan, for example, is producing something that is 1 mm cubic in size that has a camera and communication facilities. They are using them -- you can obviously scatter them anywhere, but also they are using them for measuring pressure on animals and such. Cellular communications, this has all made IoT, Internet of Things, quite affordable. We have come a long way in that.

In terms of commercial opportunities, advances in control, verification, big data have all led to tremendous commercial opportunities. There is a lot of commercial interest in this. The internet of everything, to use Qualcomm's term, or the industrial internet, to use GE's term. These are all issues where we are collecting information and using it, basically big data and techniques, to try to do things better. Say, predict when airplanes need to have preventive maintenance.

And given all of this, security and privacy are real issues and they need to be addressed.

Thank you.

MS. JAGIELSKI: Thank you, Keith. Our next speaker is Carolyn Nguyen. She is the Director of Microsoft's Technology Policy Group.

PAPER SESSION TWO: CONTEXTUAL PRIVACY

MS. NGUYEN: Thank you, Karen, for your kind introduction. And thank you Keith for giving us such a wonderful overview of the technology development of the IoT.

So good morning. I am very honored to be invited to participate in the FTC workshop to speak about the Internet of Things and really to share with you some of my thoughts regarding the impact of the Internet of Things.

I've been asked to speak about the impact on the individual. Because a lot of times when we speak about, you know, the swell of data, we forget that, at the end of the day, there is an individual in the middle of this, trying to figure out what to do with this data and the impact of the data in this really connected world.

So when one starts to discuss the IoT, as Chairman Ramirez has already mentioned, and Keith has made it evident, the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data.

Keith told us that this got all started because of the need for caffeine, just like the internet got driven because of the need for email. Since then, as Chairman Ramirez mentioned, this has grown to include plants, a teapot in Japan that can notify caregivers of unusual tea drinking patterns, a headband with embedded sensors that can track people's brain electrical activity and enabling them to control objects and applications with their minds, and my most favorite application, socks that can help look for their twin. So the impact and potential of the Internet of Things, it is definitely a radical new world.

So lost socks aside, a unique aspect of the IoT, as far as the individual is concerned, is really its potential to revolutionize how individuals will interact with the physical world and enable a seamless integration between the digital and the physical world as never before. It is this ability that I will address and that really merits our attention.

Today, people must master controls of different types of technology and devices in order to manage their environment to something that can be done and behave according to their preferences. The

IoT, with its network of sensors and potential to sense the environment, can help assist individuals and people to make optimized and context-appropriate decisions.

As such, the IoT can bring to the physical world the level of personalization that is now only possible in a digital world. This is a movement and transformation from a world when machines respond only to commands by the individual to where machines can be enabled, with complex algorithms and adaptive behaviors, and can act as intelligent agents and proxies on behalf of the individual.

So back to the individual. As the individual is increasingly objectified by the quantity of data available about them, it's important that we have a dialogue today and now, as we are just at the dawn of the IoT, to create a viable, sustainable data ecosystem that is centered on the individual.

I want to emphasize that user-centered is very different than having the individual in the middle, trying to control all of this data about them. So this is really an ecosystem that is focusing on empowering and engaging the individual.

So here's what I'll cover in my talk

today. It is really the impact of the IoT on the individual. It is really then, why is context and trust relevant in this conversation? How do individuals define context? We normally don't talk about that so much so I'll discuss some research that we've done. And lastly, what are some policy considerations? We've already heard Chairman Ramirez mention context today and Keith talked about how the NSF is working to bring the people and the individual into the technology.

For this talk, I will ask you to assume that we are already in the world of the IoT, it is here, and let's think about how to enable it, instead of how to stop the data flow.

So let's first explore the ecosystem. Taking a look at the evolution and the emerging data-driven economy, this is how we all started, where a person shares data with another person that they have a good relationship with and can trust that the data won't be misused. The terminology that I use is that the data is being actively provided to the individual.

In the evolution going forward, we evolve from this model to where I share data with an entity for which I receive a service. A store, a bank, a post office. Again, this is usually an entity with whom I either have a good relationship with or know I can trust. And this is true, whether this is in the physical world or in the digital world.

So if we evolve this a little bit further, where there is now such an entity may be able to share personal data with other entities, with or without my knowledge. We talk about the terminology, as this data that is being generated or inferred as data that is passively generated about me. In other words, I am not actively involved in this transaction.

So as we move further in the evolution, there is more and more data being shared. And furthermore, it is now also possible that other parties that are in my social network can share data about me.

So for example, a friend uploading my photo into the service. In this view, it is already very difficult for an individual to control the collection and distribution of information about me. And traditional control mechanisms such as notice and consent begin to lose meaning, as the individual most often automatically gives consent without a true understanding of how the data is distributed or used.

Moving forward into the Internet of Things with ubiquitous sensors, the situation is clearly further exacerbated. We've already heard about Fitbit, sensors in my shirt, sensors in pants that can tweet out information about me, my car giving out information about potholes in the street, average speed, etc. There are devices in my home that are giving information about activities, temperature, whether I am home or not. Devices in my workspace, as well as devices in a public space.

So increasingly, the amount of data that will be generated, as was already mentioned this morning, would be primarily passively collected and generated.

It is, however, in the data-driven economy, it is this flow of data that has the potential to create new benefits and new innovations and create a foundation for a new economy. Over-restriction of this flow can restrict the potential value, but lax regulation can clearly harm the individual and violate their rights.

So what I will be talking about for the rest of the talk is that new approaches are really needed to enable and empower the individual to control the use of their data, whether directly or innately, by using sensors and the information that is being generated for third-party proxies to help control and help associate that the data will be used in an appropriate manner to the user.

So what is the impact of this data on the individual? Today, there is already an asymmetry of power between business and individuals due to the amount that is perceived to be controlled by businesses. This is clearly not a sustainable situation and in the world of the Internet of Things and in the world of tomorrow, for a data-driven ecosystem to be sustainable, the issue that must be addressed is that the ecosystem must show, demonstrate, that it is capable of earning the individual's trust. And as such, it must be centered on empowering the individual and such mechanisms need to be at the ecosystem level.

What this does is that it takes what Chairman Ramirez talks about in terms of privacy by design, but instead of having it at the individual industry and business level, this now has to happen at the ecosystem level. In other words, there needs to be interoperable privacy mechanisms where the user permissions and preferences can be preserved by multiple parties across the ecosystems, as well as taking into consideration what are often dynamic, changing social norms as well as cultural norms across multiple countries.

So what are some existing work that was already mentioned about context. I think you are very familiar already here with what the White House report has included, which is the notion of respect for context within the Privacy Bill of Rights. The FTC Chairman Ramirez already spoke about it this morning, about the importance of the context, of the interaction, and how data is used out of context and it really needs individual input.

The World Economic Forum, in a series of global discussions on its multiyear data project and rethinking personal data, has found that, in the world of a data-driven economy, there is really a need to really move or migrate toward more of a data use model. In order to do that, it is critical to engage and empower individuals, so furthermore really validating the notion that context is a key element.

It also puts forth the role of technology as part of the solution in enhancing the trustworthiness of the data ecosystem. Based on this work, we undertook a global research to understand how people define context. We talk a lot about context, but it is not clear what context awareness means and what are the elements that define context.

So between 2012 and 2013, Microsoft undertook a multiphase project, qualitative and quantitative, to look into what are the factors that individuals take into consideration in determining whether a given scenario involving use of data about them, so not just data that they provided, would be acceptable. We termed this context, or data use context, generically.

So what we found was that there were really two groups of variables, one that consists of objective variables, in other words the facts about the actual data use, and then a set of variables that is more subjective, trust and value exchange.

In the objective variables, it has to do with the type of data, the type of entity, in other words, what is the entity that I am interacting with. It is a retailer, is it a bank, is it a bookseller, is it my employer, is it a government agency?

The device context. What is the device

I'm using? Is it a mobile device? Is it my home computer, is it a laptop, etc?

The collection method by which the data is collected, how the data is used, whether I actually consent to its use or whether it is used to automate decisions about me.

And then the subjective variables. This is where privacy becomes a difficult conversation because it is very subjective. It has to do with the level of trust that I have in the entity that I am interacting with and it also has to do with perceived value that I am receiving from the use of my information.

In the second phase -- so this was data that was, research that was done in four countries, Canada, China, Germany and the U.S. The countries were chosen because of the various different approaches that they have towards privacy regulations.

We followed up with a quantitative research in eight countries to look at specific scenarios so that we can determine what are the relative importance of these factors in the different countries and how do they vary across the different countries.

So let me walk you through a series of scenarios. I deliberately picked a rather undesirable scenario that is probably relevant to a lot of people here, looking at privacy. The scenario is location data being collected from a mobile device where the service provider here is used to mean anyone. So it could be an online book retailer collecting my information or a coffee seller, I'm not going to mention any names, trying to collect my location information as I am in the area.

So in the first scenario, I say that data usage is that the information is being collected to make automatic decisions on my behalf. I am unfamiliar with the company. So this is the first time that I've walked into that coffee store or the first time that I am entering into the book retailer, and the use of the information has no benefit to me.

So when we look at the acceptability factor, it is very low. However, there are some clear patterns here that are starting to emerge which are the western countries, the countries to the left, the acceptability is very low. This includes the U.S., Germany, U.K., Canada, Australia and Sweden. Whereas, China and India, because there is actually -- the population is more tech-aware, the acceptability of the scenario is higher.

So we vary this to say, in scenario two, we keep it at the same, the base scenario is exactly the same, it is still a company that is unfamiliar to me and there is no benefit to me, but we change the data usage to personalize my choice.

So what is the impact of this unacceptability? So we see that there is some increase, from a proportional perspective, much more in the western countries than in China and India. For example, in Sweden, the acceptability rate increased more than two times, from 5 percent to 12 percent and it is much, much less, as you can see there, just eyeballing it.

So what this says is that data usage is a more important factor relatively, in the western countries, but not necessarily in India or China.

Let's vary the scenario again. So we keep it the same that the data usage is personalize my choices, and the value of the exchange is still no benefit to me, but the company is now someone who is well-known to me. What is the impact of this?

You can start to see that trust is a large factor, both in the western countries as well as in the eastern countries, although proportionally much more in the western countries.

The last variation is when we look at the value exchange from no benefit to community benefit. And what we see here, and this is a trend throughout the rest of the survey, is that the value exchange for community benefit is much, much larger proportionally in China and India than in the western countries. I am not going to make any general comment about that.

So hopefully, you know, with some of these data, I can -- you can start to see the point that these factors really impact acceptability of data use. And it is very much a nuanced conversation. This is what makes privacy so difficult. And these factors do vary across personal, social, and cultural norms.

What are some of the other factors that may impact context? Because what we did is we took a fairly difficult problem and just took a fairly straight-forward and limited approach to it. In our research, we found that demographics, culture, and perceptions also have an impact. Age, gender, occupation, in terms of demographics, culture, in terms of nationality, historical impact, the level of technology adoption of a particular country, and in terms of its population and regulations that are in place. This may have to do risk perception and so variations, in terms of perception of the regulation.

So again, we took a first stab at defining context, but there is a lot more work to be done. This is a really complicated issue.

So how do you actually use this information, again, to try to build out a context of where a system, within the world of the Internet of Things? Let's take the case where I'm a user and I'm accessing a mobile device. The application is being provided and then there is a user agent or a proxy that would provide personalized UX to me.

How is that personalized UX. driven? Well, it's driven by something that I call a recommender system that implemented a variation of the model that I just described. So this is how, by using and by knowing and getting some information, either through the application or through other things, about the user and the session, I can actually personalize data usage recommendations to the user itself.

So by this way, if we look at it as, you know, the beginning of starting to build out context aware systems and the next step, in terms of enabling trust within the system, so that we can hold on to the preferences of the user consistently.

Now, if the user, remembering that, you know, these are just systems and there are models behind them, so if the user happens to make a different choice or a different setting, the notion is that this should then be captured in something that we call a use preferences model. Now, the FTC has the notion of common acceptable practices and by capturing such use preferences, the notion is that we can then start to look at changes in use preferences dynamically. So this starts to look at how can we build out dynamic systems. At the end of the day, after all, the IoT is a completely dynamic system.

So where can these systems be used? They can either be used by a service provider to enable a personalized or what we can contextual privacy, or actually by users to assist in context-sensitive data settings. So they can be used by both sides, again, to assist the end-user.

So in conclusion, what I have presented

here are some preliminary findings that hopefully will motivate you to think about the world of the user and what user attitudes are with respect to the user data. Hopefully, we can continue to explore, throughout the day, in terms of health care, in connected homes, in connected cars, with respect the world of the Internet of Things. The only thing that is sure is that, you know, the existing model, in terms of we really need to transition more to use-base and context aware data use is somehow -- we feel that it is essential to creating a sustainable ecosystem.

But just as Keith mentioned, you know, privacy is difficult because you really need to take into consideration the user, the human beings. It really needs to be a multidisciplinary conversation, not just technology, but at the same time economics, ethical usage of data, and policy at the same time. We talk a lot about technology research, but we don't often talk about the need to do policy research.

What I'm hoping for is, with some of the messages that I'm talking about this morning, that there would be some efforts to try to also look at policy research. Again, put yourself in the future world and in the world of the Internet of Things.

The last message I want to leave is there is a lot more work that needs to be done in order to understand the Internet of Things. We've never encountered a system that is so dynamic and complex and changing so quickly. It would be great if we could work together to really understand what the questions are so that we can formulate the problem appropriately, before we jump to an answer.

Thank you very much.

PANEL ONE: The Smart Home

MS. YODAIKEN: If we could ask the Panel 1 panelists to come on up.

Hi, there. I'm Ruth Yodaiken. I'm with the Division of Privacy and Identify Protection and I will be co-moderating this panel with Mark Eichorn here, who is an assistant director in the division.

While everyone is getting seated, let me just say two things. It is a pretty crowded room today and so we've been asked, if you have an empty seat by you if you can just either squeeze in or identify it, as people are going around and looking for seats.

And also, if you are in the room and you have a question during this panel, you should have a question card, there were some outside. If not, we have some paralegals who will be, honors paralegals, who will be wandering around the room. You can flag them and either give them a card that you've filled out or ask them for one.

If you are watching online, there are online methods for asking questions, including Twitter and email.

Okay, so we are going to have short introductory remarks from each of our panelists and

Eric Lightner is going to start us off. He is a program manager for Advanced Technology Development at the Department of Energy and Eric is the Director of the Federal Grid Task Force.

MR. LIGHTNER: Thank you, Ruth. I appreciate that. Good morning, everybody.

I thought a lot about what I should say here today, thinking about what people are thinking in the audience. Like, why is DOE here, why are they involved in this? So hopefully I am going to give you a little bit of context and maybe you'll have some questions later about the story I'm going to tell as to why we are involved and why we are of interest here. And we are a small part of this, you will see, from my little story here.

So I come from an office at DOE where we do a lot of research and development. We work with the utilities on modernizing the infrastructure to supply electricity to homes and businesses throughout the country. That is basically what we do and we've been doing that for decades.

I guess about five, six, seven years ago or so we realized that the industry really wasn't taking advantage of all the information technology, all of the communications technologies, and really modernizing the way that they could be, really, to meet the demands of users of electricity.

So we decided to work with the industry to really come up with a term that we later called Smart Grid, but basically said hey, what is the future of the grid really going to look like and what kind of functionality do we really want to see?

And the reason I mention that is because one of the functions, one of the seven that we came up with, was really actively engaging the customer. That really hadn't been done in the past. In the utility industry, you basically get your bill once a month, it's confusing, you just look at the bottom line, okay, that's what I owe, here you go, and that's basically it.

So we really felt that was an opportunity there, specifically, really to engage the customer in how they use electricity, make them more aware of how they use electricity, so they can make better decisions about how they use electricity, efficiently and for their own purposes of potentially maybe saving some money or what not.

So we really got into trying to figure out how we can bring technology to enable the customer. We did some research in that area and, in 2009, we got a big amount of stimulus funding, about 4.5 billion dollars, to work with the utilities to begin implementing and adopting some of these technologies. Well, it's a huge advantage, or an opportunity, I should say, for us to really learn about how are these technologies used, what can we learn from them, how much do they cost, what is the benefit to the consumer. So we started those projects.

Around 2011, the administration came out with the policy framework for a 21st century grid, in which they had four pillars that say, hey, we really need to focus on these things to advance our grid. One of those was empowering consumers.

So with the ARRA dollars, with our definition of empowering consumers, enabling consumer participation, a lot of that money went into advancement of infrastructure projects. So smart meters, which everybody has probably heard that term.

And so that really opened the door for, okay, we have communication now, a monitoring point at the consumer, that really opens the door for the customers to know more about how they use energy.

So we started a number of, I would say,

initiatives around this, centered on the consumer. A couple I will just mention quickly. One is called Green Button and that's really an effort to standardize the information, the customer usage, the energy usage information that you can have access to through your utility in a standardized format and download that information and use that in different applications.

We also stimulated the market by funding some developers of technology to look at, okay, if you have this standardized customer energy use and information, what kind of applications and services could we create around that. So we funded some companies to develop some of those technologies.

That sort of gave rise to questions of privacy. Hey, I want to use my information, I want to look at it in a more detailed fashion. I probably want to share it with third parties for additional services to me, what are the privacy implications of that?

So we started another initiative called the Voluntary Code of Conduct on Data Privacy. This is something that is actively ongoing. We are working with utilities and a number of stakeholders to really figure out what sort of -- just the baseline of protections and processes that we can put in place across utilities in a voluntary way.

Many utilities are regulated by their states and they already have policies and laws about how to handle data, but it's not consistent across the states, so we really wanted to try to develop a voluntary, consistent practice. So you, as a consumer, would then feel more comfortable about how that information is being used within the utility and what the process is for you to give consent to share that information with third parties of your choice for different products and services.

And a real quick example, if I may, Ruth, is why would we want to do this? Well, you know, there's a lot of solar going on roofs nowadays. A lot of people are purchasing those. And in the past, the company really would look at what your monthly usage was to help size that system. But now they can ask you, hey, if you just give me access to your Green Button data, which is hourly data of your usage or better, they can much better size and design that system to actually meet your usage needs. So that's just a small example.

So instead of oversizing the system or under-sizing the system, you know, based on just your bills, they can much more accurately size that system to fit your needs. So that's just one small example.

So anyway, I think I should end there because we don't have a lot of time. But questions on any of these things, whether it be on the ARA projects or our definition of Smart Grid or the Voluntary Code of Conduct Process, I am here to answer those questions, so thank you.

MS. YODAIKEN: And Eric, let me just ask you, while you're at it, when is the next Voluntary Code of Conduct meeting?

MR. LIGHTNER: The next meeting is this Friday at the FCC at 9 a.m.

MS. YODAIKEN: Great. Okay, so next up we have Michael Beyerle, who is a marketing manager at GE Appliances and he is responsible for identifying and developing new products.

MR. BEYERLE: Good morning. I'm Mike Beyerle and I'm with GE Appliances.

We are actually working on our second generation of connected appliances. In case you didn't realize it, almost all of your appliances are microprocessor controlled these days. Our top of the line refrigerator will have three, maybe four, microprocessors actually running it. BMW apparently has me beat by one, but we can always fix that later on.

In fact, some of our engineers view a refrigerator really as a 72 inch computer, right, that just happens to keep your food cold. They keep wanting to give me a laptop version and I say no, there's no value in that, right?

But you know, we are actually doing quite a bit in this area. We have been working at it for quite awhile. I'd like to tell you just a little bit about what we are doing with some of our cooking products.

First, let me talk about a little bit of platform first. The platform is very, very simple, very, very straightforward and much what you would see with any other connected product. You've got a device, in this case your appliances, tied back into your home wi-fi router system. The wi-fi router system is feeding into the GE servers, the GE server allowing you to connect into your smart phone, your tablet, whatever device you may have, as well as some data storage. So very, very similar on your appliances to what you might see for your tablet or any other kind of device you might have inside the house.

And the video is at the --

MS. YODAIKEN: At the end.

MR. BEYERLE: Okay, we'll talk through and show the video at the end then.

Different things that you can do with it? You say "Why do I want to connect my appliances?" The connected appliance provides you some value and convenience, in terms of the consumer. In this case, you've got the ability to set your temperatures remotely, the ability to develop new recipes, to control the oven, you've got the ability to change the cycle, to go from bake to broil, to pull up special cycles, to use things such as your meat probe to look at interesting new recipes that you might not have cooked before. Things such as, you know, lamb or temperatures for meat or fish or any other kind of food that you might be interested in.

You can monitor your products from various locations inside your house and outside your home. If you want to be outside in the garden, pulling some weeds, while you are checking to see how the roast is cooking, you can now do that without too much trouble.

It will allow you convenience, right? The ability to set clocks, to set special cycles, to download recipes from our websites, to make your life a little more convenient and to give you more functionality from your products.

Here is just a little bit of an example. (Video)

Our connected wall ovens are in the marketplace today, we are selling them to consumers, we are connecting consumers. Other products will follow shortly. We will soon see refrigerators, water heaters which will allow you to set the temperature from upstairs, as opposed to having to go down to the basement. You'll see your refrigerators hooked up, your laundry, with the ability to pull down new stain cycles. All of those products will be coming to you within the next year.

Thank you.

MS. YODAIKEN: Thanks, Mike. Okay, next is Jeff Hagins. Go on up. Jeff is the cofounder and chief technology officer at SmartThings, the startup that connects things in the physical world to the internet.

MR. HAGINS: Good morning. So I wanted to talk for a few minutes about some of the macro trends here. We are really living in a world where two big things are happening. Number one, we are seeing ubiquitous smartphones. In the U.S., now more than 70 percent of consumers have a smart phone. In other countries, it is even higher than that.

At the same time, we are seeing this explosion of connected devices that is being driven by reduction in manufacturing and costs for designing hardware, but also in the reduction in costs for how you actually connect.

And what is at the center of that is this interesting development that, each of these manufacturers is pursuing a model where I build my device, I connect my device to my cloud, my manufacturer-specific cloud, and then I give you, as a consumer, an app for your smart phone. And it begs the question, where this goes. Where does all of this end up? Do I really end up, at the end of the day, with an app for my oven and my refrigerator any my hot water heater and my thermostat and my General Electric lightbulb and my Sylvania lightbulb and my LIFX lightbulb, and my Phillips U lightbulb. I literally have three different apps for lightbulbs on my phone right now.

And it just doesn't seem like this is where this should end up, from a consumer perspective. If I end up with more apps on my phone to control the physical world than I have on my phone to begin with, to control all of the other stuff, it feels like we've failed the consumer in a big way.

And so at SmartThings, what we are working on is actually bringing a solution into the middle of this. We've created a platform that is targeted at the smart home, initially, and to put in the palm of the consumer's hand not one app per device, but rather one app. But more importantly, to allow these devices to work together.

Because what the manufacturers are doing, and I don't want to beat on GE or any of the others because, in fact, what we are witnessing is the right and logical evolution for where we are, right? That it would be unreasonable, in fact, to expect manufacturers to instantly work together to try to make all of these devices work together and allow you to use a single smart phone app, right? It would slow down the natural evolution of things.

And so where we are is the right place, we shouldn't act like it's not, but we also need to work on platforms like this, right? A single platform that can connect all of the devices within the home, give you a single app for controlling them, but again, more importantly, a single way in which these apps or devices, rather, can work together.

So that if I want to start the internet-connected coffeepot not at a particular time, but rather when I start waking up in the morning, because I'm using a quantified self-sensor that knows that I'm waking up. Waking up, not woken up, right? I'm stirring, start the coffeepot. So that by the time my feet hit the floor, the coffee is ready, right?

Now that's an example of two devices working together that frankly don't have any business talking to each other, right? We hear a lot about this idea that, well, your devices should talk to each other. That actually seems like a recipe for building incredibly expensive and complicated devices, right? If my sleep sensor has to know about my coffeepot, how much does the sleep sensor end up costing? A lot, right?

So devices actually shouldn't talk directly to each other. Devices should simply do what they do, but we will need some of these types of frameworks in order to allow devices to work together. And in the end, to deliver real value to the consumer. Because at the end of the day, this is about value.

You know, I have 130 connected devices in my home. And you should expect that, right? This is the space that I'm in. But I can tell you that most of those devices, in and of themselves, don't deliver a lot of value. It's the software layer, the applications that set on top of them that deliver the value.

So what we sell at SmartThings are kits of both hardware and connected devices, our own hardware, but we even sell lots of hardware from third-party providers like General Electric, so all of the inwall switches in my house are General Electric switches that are controllable.

And the timer is telling me that I'm out of time, because I actually did start a timer. We are redefining what the smart home means, because we believe that this isn't just about applications, it is ultimately about redefining services into the home, right? Connected devices, as we've already heard, provide an opportunity for integrated services.

So finally and to wrap up, we believe that the Internet of Things, done correctly, will provide a lot of benefits, and I'm not going to read through them. But in order to do that, there is a few things that we believe in that are really important.

Our things and our data have to be secured. And we, as the consumer or the owner of our things, need to own the data that comes from those things. They are our things, it should be our data. Just because I bought it from a particular manufacturer doesn't mean it's their data. It's my data.

That sharing of that data then needs to be contextual, and we've heard a lot about context already, and explicit. These systems need to be highly reliable and available and they also need to be open. One of the things that we are very concerned about, in fact, is manufacturers building products that will only work together and that won't be open so that they can be integrated with other systems. Because again, the value in most, or in a lot of cases, is in getting these devices to work with each other.

Thanks.

MS. YODAIKEN: Thanks, Jeff. Lee Tien is a senior staff attorney at the Electronic Frontier Foundation, a public interest law firm active in privacy and cyber security issues.

MR. TIEN: Good morning. I'm not really a cheerleader for the Internet of Things. To me, it raises a huge number of privacy and security issues, to the extent that IoT devices entail ubiquitous collection of large amounts of data about what people do.

And I mean, I think that's the main thing, that what we are talking about is collecting data about people's activities, and therefore that is always going to raise some very serious privacy issues.

I also wanted to -- you know, we are breaking up the agenda between like the home and the car and various other sorts of ways. I want to suggest that another way to think about this is, you are talking about, as Mike was saying, about your own devices. But you are also concerned about being targeted by other people's devices. And you are also concerned about -- or should be concerned about the environmental collection, a non-targted dragnet collection from devices in the environment. And the full range of privacy and concerns about the Internet of Things has to be thought of in that complete context.

So with respect to the home, my starting point is probably pretty conventional. As Justice Scalia said in the 2001 Kyllo Thermal Imaging case, in the home, our cases show all details are intimate, because the entire area is held safe from prying government eyes.

Now we are not discussing government surveillance today, but I think all consumer privacy, anyone who thinks about the privacy issues thoughtfully, is going to have an eye on what data about household activities or personal activities the government could end up obtaining, either directly from the devices or from IoT providers, whether using legal process or other less savory means.

Smart meters are a good example. This is an area where EFF has been very active over the last five years, we participated in the (inaudible) in terms of the privacy issues. And in California we, along with the Center for Democracy and Technology, helped write very strong FIPPS-based approach to energy usage data that is in the hands of utilities, recognizing in California that there was a lot of serious privacy issues around the granular energy usage data.

I like to use this quote from Siemens in Europe a few years ago where they said, you know, we, Siemens, have the technology to record energy use every minute, second, and microsecond, more or less live. From that, we can infer how many people are in the home, what they do, whether they are upstairs, downstairs, do you have a dog, when do you usually get up, when did you get up this morning, when you have a shower. Masses of private data. And obviously, this is a European perspective, which is especially solicitous of privacy, and yet the ability to make those kinds of inferences from energy usage data is clearly there.

Now in the Calfornia proceeding, one of the things that we do not do is we do not regulate anything about what the consumer, per se, can or can't do with the data that they have. Indeed, the whole thing is, right now, very consumer empowerment based, because it is consumer consent that provides the main way that utilities can hand the information off or share it with someone else.

We have, in addition, sort of primary and secondary purpose rules whereas, under the -- so that anything that is not for energy efficiency purposes ends up requiring express consent.

We also use rules that are modeled after HIPAA business associate type rules, so that downstream recipients of data shared from the utilities are bound in a similar way.

In the current phase of the proceeding, we are seeing a great deal of interest from academic researchers, from commercial entities in the solar field, and also from government in how to get data from the utilities. And right now, they were late to the proceeding so they now are unhappy with some of the rules, because it is actually much harder than they expected to get that data.

The thing that is interesting here is that, while there are real privacy risks, very, very few consumers seem to be aware of them. Indeed, when I spoke at a public utility lawyers conference about a month ago and we talked about the subject, along with the utility representatives, nobody in the room had any idea that there were privacy issues.

And so the thing that -- one of the issues I think we have to face is that the modern consumer just doesn't know that much about what can be learned from their data and therefore a lot of the notice and choice issues that we normally rely on for consumers to protect themselves, that's going to be a problem.

And as we are doing surveillance of the ordinary, and a lot more of the data is -- and it's a collection of extremely humdrum data, people have a tendency to underestimate what can be done with it.

So I want to end here with a couple of quick comments on the security issues that are raised by things in the home. I think that you have to worry also about the way that the wireless networking exposes data to interception. We are wary that industries who are moving into this space are not necessarily as mature about the security issues as those as, say, at Microsoft. The relatively cheap or lower grade devices may lack the computing resources or, for economic reasons, there will be less incentive to put good security in them. And fourth, that the security perimeter for IoT devices is actually rather different because, depending on where the endpoint devices are, there may be a higher risk of direct tampering. And there is also a likelihood of multiple or changing environments that IoT devices are expected to operate in, where they will connect promiscuously, don't necessarily have the ability to really know what kind of configuration of what the other device is going to be like.

I think that one of the things that is going to be important in this area is also the ability of the consumer to exercise what we at the EFF call the right to tinker or right to repair. I think in the comments, there were some rather interesting points about various kinds of consumer rights that could be built into this area. But I think one of the most important is actually being able to know, inspect your device, and understand them, to know what they do, because transparency is going to be a big problem.

And I'll just end with a quote from Microsoft in 2004, which actually did a really good report on RFID for the FTC workshop where they said that, "Trustworthiness demands not only that technology providers create hardware and software that embody integrity and provide fundamental security with reliability and privacy protection, but that all of these elements be demonstrated to the public inclusively."

Thank you.

MS. YODAIKEN: Next we have Craig Heffner, who is a security researcher with Tactical Network Solutions, a cyber intelligence company based in nearby Columbia, Maryland, with a focus on embedded infrastructure security.

MR. HEFFNER: So I think, unlike most people on this panel, I don't make things to make consumers lives better, I try to break those things. So I have a little bit different perspective than maybe a lot of people. And obviously this works out to kind of look forward into the future, how do we deal with these problems. But I kind of want to take a step back and talk about the problems we have now.

I mean, the Internet of Things, I think, really is -- it's a nice buzzword, but we don't really need that term. We already have things that are on the internet and we have a lot of them.

And consumer devices typically, they don't have any security. At least by today's standards. I mean, you have simple things like vendors leaving backdoors in their products, either because it is something that the developer left in and they just forgot about or maybe they left it in so that when they get a customer support call, they can remote into the system and fix it for them and so it lowers, you know, the time they have to spend doing tech support and things like that.

And we are not even dealing with sophisticated types of attacks to break a lot of these systems. I actually teach like a five day class on, you know, breaking embedded systems. And people -- that's why I'm trying to condense five days into five minutes here, but people are astounded at, you know, especially people from the security community who are used to breaking things like Windows and PCs and things like that, they don't really have experience with embedded devices, are astounded at the lack of security that they have typically.

And so I did a talk this year at a security conference on breaking cameras, like the ones we have in this room. And these devices range from cheap consumer cameras, you know 30 dollars, 50 dollars, up through 1,000 dollar cameras, 1,000 a piece. And I didn't have to do anything special to break into them. They had backdoor accounts left on them. They had simple vulnerabilities that anyone in the security community who looked at it would be able to break. And it doesn't take a lot of technical expertise to do that.

And I think the real reason why these exist, why we have these problems in embedded devices is there is no financial incentive to companies to make their devices secure. The example I always throw out is, when is the last time you saw a bad review on Amazon because some product had a security vulnerability? Never.

You see a bad review on Amazon because it had bad customer support or maybe because it lacked features, so that's where they focus. They focus on putting more and more features into their products, they don't focus on security.

And this is a two-fold problem because, with more features, comes more complexity and with more complexity you have more potential to mess something up, to have a bug in your software, to leave something there that you didn't think about.

You also have a problem with combining different technologies. So as we are trying to integrate everything together and put more features into our products and make end-users lives simpler, you are combining a lot of different technologies together and sometimes kind of mashing them together when they may not necessarily work. Or you might not necessarily understand the implications of things.

A good example is of one vendor trying to push cloud storage on one of their products. I won't name it, but they are putting cloud storage on their product and so they have these -- their products trust certain domains on the internet, certain servers on the internet, that are supposed to be their actual cloud servers.

Well, they forgot to purchase one of those domains. So I bought it and I now own a trusted cloud server for that vendor. And so these are simple things, right? I mean, I didn't even hack anything, I just legitimately paid nine dollars and bought the domain. And these are simple things that people may not think of, and may not think through, but they can be very difficult to go back and change, especially in embedded products. Because updating the software, updating the firmware, is not necessarily trivial in many cases.

So going forward, I think we need to really push vendors, give them some form of financial incentive or perhaps a slap on the wrist or something when they do things like this. And I think the stuff the FTC has done with TRENDnet recently is a good step in that direction.

Unfortunately, I don't think that trying to educate users will get us where we need to be. You know, the mantra for years in computer security has been educate the user, educate the user. Well, guess what? We've had security problems for decades. That clearly isn't working. Users don't understand the technologies they are dealing with. I hear the term, people always say, people are so technologically -- you know, they understand all this technology. No, they don't. They have a phone with pictures on it and they point at the pictures. That is not understanding technology. My 1-year-old can unlock my phone. She has no idea what technology even means.

So I think we really need to push vendors towards security as these embedded systems come out and become more prevalent and, in reality, they already are.

So if you have any questions on security, that's what I'm here for.

MS. YODAIKEN: Thank you very much.

MR. EICHORN: Thank you for those

incredible presentations. I feel like I'm taking us back to the Internet of Things 101, but I just want to get, as a foundational question, you know, Keith mentioned, you know, telerobotic surgery and autonomous cars and Carolyn mentioned finding lost sock pairs, which seems like a killer app, but all of these things sound kind of futuristic. I am just wondering, you know, to what extent the Internet of Things is here now and sort of a reality today.

MS. YODAIKEN: In the home.

MR. HAGINS: I'll take that. Certainly, we believe it is here today with the variety of different killer apps. Part of what we are doing is to actually trying to make it so that those apps are something that is in the hands of the consumer to choose which applications they want to layer on top of their devices.

And so the extent to which it is here today is really a function of whether those applications are delivering real value to the consumer, right? Because again, the devices, as I said, the devices don't deliver the value, right? At the end of the day, it is the software layer that does something functional and useful for the consumer.

And so it is here today and everybody in the room can answer this question, right? Do you have connected devices that are delivering value to you in your home? And I think a lot of us would say, yeah. There is probably at least one that is delivering some kind of value.

In my case, the killer app is having a sensor on my garage door so that, if I drive away, my garage door never gets left open. To me, that's the killer.

MR. BEYERLE: You know, I would agree. We are also looking for those applications, right, which allow the systems to do more, to deliver more to the consumers.

You know, one of the examples I use is what I refer to as the lasagna story, right? The idea that a consumer should be able to download a recipe for lasagna, let's say you are going to cook a Stouffer's lasagna, right? You pull that recipe down easily from the internet, you want to be able to load it on to your range so that it can cook it for you properly, make it nice.

At the same time, you'd like that system to be able to prepare for things which might happen afterwards, right? So for example, you'd like the dishwasher to set up for say a steam cleaning cycle because it knows it is going to see a bunch of baked on, burned on cheese. You'd like your washing machine to pop up a couple of stain cycles, you might suggest tomato sauce and red wine, because that is probably what it will see next because it ties back to the lasagna.

How can I deliver a little more to the consumer that makes the consumer's life a little easier by giving them new applications and an ability that they didn't have before.

MR. EICHORN: And I'd just say that being able to turn off your stove when you are heading off for vacation is kind of a useful thing, too.

MR. BEYERLE: There are two things we see repeated requests for. One is to check to see if my stove is off, right? Actually, three things. The other one is to turn the water heater down when they are sitting at the airport, because everybody wants to do that. And the third one is to be able to turn on the stove and preheat, right? So for example, when they are at a grocery store and they are coming home and everybody is rushed for time.

MR. LIGHTNER: And I think, you know, in the electric industry we are kind of stuck behind most -- I would think we are actively working on getting consumers access to their own information, in a standardized format.

Again, I mentioned Green Button in my remarks, but that's really where we are at now. How do we do that in a secure and private fashion, just to give consumers that access to that information.

MR. EICHORN: And I think the Smart Grid is obviously very well-developed. It is sort of a --

MR. LIGHTNER: Well, that's not really on a consumer level.

MR. EICHORN: Right, right.

MR. LIGHTNER: That's really about utility operations more than anything else. How we are going to automate and operate this system more effectively and efficiently, to handle things like natural disasters and other things.

MR. EICHORN: And Craig, what are you seeing out on the internet as far as devices that you can see online? A lot?

MR. HEFFNER: So a lot of stuff we are seeing is network infrastructure stuff, so you think of things like your wireless router, network cameras. I don't think that things like toasters and ovens are very prevalent on the internet right now, but obviously they're just not prevalent, period, in terms of something you can access remotely.

And certainly as these technologies are pushed forward, whatever they are, people will want to have remote access to them, so you'll start seeing more of them out there.

MR. LIEN: The only thing I wanted to add is that I think it is clear that it's here, in the sense that there is a lot of money being put into this particular trajectory, but I think that what is also here are little hints of the kinds of security and privacy issues that we're going to have.

You know later today, we'll be hearing from folks who are talking about medical device security and automobile security and we've already seen, in the early generations of internet connected cars and remotely accessible implantable medical devices, serious security vulnerabilities. And obviously one of the big differences between, say, a problem with your phone and a problem with your, you know, diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.

So one of the issues around this is not sort of thinking of this as the same kind of privacy and security issue that we have had before, but one that has much higher stakes.

MS. YODAIKEN: And we're totally going to dive into that a little bit more in this panel, but let's go through a couple of steps to get there.

So first, we talked a little bit about the devices we are seeing now in consumer's homes. Can you all talk a little bit about how those are getting there? Are they devices that are being manufactured to be smart, you know, rolled out as you get a smart meter, or are there technologies that are being rolled out that will add connectivity to a device that you already have, that perhaps wasn't originally manufactured that way? Anyone want to talk about that?

MR. HAGINS: Well, certainly we are seeing the whole spectrum of what you've just described. There are lots of lots of cases where I can buy sensors to attach to existing things, like a door, to know whether it is open or closed. Or devices that are advertised and promoted as connected devices, where part of the clear function and benefit of that device is its connectivity, ala the thermostat.

But also devices where the connectivity is a little bit more subtle, like the range or the refrigerator, where the primary function of the device is to keep things cold, right? And yes, it may happen to have that connectivity.

So I think we are starting to see things work their way into the home through lots of different channels and pathways. And over time, you know, we are going to see more and more and more of that. And I think that the point there is that devices are going to show up in your home that have the capability to be connected, whether you like it or not.

And so what's incumbent on the manufacturers is, again, to give that transparency and choice to the consumer, right? Just because a device has the capability to connect doesn't mean that it should.

MS. YODAIKEN: So Eric, can you just mention -- with smart meters, are all the capabilities turned on when they are installed or are they --

MR. LIGHTNER: In general, no. Normally

in an AMI, in a smart meter, there is really two radios, right? One radio that communicates your usage back to the utility for billing purposes. And a radio that is usually turned off, or that is always turned off, for now, that would communicate the usage directly to devices in your home. And that currently is a function that is not utilized to date.

So to really get access to your energy usage information, you usually go through a web portal that the utility has set up and that's password protected and it's your account information and that's how you usually get your usage information. It's usually a day late, so today is Monday, that usage won't really be available until the next day, on Tuesday, for you to see.

So it's not in real time, that would be the advantage of having communication directly with the meter, into devices. It would become more a real-time look at your usage, but for now, it is the next day.

MS. YODAIKEN: And just -- oh.

MR. TIEN: And again, I think it varies a lot with the industry, right? When we look at the appliance industry, we look at some of these more mature industries that have not been -- I mean, they have a lot of embedded computing, but they are fundamentally not like a Google or an Apple or a Microsoft. Then, you are looking at sort of a slower growth, I think.

Whereas, when I look at a company that -- one of the things we do at home is we play games, right? At least the generation younger than mine, very, very much into XBox and Kinect and all of these kinds of really, really cool gaming technologies.

But these gaming technologies are ushering in a tremendous amount of sensory collection and capture in the living room, right? Between voice commands and machines that are active that are able to listen and detect whether or not particular words are being stated in the room. They contain biometric technology, so they can do some level of face recognition and other kind of avatar recognition for personality. This is, I think, one of the most interesting factors for bringing this kind of connectivity and technology into the home.

MS. YODAIKEN: So Lee has given us some examples and also, when you were talking, you gave us some examples of the type of data. We are just focused on the data part that is being collected or generated by these machines.

Can you all just add a little something to that? What type of data, as we are going to start diving in soon into the ramifications of that, but what are we actually talking about? Because I think there is a lot of different information about that.

MR. BEYERLE: Well, you know, in the case of the appliances, right, as I mentioned, they are smart appliances to begin with, right? So you've got a refrigerator and the refrigerator is keeping track, for example, of how often the door is open, because we use that to determine when the refrigerator ought to go into defrost. And we can keep track, for example, when the doors are open, right?

So you might have time, you might have usage, you might have how many cycles you've done on your washing machine. How often are you using the white cycle or the color cycles, right? Those types of information become available on the device. They could be pulled down and a consumer can use them to better change their usage behavior, right?

So if you know when you are using a lot of electricity -- our first generation of appliances were tied into those smart meters and you could adapt the usage of your electricity to the time of use pricing that you might have in your area. So you could try to minimize the consumer cost.

You might realize, you know, how much money you are spending to do a hot water wash versus a cold water wash and change your behaviors, save a little energy and save a little money. So all of those types of usage information are available on those appliances.

MS. YODAIKEN: And Jeff, you were going to --

MR. HAGINS: Yeah, I think we see a couple of things. Number one, of course, the devices are generating data, and I'll get back to that in a second.

But number two, the consumers actually add contextual data into the systems. So with our system as an example, consumers get to group devices by room, for example. And so you can tell at my house, by looking at the data that we have in our system, right, I have my daughters' rooms. And what are they named? My daughters' names, right? Caitlin's room and Claire's room, et cetera, right? And there are motion sensors in those rooms.

So access to that data would tell you my childrens' names and whether they are in their room or not. It's very, very private information. We have less than 10,000 households today, so we are a startup. We just started selling actively at the end of August. Less than 10,000 households using our product, we generate 150 million discrete data points a day out of those 10,000 households. It's an enormous amount of data, most of which would put everybody to sleep.

It's not -- what's the battery level on this particular sensor, every two minutes. What's the signal strength on this particular sensor every two minutes. Most of the data is not meaningful or useful to anyone, and yet, as I've said, there's a lot of -- you can get the entire context of my home. Who is home, what rooms are occupied, the comings and goings of the family. There is an enormous amount of data coming out the house that has to be protected. And certainly I'm at the forefront of this as an industry, but as a consumer, I get very concerned about that data.

MR. LIGHTNER: Well, I think as far as utility is concerned, one of the major benefits of advancing the infrastructure is being able to tell whether the power is on or not on at your home. And that's an incredible advantage now, especially like in outage management. So if there is a storm that comes through and your home is out, in the past you had to call for them to know whether you were out of power or not. Now you can know automatically, so they can start scheduling crews and things to target, you know, where the outage is directly. So it's made it a much more efficient and quick way to recover from outages.

I mean, that's one obvious benefit. Not to mention some services that could be built around that for the utility, right? They could send you a text message like, hey, did you know your power was out and it will be restored in an hour or whatever.

So there's a whole outage management benefit to knowing specifically, at the endpoints of the system, where there is power on or off.

MR. TIEN: And the thing I wanted to add on this, I mean, there's two quick points. One is, it may be the same data. Sometimes it's the same kind of data or the same kind of inferences can be derived as might be from a more direct method. I mean, certainly there is research in the area of devices that are measurable -- hooked up to TV monitors that can basically distinguish between different types of movies and even identify movies because of the signature of either the noise or the power supply variations. You know, to an electrical network Die Hard looks very, very different from Remains of the Day.

And you know, another -- but you might know that from what I watch on Netflix, but the idea that the electrical signal variations are also a vector for that may not be, you know, as well known to people.

The other thing that I think is important is the way that particular devices get identified. And that may include, say, in the home, medical devices, dialysis machines, et cetera, et cetera, which become, you know, because of their addresses or other kinds of specific identifiers, leads to a high association possibility.

MR. EICHORN: So Lee just reinforced this point, I guess, which is Jeff, in your presentation, you had a slide about a lot of the benefits that consumers get, which we skipped over pretty quickly. But things like efficiency and convenience and so forth, things like that.

But just for the panel, I just wanted to ask what are the privacy and security implications of all of this? And Jeff, do you want to start on that?

MR. HAGINS: Well, as I've said, the data that is going to come out of this -- and everyone has pointed this out, right? You can derive an awful lot of very interesting and useful information about the data that is going to come out of this.

I think, and to echo Craig's point and maybe go a little deeper, it's not just that consumers don't understand the technology, it's that the people who are building it don't understand it. And for the non-engineers in the room, just because I'm a software developer doesn't mean I understand anything whatsoever about the security of an embedded device. Just because I know how to write PHP code on a website doesn't mean I have any appreciation for that at all.

And so, as engineers, we tend to think in this black box kind of way, right? I use these tools that are black boxes and a black box might be a piece of hardware, it might be utilities in an operating system, et cetera.

And so, you know, part of the issue from the security and privacy perspective is that the companies that are building this technology don't actually have all of the skill sets that they need and they are not applying them correctly to be able to actually address security and privacy from top to bottom.

MR. HEFFNER: Another issue that I've seen a lot is that a lot of companies, they are selling products, so they are trying to cut costs. So are they going to hire the best developers? No. They are going to hire the developers who work the cheapest. And those typically aren't the best developers and they are not going to be the ones who have the most experience with the technologies they are dealing with. They are going to be the ones who make rookie mistakes because they probably are rookies.

And without a good quality assurance process, which also takes money and people and affects their bottom line, those types of bugs will make it out into products in the wild.

MR. EICHORN: Lee, let me follow-up on a point that you raised earlier about the dragnet, because a lot of the products we have been talking about here for the home are products where I, as the consumer, go out and affirmatively seek it out and hook it up and connect it to my smart phone or whatever. So talk about the dragnet a little bit.

MR. TIEN: Well, I mean obviously I have been working in a smart meter environment, so that's one where, certainly in California, consumers don't have a whole lot of choice. The PUC has basically allowed PG&E and the utility to simply install smart meters. So that is sort of the classic example where you are instrumenting homes, with or without consumers real consent.

And it becomes part of what sociologists would call the furnished frame, as opposed to something that you deliberately chose to bring into the home environment, it's just there.

The variation on a furnished frame in the Internet of Things is that you don't really understand what it is that you brought into the home. You know you brought in an internet connected device, but as I mentioned before, you have no idea what the implications of it are.

You know, everyone in this room is familiar with the Target pregnancy assessment score issue, which is a classic example how, not so much on the technology software/hardware side, but on the data side, people just don't understand how various kinds of big data, operations can analyze the data to bring much more out of it than you ever would have expected.

And so this is not necessarily -- and it's not targeted because it's not like, gee, I want to know about you. It's that here's a lot of data that's become available, through the fact of embedded sensors. And I'm -- it's really a larger issue in the build environment overall. We see it in parking meters and we see it in various kinds of transportation and other context.

But it just produces these very, very large masses of data, which you can do all sorts of really fascinating analysis of, but the implications of that are that, even if you're not being targeted, it can be figured out, many, many interesting things about you, that you might not want, or probably don't want, anyone who has access to the data to be able to figure out.

MR. EICHORN: Yeah, I was thinking of -- this is an application outside the home, but in the U.K., they've had some instances of garbage cans that were internet enabled and were tracking people's locations around, you know, I guess, London.

MR. TIEN: Yeah, I mean government, it's an interesting question that we haven't talked about a lot, you know, sort of government embedding of these types of technologies into objects. I think we might get into that with the cars, because I think one of the big vulnerabilities in the car that Professor Kohno looked at is that there is a weakness in the onboard wireless interface that is apparently a regulatory mandate. So you are sort of stuck with a security problematic interface in automobiles. And that's not out of malice, that's just simply out of, I believe, a failure to do the good technology work.

MR. EICHORN: So, we have a question from the audience and it is basically about, you know, third-party sharing, which we haven't yet discussed. So about companies that have a direct relationship with consumers, but may be sharing that data in other ways and also whether information can be subpoenaed as well.

I guess I'd ask Mike, do you share information that you get from the use of the oven? Do you share that with third-parties or --

MR. BEYERLE: Well, right now we have very little data to share with anybody. We are trying to acquire some more data as we go along, as the product is rolled out.

I mean, we've got a very strong privacy policy. I mean, our kind of view of the world is that the data belongs to the consumer, that you ought to tell the consumer what kind of data you are going to collect, what you are going to do with the data, and who you might share that data with.

So for today, we do not share the data with anyone else, right? We may choose to market something to you, right, based upon your behavior interacting with GE, but we will tell you that ahead of time. So today, we do not share the data.

MR. EICHORN: And Jeff, what about the SmartThings model? Because part of the whole idea is that, as you said, you know, your alarm clock will allow you to sort of interface with some other app that is based on the time that you woke up or whatever, but does that information necessarily go somewhere and get shared or can it be resident --

MR. HAGINS: It stays on our service, so it goes into the cloud. It doesn't get shared with anyone necessarily, because when we talk about applications, they are actually running within the

SmartThings service.

That said, we do support a model that allows an application, that the consumer might install, to share certain information externally, but part of that model is an agreement, it is that contextual approval by the consumer that says this application is going to share this information for the following purposes, right, with the following third party. And the consumer has to agree to that sharing contextually before that application is able to access that information.

So we certainly believe in the idea that there is value that the consumer may want, right, that can be gained through sharing of information, but it has to stay entirely under their control.

And I think we are taking steps in the right direction, in terms of that contextual sharing of information, presenting explicit information in front of the consumer about what is being shared and why.

Whereas there are so many examples today of cases where information is getting shared, like how many people have pushed the button to say "okay" on a notice from your phone that says such-and-such application wants access to your location. And you say, okay.

Well, what's it doing with that information, right? And does it mean that the phone is just accessing the location, that the application is only accessing the location local to the phone or is it accessing that location information and shipping it off somewhere? And the answer is, you don't know. But you've said okay.

So I think that kind of context is just super, super important.

MS. YODAIKEN: Great.

MR. TIEN: And that's assuming, you know, that the device even has any kind of an interface for the user, right? Many of the devices -- I think many of the devices we would be looking at, especially with smaller ones, I mean, we already have display problems even with the machine that is designed to show you all sorts of things.

The idea that anyone would -- you can't do 80 screens, it doesn't make sense. And if it is an alarm clock, that is not actually going to be providing any sort of direct notice. You know, the entire sort of notice and choice aspect of Fair Information Practices has a real breakdown with a lot of these kinds of built-in devices.

MS. YODAIKEN: So Eric, I know you're trying to jump in and tell us this is a little bit different in utilities, is that what you were about to say?

MR. LIGHTNER: Yeah. I mean, the utility industry is fragmented, in that there are several different kinds of utilities, right? So for the most part, I think sharing information through large, investor-owned utilities is regulated and very much closely monitored. You need to give consent and those kinds of things for third-parties to have access to your information.

But as far as municipalities, electricity providers, due to conflicting regulations or conflicting laws, transparency laws, so if you're a customer of a municipality, your energy use information is public information. I mean, anybody has access to that, by law. And it varies state to state, there is not consistency across states in this category.

So it's really convoluted, I would say, and complicated in the electric industry and it really depends on who your provider is and what state you're in.

MS. YODAIKEN: Okay, so I'm going to jump in next to move us on, because we have about 15 minutes I think.

There are questions from the audience about how these devices, and I won't say talk to each other, Jeff, I got your message. But how these devices kind of interact, right? So some of the systems may be proprietary, other systems may be more open. And we've heard several mentions of wi-fi, perhaps, at home.

Can you all talk a little bit about how they actually are connecting and any implications of that?

MR. HAGINS: So there are a number of different standards that apply in the home. In our case, we support three different standards, wi-fi being one of them, but also two different home automation standards that are networking standards specifically for connecting these kind of home automation devices.

One is a standard called Zigby and the other is a standard, pseudo-standard called Z-wave. These are both mesh networking standards that are wireless, different frequencies. Zigby is 2.4 gigahertz and Z-wave is a 900 megahertz ISM standard, but these are RF standards.

At the end of the day, Zigby and Z-wave actually end up being potentially more secure than wi-fi. And I'd be interested as to what Craig has to say about this, but one of the interesting things that we are seeing, and Craig made this point, is that device providers tend to rely on the home network itself as the security boundary, as the only security boundary. Once you get that device connected to your wi-fi network, that's it.

And if you have security on your home network, then that's the security. And if you don't have security on your home network, then there is none whatsoever, right? But once the device is connected to that network, that is the only security.

So I think there is a lot of room for improvement, in terms of, you know, the context, the security context for the devices on these networks.

MR. HEFFNER: Yeah, so one of the problems obviously with using wi-fi is that you rely on the end-user having a secure wi-fi connection. And if that wi-fi connection is not secure, your data is now not secure, unless you've taken additional steps to encrypt it or otherwise secure it.

So I don't think that to rely on their

wi-fi being secure is particularly good. Even in situations where the end-user has done best practices, we've seen other technologies come out that subvert those.

Wi-fi protected set-up, I don't know if anyone has heard of that, if you have a wireless router, pretty much anything made since 2007 has this little push button on it. And the whole idea behind it was that, hey, end-users can't set-up stuff securely, even if they use the right, you know, encryption, like the strongest encryption, they choose a weak pass-phrase because it is something that they are trying to remember.

So the idea was look, you push a button on your router, you push a button on whatever you want to connect to your wireless network, and they automatically exchange, in a secure manner, this network key so this device can connect to your network. So you can have a very long, auto-generated, very random password that you don't have to remember.

The problem is that that technology, WPS, was itself broken. And so attackers can come along and break WPS and then, oh yeah, here's the network key.

And so now it doesn't matter how secure -- how good your encryption is, I have the encryption key and I can decrypt everything.

And you mentioned Zigby, I think Zigby does have -- with that in mind, Zigby does have the potential to be more secure. However, it has been broken. It has been shown, at least -- I don't know if they've come out with a new standard since there were some researchers who looked at it and found that the encryption could be broken.

So these are technologies that a lot of -- I am not an electrical engineer, but I do hardware stuff, obviously since I work with embedded stuff and I do build stuff, and it is technology that a lot of people, including myself, rely on. We say, hey, here's a chip, plop it down on your circuit and it just works. And you are kind of trusting all of that underlying stuff to have been engineered properly and that might not necessarily be the case.

And if stuff like that is broken, it is something that typically is very difficult, if possible at all, to upgrade. Everything deployed is insecure at that point.

MR. HAGINS: The other thing that we are seeing I think is interesting is that the level of, regardless of the connectivity, the level of security that we are seeing across devices tends to be relevant to some perception of risk on the part of the manufacturer.

Meaning that connected lightbulbs tend to have no security whatsoever, but the connected door lock tends to have more security, right? Because the manufacturer doesn't perceive, and rightly so, that the lightbulb should be secure. And so they put a lot more energy into securing the doorlock than they do the lightbulb.

And the question becomes whether that is -- is that an okay thing from a consumer perspective, right, that somebody can drive along in front of my house and hijack my lights, right? Which is completely doable.

MS. YODAIKEN: So -- yeah, go ahead.

MR. BEYERLE: I was just going to jump in with a couple of thoughts. One, and we want security by design, but it's difficult for the consumer. Because we want the consumer to input a 32 digit character string, right, to be able to connect two devices, and they don't get it right very often. And we started there, so we've kind of brought it back a little bit and have tried to make it easier, but you don't want to make it too easy that it causes problems.

But you have to make it so a consumer can actually use the devices, otherwise it provides no value, right? So you've got to work with those two trade-offs.

But there are things you can do to make these devices secure as well as safe, you know. For example, all of our appliances maintain their own software inside of there. So you can't set your range to 1,000 degrees. Somebody can't set your refrigerator to 90 degrees and have all your food go bad and the milk spoil. They only work within reasonable parameters that a consumer might use the product for. So you can build that software into the devices themselves, which further adds to the security and the safety in the system.

MR. EICHORN: So, there were a couple of reports that came out yesterday, white papers basically, and they both suggested a similar thing which is that the Internet of Things presents some new challenges to notice and choice.

And one conclusion that they both supported was that basically, because of the potential new uses of information that may occur to companies after collection, that sort of the idea of specifying the purpose for what you are collecting information is sort of passe.

What do you all think of that?

MR. HAGINS: I'm a big fan of contextual privacy and contextual sharing. You know, our terms of service say specifically that we use the data only in as much as we need it to provide the service that we are delivering back to the consumer and that anything beyond that has to have explicit notice and consent from the consumer.

That sounds like a cop out to me, it really does. That it's not -- it's not an easy problem, there's no doubt. But I think that there is also no doubt that, if we just say that that's a passe notion and don't try to solve it, that predictable things are going to come from that.

MR. TIEN: And let me jump in here for a second. I mean, the predictable things that happen when large, large amounts of consumers' information is stored is that they -- it either gets monetized or it gets made accessible to the government. And the question of government access which was raised by an earlier question is a very significant one, especially when you -- because what you are essentially talking about is that an infrastructure -- when you look at it from a law perspective, the Internet of Things is an infrastructure of surveillance.

And so the only question is, how do you -- is there a way to actual govern government access to that kind of information? And all of the security stuff that we've been talking about is, you know, in this day and age, we have to wonder about how well that actually works as a defense against any kind of subpoena or other kind of legal or nonlegal process, given that we are seeing a lot of operations now that are designed at obtaining keys.

And to use SSL as a relatively convenient kind of process, you're talking about a key -- and so if there is a compromise of this private key, it compromises every communication, you know, transaction that uses it.

So the question of surveillance naturally sort of leads us to say, well, you know, there should be strong presumptions in favor of minimizing not only collection, but minimizing retention.

MS. YODAIKEN: So along those lines, I guess, we are talking about all of the things that can go wrong and folks who are trying to, you know, make some effort to secure devices before they are in the home, what are some of the things that these companies should be doing?

And let me start off with Craig, because I think Craig has an idea of what they're not doing, but when you were talking up here, you talked about how there were really simple things that have been overlooked.

MR. HEFFNER: Yeah, so I mean basic best practices in writing code, really. I mean, we've known for years that there are things that you should not do if you are dealing with untrusted data, i.e. data from an outside source, like a user or anybody else. And you see them doing these things that, you know, people for literally decades have been saying don't ever do this, this is bad.

And it is clearly an experience coupled with, I'm sure, a push from management to get a product to market. And so they are trying to push this product out as quickly as possible and they do whatever they need to do to get it working, but that doesn't mean that they've done it in a secure manner or that they've done it properly.

So I think that, if you can get vendors to realize, or if you can make, somehow, the market affect the bottom line of the vendors when they do insecure things like this, then they will actually spend money on that.

Until then, I don't think we are going to see vendors take security really seriously. I think the bottom line is, until consumers care enough to stop buying their products, vendors aren't going to care.

MR. HAGINS: Yeah. Well, I've got a long, long list of what, you know, of what vendors should be doing that they probably aren't, but let me try to give you some of the highlights.

You know, I think security from top to bottom, in every possible aspect of your product architecture. From a skill set and an responsibility perspective, I would guess that if you went into most of these manufacturers or vendors and tried to find somebody who had security in their job title, you wouldn't. And so there is some kind of simple organizational and responsibility kind of approaches here where, if someone at an executive level, has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security.

I think basic best practices from

development and networking, et cetera perspective are important. But also, you know, we've talked a lot about the data that comes out of your devices, but not about the control -- a little bit about the control, but not enough about the control of the devices themselves.

So as an example, in our service, in our platform, you know, we -- I've talked about contextual sharing, but in fact even the applications that we write on our platform have to have explicit authorization from the consumer in order to access a particular device. So even our own applications can't access a device unless you, as the consumer, say that's okay.

And so we've built -- it's security by design. it sounds a little trite, because we say it all the time, but it is, you know, building security into every possible level and layer and to not just look at security as something where you are addressing a threat or an attack vector from the outside. You have to address it from inside out and address all levels.

MR. TIEN: I want to throw in just a couple of quick points. Earlier, I talked about the right to tinker, the right to repair, those sorts of important things for the consumer. And obviously no one assumes that everyone is going to be able to hack their own devices, the general rationale here is that, if they are open enough so that people can play with them, then the security researchers and the hacktivists -- will apt to really be able to do some decent testing and analysis of what is going on and how others understand what the devices do.

The other, I think the other really, really big issue here is simply that the companies need to make -- somehow figure out a way around the incentive problem, or we have to figure out a way around the incentive problem. It is not always that mismatch, it is just structurally the market is going to be very, you know, geared in the wrong direction for what we need. And I think we are going to have to expect the monetization of data, the over-collection of data, and the weakening of security without a large systemic approach.

MR. EICHORN: We are about to wrap up, I guess. There is a question from the audience about, is there any device that would not be more useful if internet connected?

And I know there is an internet connected toilet, so my answer would be no, but in a corollary, is there any device for which there is not a security or privacy risk? I don't know if anyone wants to jump on that.

MR. HEFFNER: So I think, from the standpoint of security, let's say that you hypothetically have a device that you don't care if someone breaks into, you just don't care. It has no important data on it whatsoever.

But if I, as someone out on the internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about.

So I would say, at least theoretically, no. There should never be a device on your network that you shouldn't care about the security of.

MR. EICHORN: I think on the smart meter as well, I mean, there are things that you might not care about where, you know, you might not care about your toaster, if someone knows that your toaster is on or something. But then, as Lee mentioned, if it is continual real-time data, somebody could figure out what TV show you are watching that you might care about or --

MR. LIGHTNER: Well, but that's not -- I mean, smart meters basically monitor the total usage of your home, not individual circuits or plugs, so it's really apples and oranges really.

MR. EICHORN: And also they don't -- they usually do not report on a real-time basis, right? It is usually about a 15 minute snapshot or --

MR. LIGHTNER: The data is usually collected in 15 minute intervals, that's correct.

MR. TIEN: It does raise a perimeter issue though, right? I mean, there are a lot of ways you can design the systems for devices to strongly favor local storage. So you can imagine systems that utilize connectivity and computing resources, but keep the data within the home boundary or at least keep the interesting variations within the home boundary.

I mean, in the smart meter area, people have talked about a neighborhood or block aggregation and various other types of techniques where the signal -- where it is not necessary, you might believe, to get the -- for the energy efficiency uses or for demand response to actually know things to a certain level of detail.

So a lot of what we are talking about is how much detail do we need and how much data actually has to leave the home or device in the first place.

MR. LIGHTNER: Right. So that's not in the application --

MR. HAGINS: And my advice for consumers is, certainly there is no rush to connect things, but rather focus on the real problems that you want to solve, right?

What is -- in my case, having my garage door left open overnight, you know, repeatedly, led me to want to solve that problem because I've got valuable things in my garage that I don't want to have disappear. That's a problem that I wanted to solve.

So I think if you focus, as a consumer, from the standpoint of the value that you want to create and the problem that you want to solve, that's what should limit, you know, what things that you connect in the near term.

MS. YODAIKEN: Okay, great. I think we don't have any time for anything else. So thanks to all of our panelists, it's been great. I'm sure this conversation is going to continue.

And now, we have a 15 minute break before our keynote speaker.

(Whereupon, there was a brief

recess.)

MS. MITHAL: Thank you everyone. If everybody could take their seats. My name is Maneesha Mithal and I am with the FTC's Division of Privacy and Identity Protection.

It is my absolute honor and privilege to introduce our keynote speaker at today's Internet of Things workshop, Mr. Vint Cerf. Now, Vint Cerf needs absolutely no introduction. And for those of you who do need an introduction, we have his bio outside with the materials.

Let me just spend one second going over some of my favorite things that I picked out from his bio, including just some nuggets.

So as many of you know, he is Vice President and Chief Internet Evangelist for Google. He has been known as one of the fathers of the internet and, in terms of the awards he's won, they include the Presidential Medal of Freedom, the Queen Elizabeth Prize in Engineering, the Library of Congress Bicentennially Living Legend Medal, and my favorite, simply from Stanford Engineering School, Hero.

So Mr. Cerf has agreed to take questions after his presentation, so we have paralegals coming around with notecards, so you can write your question on a notecard. I will sit here, I will take the notecards, and we will have ten minutes of Q&A at the end of Mr. Cerf's presentation.

So without further ado, Mr. Vint Cerf.

KEYNOTE SPEAKER: VINT CERF

MR. CERF: Thank you very much. I always get nervous when people clap before you've said anything. It won't get any better than that, so maybe I should just sit down.

I have a hard stop at noon, I'm going to try very hard to leave some time for questions because I think that it's important for me to know what you really wanted to hear as opposed to what I composed.

I'm going to start out by giving you a little bit of sense of what the internet is like today. It looks something like this. And the picture is really colors of different internet service providers. There are 500,000 internet service providers now, or more, that make up the global internet. What's interesting is that this is not controlled from the top, this is a completely distributed system. Every one of those internet service providers has his or her own business model and it could be for profit, not for profit, government, amateur, whatever it is. They run whatever software and hardware they choose to use, they choose to interconnect to people, and there is no dictated requirement for interconnection. There are no rules about whether you pay or don't pay, whether you peer or not.

This is an entirely collaborative activity and it is global in scope. So it's really quite astonishing and it has been expanded by RF, you know, radio frequency devices, including wi-fi and all kinds of mobile communications capabilities.

I would like to point out to you how interestingly powerful the mobile has turned out to be. The two things, the internet and the mobile, mutually reinforce each other's utility. The mobile allows you access to the internet at any time, assuming you are within range of a base station, and the internet allows the mobile to get access to all of the content, all of the computing power, and all of the other functionality of the internet and the world wide web. So the two have been very mutually reinforcing and, as you can see, the rapid expansion as a consequence.

There are -- these are statistics that are probably midyear, slightly under a billion devices on the network. These are devices that have domain names and have fixed IP addresses that you would typically find if you were searching for things. It does not include laptops, desktops, mobiles that are intermittently connected to the network.

So the absolute number of internet-enabled devices could be in the billions, probably three or four billion devices, maybe not all connected all at the same time.

The number of users, again, is not exactly well-known because there isn't one place where you have to sign up so that we can keep track, but a reasonable estimate is about 3 billion people. Which means that, as the internet evangelist, I have 4 billion more people to convert, so I can use help if anybody is interested.

There are on the order of 7 billion mobiles in use, although that does not translate into 7 billion people because a lot of people have more than one. Maybe many of you do. Certainly, in other parts of the world that is the case. Maybe a billion-and-a-half or so personal computers and laptops and things like that. So that's sort of the global picture. It is a very large, very distributed system.

But I want to go back in history, this is mid-1975 and we were experimenting with mobile radio and we needed this giant van at SRI International in Menlo Park, California to do the experiments because the radios were about a cubic foot in size and cost 50,000 dollars each. So the white boxes that you see behind the lady in the bottom part of the picture are the cubic foot sized packet radios.

But the point I wanted to make is that we were experimenting with packetized voice in the mid-1970s. And so a lot of the applications that you think of as new today have pioneering exposure, literally 35 years ago.

Now this was particularly amusing because, in order to do this, we had to take the voice signal, which was 64,000 bits per second, and compress it down to 1,800 bits per second because there wasn't very much capacity in the network in those days. And when you do that, you basically model the voice track as a stack of cylinders and you send the diameter of the cylinders to the other side, there is only 10 parameters plus a forming frequency, and the other guy inverts that to make sound.

It made everyone who talked through the system sound like a drunken Norwegian. And there's a long story about trying to demonstrate this to a bunch of generals in the Pentagon which is pretty amusing, but they came away impressed that we could do other than data with a system like this. We were also experimenting with packetized video as well.

So I want you to -- you heard in this earlier panel, which by the way was really good, I enjoyed listening to the comments that were made. The list is really quite long now of things that are either currently networkable or will be networked in the future. Television, the mobile obviously, tablets, picture frames and things of that sort, lots of sensory systems are becoming part of this environment, and those systems are used for a variety of different purposes. Some of them might be for security, some for environmental monitoring. In one case, agriculture, there is a guy that has a GPS location for every vine in his vineyard and he keeps track of the state of the soil, watering, pH and everything else, literally on a vine-by-vine basis and he uses that data to decide how much water and what kinds of nutrients should be made available to each vine in his vineyard. And that's the sort of thing that is not at all unreasonable.

Medical instrumentation also becoming very common. Here is a simple example of an insulin pump, which is keeping track of the blood sugar levels on a continual basis and then instructs the

-- the pump decides, based on that sample of information, whether or not to inject some amount of insulin into the body.

That information could be captured, for example, by a mobile and then used for analytical purposes. And I think this notion of continuous monitoring, which came up very briefly in the panel discussion, is important for several reasons, not the least of which that continuously monitoring things tells you about the processes in a much more refined way then if you showed up at the doctor once every six months or once every three months or only when you're sick.

And so this continuous monitoring is not just for the medical cases. It is for many other kinds of instrumentation and turned out to be really important and valuable ways of observing dynamic processes and then using that data to analyze their state.

Fitness kinds of measurements, many of you might be wearing Fitbit or might just be using applications in your mobile that are keeping track of how much movement during the day, whether you went up or down or sideways, how many steps did you take.

This, by the way, is also important because there is a feedback loop here. So one of the interesting things about gathering data in this way, with this internet of things, is that you get feedback that tells you something about the consequences of the choices of your behavior in the course of the day or the month or the year.

In the case of electrical appliances, as in the Smart Grid, if you get enough information back about what devices you use during the course of the month that generated a bill, you know, this might actually tell you or cause you to change the choices that you make because the costs might be less.

And you can imagine a third-party analyzing the data, which you presumably authorized, to tell you what steps you could take to change the way in which you use not only electricity, but possibly other consumable resources like water and gas and so forth.

So there is an important benefit, potential benefit here having to do with feedback to us about the consequences of our behavior, whether it is health consequences or financial consequences or something else.

Remotely controlled devices turn out to be pretty important, especially in crisis response. It was mentioned, for example, that knowing that the power is out in your home might be a very important thing to know, especially if you are not there. It is also helpful for the power company to know which houses are out of power. Often, that's not as easy to find out as you would like and, of course, it's clumsy to have people call a telephone number to try to report that.

There are an increasing number of devices that we'll call wearables. Google is experimenting with one called Google Glass. Here, I want to emphasize something interesting about this sort of internet enabled device.

The Google Glass is an experiment. What's interesting about it is it is essentially no different, functionally, than strapping this to your forehead, but I can tell you this is very uncomfortable. Google Glass is a little bit easier. It has a camera, it has a microphone, it has a bone conduction speaker so that you can hear what it is saying and no one else can, it also leaves your ears free to hear the ending sound and it has a little video display.

And the reason this is so interesting is that it brings the computer into your audio and video environment. It sees what you see and it hears what you hear.

So here's an example that we can almost do. Imagine you have a blind German speaker and you have a deaf American sign language speaker. They are both wearing Google Glass and they want to communicate with each other, so let's see what happens.

The German guy says, "Guten nachtmittag. Ich heisse Vint Cerf." Which is good afternoon, my name is Vint Cerf. And of course the deaf guy doesn't hear this, but the Google glass picks up the sound, translates the German from German to English and then presents the English on the display so the deaf guy can actually see the captions.

Now, the deaf guy responds by signing, which the blind guy can't see, but the camera in the Google Glass that the blind guy is wearing can see the signs, translate the signs into English, translates the English into German, and speaks that German through the bone conduction speaker in to the head of the blind German-speaker.

So the two of them are now communicating thanks to the intermediation of this Google Glass. Now, I don't want to mislead you into thinking that we can actually do all of that. We can come awfully close. The one thing that we can't do right now is actually correctly interpret signs at speed, but this is not something that is crazy. I mean, this is the kind of engineering thing that is possible.

And then, of course, automobiles with OnStar being an example of that, but there are lots and lots of thoughts about having automobiles communicate with each other. When you get into some of the exotic cases that Google -- self-driving cars, you begin to see some fascinating possibilities for the utility of cars talking to each other. When all four of them come to an intersection, instead of one of them wanting to be macho and everything else, they just run the standard algorithm to figure out who goes next. They don't have road rage, they're not impatient. They just do the protocol, unlike human drivers.

So here's an example of things that are already in use. The internet-enabled refrigerator is interesting because I used to wonder, you know, what would you do with an internet-enabled refrigerator.

Well, one obvious thing is that it might have an nice touch-sensitive panel on the front and it augments the ordinary American family communication method, which is paper and magnets on the front of the refrigerator. Now we do blogs and email and web pages and so on.

But then if you had an RFID detector inside the refrigerator and the things you put in had little RFID chips on them, the refrigerator would know what it had inside. So while you're off at work, it is searching the internet for recipes that it could know it could make with what it has inside. So when you come home, you see a display saying, you know, here's all the recipes you could make.

And you could extrapolate on this, you could be on vacation and you get an email, it's from your refrigerator, and it says you put the milk in there three weeks ago and it is going to crawl out on its own if you don't do something.

Or you are shopping and your mobile goes off and it says, you know, don't forget the marinara sauce. I have everything else I need for a spaghetti dinner tonight.

But the Japanese have messed up this whole beautiful idyllic view. They've invented an internet-enabled bathroom scale. You know, you step on the scale and it figures out which family member you are, based on your weight, and it sends that information to the doctor and it becomes part of your medical record.

Which is all perfectly reasonable except for one thing. The refrigerator is on the same network as the scale. So when you come home, you see diet recipes coming up.

Everybody is familiar with internet-enabled picture frames. Many of you probably have them. Some of them are on the net. They pull images from a selected website and then they will cycle through. We use them in our family, you know, we have mobile phones with cameras in them, so we take pictures and upload them to a website with all of the family picture frames, download those pictures, and you get up in the morning and you kind of see what the nieces and the nephews and the grandchildren are doing.

There is a security issue here. You know, if the website that has these pictures gets hacked, then the grandparents may see pictures of what they hope is not the grandchildren.

There is a guy in the middle here who has built an internet-enabled surf board. I haven't met him. I have an image of him sitting on the water, you know, waiting for the next wave thinking, you know, if I had a laptop in my surfboard I could be surfing the internet while I'm waiting for the next wave.

So he built a laptop into the surfboard and he put a wi-fi service back at the rescue shack and now he sells this as a product. So if you want to go out on the water and surf the internet while you are waiting for the next wave, that's the product for you.

Mobiles are everywhere. Internet-enabled lightbulbs got mentioned in the panel discussion. I actually used to tell jokes about this 20 years ago. I'd say, you know, someday every electric lightbulb will have its own IP address. Ha, ha. I thought that was funny, until I was given an IPv6 radio-enabled LED lightbulb. They cost about 20 dollars, they probably last about 15 years. The cost of putting the radio in might be 50 cents or something, which is not bad considering the total price of the lightbulb. And if it lasts for 15 years, maybe this isn't so crazy.

And finally, Google Glass, which you see being modeled by Sergey Brin.

So let me go -- this is another example. I have a sensor network in my house that is using IPv6, it is a radio-based 6LoWPAN system and this is -- it was a product. So it was not me in the garage with the soldering gun. The company that made this was called Arch Rock, which was acquired by Cisco Systems a few years ago.

Basically, each one of the devices is about the size of a mobile. It runs on two AA batteries for very nearly a year. As an experiment, I just let it run until it wouldn't work anymore and we got down to about 2.4 volts when it finally pooped out. The guys at Arch Rock were actually kind of astonished it lasted that long.

But this thing is a mesh network, so when you turn it all on, it self-organizes and the storing forward hopping takes the data from each one of the sensors and ultimately delivers it through the mesh network to a server that is down in the basement in a rack of equipment.

So it is measuring temperature, humidity, and light levels in each room in the house every five minutes. And the comment that was made earlier about the quantity of data that could be generated by devices is exactly correct. It is possible to produce a substantial amount of information.

Now in my case, I am actually very interested in gathering the data that way. I know it sounds like something only a geek would do, but think for a minute of having a year's worth of information about heating, ventilation, and air conditioning in every room of the house. At the end of the year, you have a pretty good idea of how well was the heat distributed and the cooling. You don't have to rely only on anecdotal information, you have real engineering data to do that. And so that's useful.

I haven't got to the privacy side of this and I'm not ignorant of it, nor were the panelists, but I want to keep going a little bit further.

One of the rooms in the house is a wine cellar and I'm concerned that the temperature stay, you know, below 60 degrees Fahrenheit and the humidity stay about 40 percent to keep the corks from drying out.

So this room has been alarmed. And if the temperature goes above 60 degrees or the humidity goes above 40 percent, I get an SMS on my mobile.

And this has happened once or twice.

One time, I was away for several days, and my wife was off somewhere else, and so every five minutes for three days I kept getting a little message saying, "Your wine is warming up." So when I got back home, I called the Arch Rock guys and I said do you make remote actuators so that I can actually reset the cooling system. They said yes. And then I said well, do you have strong authentication because I have a 15-year-old next-door and I don't want him to mess around with my wine cellar. And he said yes. So that was a weekend's worth of work.

Then I got to thinking, well, what else could I do. And I could tell, for example, that somebody went into the wine cellar when I wasn't there because I could see that the lights went off and on, but I don't know what they did.

So back to the RFID chips, if you hang an RFID tag on every bottle, then you could run an instantaneous inventory to make sure that no bottles have left the wine cellar without your permission.

So I was proudly describing this design to one of my engineering friends and he says, there's a bug. I said, what do you mean there's a bug? And he says, you could go into the wine cellar and drink the wine and leave the bottle. So now we are going to have to put sensors in the cork. And as long as you are going to do that, you might as well sample to figure out whether the wine is ready to drink, so before you open the bottle, you interrogate the cork. And if that's the bottle that got up to 80 degrees or something during the summer heat, that's the bottle you give to somebody who doesn't know the difference. This is an entirely practical thing to have around the house.

In all honesty though, this is going to be a very common kind of thing to do. I would expect this to be built into most new homes. It would be, certainly that plus many other kinds of security controls, heating, ventilation, air conditioning, other kinds of things, building on the notion of the smart home, which we heard about a little earlier.

Here is an example, and this is not so much about the beer as it is about a sensor which is very cleverly designed to help you figure out if a big keg of beer is empty. The normal way that this is done, you know, in a bar is that some guy has to go back behind the counter and rattle the kegs to try to -- and lift them up to try to figure out how much beer is left.

So this company made a little doughnut-shaped sensor and it goes underneath the keg and you've outfitted it with information about which kind of beer is in the keg with just using the scanner and a uniform product code, and that outfits the sensor with the correct information so that it knows how much weight to anticipate for a keg full of beer of that particular variety.

And so you just interrogate the sensor. So this little doughnut thing just automatically tells you, based on weight, how much beer is left in the keg. This is a good example of the simple kinds of ideas that make things a lot easier, that would otherwise be awkward. And that's all about using sensors as a way of making life a little bit easier to solve a variety of problems. Now this also, of course, introduces a lot of the problems that we heard from the panel.

Smart cities are another extension of the smart home, the smart grid, and the smart devices. And given that -- I have to be careful of my time here. I don't know that I can go through everything here, but you can imagine for a moment that a city that is able to monitor what is going on in the city, with traffic flow being an obvious example of that, could make quite a big difference for people trying to select which routes to take.

At Google, we bought a company called Ways and that is being reported as a crowd-source thing that you can imagine instrumenting the city to get even more precise data, dependent on simply voluntary reporting.

But you can see that other kinds of information, like outages or usage of water or other kinds of gas and so on, all of that information could be available to a city for use in immediate operations and possibly also for use in projecting demand in the future.

So I have this sense of monitoring reporting in the city being a very powerful idea that -- there are some cities, like Barcelona, that are rapidly moving in that direction. So if you are interested in smart cities, you might do a Google search for Barcelona and smart city and see where they are.

It's obvious that there are all kinds of things that the governments can do, local governments, state governments, and so on, to communicate with citizens about things that they care about. Whether it is license fees or taxes or other sorts of things, it is yet another example of smartness. It is not so much to do with sensors, it just has to do with city services being presented users on a 24-hour basis.

It is kind of interesting that the government -- after companies realized that they should be available to consumers 24 hours a day, the consumers started to say, why can't the government do the same thing? I don't want to hear "Sorry, our offices are closed."

Another issue is access to the information that the city might be able to provide. And setting aside privacy concerns, not to ignore them, but merely to say if there is information which does not have a privacy issue associated with it, open access to information that the city knows about its operation could facilitate the creation of new businesses that gather the data or analyze it for purposes of being useful.

So this notion of using information from an online environment, from a monitored environment, is actually an opportunity to create new businesses, new jobs, and things of that sort.

In fact, one of the interesting statistics

I wish I had, and do not have, from the Labor Department is some sense of how rapidly jobs are changing. You know, it would be interesting to look over five year intervals at what jobs are commonly being occupied and what those tasks are and do those jobs still exist or, you know, how many jobs are there that didn't exist five years ago? And I think if you were to look, certainly in the high-tech industry, you would discover very quickly that jobs in that space change very, very rapidly. I mean, think about the world wide web in 1994, there were no webmasters. And now, of course, there are lots of them because, you know, they figured out how to be webmasters by looking at the HTML code in the web pages.

And finally, there is a smart grid program, but I am assuming that that might have already been discussed, so I won't bore you with a repeat.

Now here's an example of a self-driving car. This man is blind, he's one of our employees, and I have a little video here that runs about three or four minutes.

How many engineers does it take to train me on the computer? I think I may have pushed the wrong button, let's see. Add favorites? I certainly don't want to do that. There. No. This is a Microsoft product, that's why. Here we go.

(Video)

Isn't that great? How do I get back to my slides? Here we go. This is really amusing, isn't it? Here we go, okay.

One of the things that I wanted to point out about the self-driving car is that it is one thing to get a car to drive on the road, you know, out in traffic and so on, but it is something else to get it go door-to-door. Because then you have to navigate underground parking garages and a lot of other things, it's actually hard.

Let's now move back to the Internet of Things. There are really enormous potential here for all kinds of optimizations based on the data that is accumulated and potentially shared. And so we should not lose track of the fact that having greater knowledge of how resources are consumed, when they are consumed, and at what rate and everything else, and aggregated over, you know, potentially larger and larger regions, could really tell us a great deal about how to manage those resources better.

The second thing is that standards are really important here because interoperability is very, very important. And so finding standards that everybody can follow, even though there is a natural tendency in some product development to do things that are proprietary, locking into that particular standard, there is almost invariably pressure arising in the end to have common standards, so that devices are able to work.

If you go and buy an internet-enabled device from Company A and then you buy another one from Company B, there are good reasons for you to want to know that they can both be managed through a piece of software that understands what the standards are and not have to be adapted to every possible proprietary protocol. It doesn't mean that we will end up necessarily with exactly one protocol, but you certainly don't want too many of them.

And by creating those standards, you create a real opportunity for new businesses to form, whether they are to manage the devices, to make the devices, to analyze the data coming from the devices, to control the devices, there are new businesses that can be formed. And we should care about that because these types of devices can create new job opportunities for all of us and improve GDP growth.

It's obvious that we have health management and wellness opportunities similarly through this continuous monitoring, which we talked about before. There is even some very interesting educational implications of all of this. If you have internet-enabled devices, you may be able to get access to information from anywhere and we are seeing that effect in the internet with things called MOOCs, which I imagine everybody has heard about by now, massive online open courses.

One observation I want to make about the MOOCs is that, if you do the math with regard to the economics of it, it's pretty stunning. If you have 100,000 people taking a class and you charge each of them 10 dollars, it's a million dollar class. There aren't very many professors that can claim that they are teaching one million dollar classes. And the cost per student is very low because of the scaling effect. So I am very excited about the potential to provide access to a large amount of educational material at a very modest cost to a very, very big audience. And by reducing the cost, you make it affordable to a larger cadre of people.

And second, because they are online and you can take them whenever you want to, continuing education becomes a pretty attractive possibility for people who want to continue to grow in their jobs. And it's pretty obvious that as soon as it's easy to internet-enable things, people will go out and do that, so there will be new products and services on that basis.

But there are challenges, and so I think we should at least look at those. One of them is, again, standards. I am a big fan of IP version 6. In fact, I would like to ask all of you a favor. You understand that when we did the design of the internet in 1973, we didn't know if it was going to work and we didn't know how big it was going to get. So we guessed 4.3 billion terminations should be enough to do an experiment, that was a 32-bit address space.

Well, in February of 2011, we ran out of the IP version 4 32-bit address space, so we standardized in 1996 an IP version 6 128-bit address space. We trained that system on the internet, with any ISPs and service providers that were prepared to implement IPv6 on June 6th of 2012. So the 21st century internet is functional, but not enough people have implemented IPv6 at the ISP level.

So what I'd like you to do is to go ask your ISP when will they have IPv6 available for you. And the reason it is important for you to do that is that a lot of them are saying, nobody is asking for it. And of course no reasonable consumer should even know what IPv4 or IPv6 is, so it's a silly excuse. But you can help by just asking what is the plan.

The 128-bits, by the way, gives you 3.4 x 1038 addresses, which is a number only Congress can appreciate, I think.

There is a very big problem in configuring large numbers of devices. And anything that we could do to make that easier -- the comments about security really resonated with me. It's very hard to expect users to understand and even have a reasonable working model in their heads about what these things are doing.

The comments about privacy and the alerting of users to the use of information, although I think that it is well-intended, I am thinking about the ordinary user who isn't really either sure or may not have the patience to try to figure out exactly what does it mean, what are the implications of this particular piece of information being made available.

I think people are lazy and don't want to be bothered and they just want stuff to work, which I think puts an even bigger burden on the implementers and the operators of these systems to be very, very cognizant of protecting users' safety and their privacy.

It's not simple to figure out what to do with all of the instrumentation and the data that comes back. But as I said, I think there are huge opportunities for analysis of that information.

The other big problem is there are going to be bugs. And those bugs can either be hazardous, because they offer an attack surface to allow someone to take control over the device, or possibly through control, will get to other devices in the home network, or they will simply cause problems. And getting things fixed is hard, especially if you don't have a good model in your head for exactly how this stuff works.

So by the way, that may actually create yet another set of job opportunities for people to come out and help fix your internet-enabled devices when they don't seem to work. That suggests, again, the potential opportunities for third-party businesses.

That says lunch, so before you break for lunch, I am happy to spend another ten minutes on questions, if there are any. Otherwise, you can go to lunch early.

MS. MITHAL: Sure. So let me ask the first question that has come in. This is from Commissioner Brill. Do you worry about what IoT will do to deepen the digital divide between those who can afford a wired home, a smart car, et cetera and those who cannot? How should society address these concerns? Or from your perspective, are costs issued really a matter of developing the correct investment horizon, short-term versus long-term?

MR. CERF: So my first reaction actually is I'm not too worried about that and let me try to explain why. It's not a cavalier answer.

Physics is really with us here. The costs of these things have been dropping on a regular basis. The cost of internet enabling things has gone down, the cost of access to service, the cost of devices themselves, have all been dropping. And that is, in fact, why we see an expanding number of users of these systems.

We will still have divides, but I think they will eventually close-up because the costs will tend to come down. Scaling helps in many respects. So my belief is that that won't be a problem, at least in terms of affordability.

MS. MITHAL: Okay, this is a question --

MR. CERF: That's the only question there was. Nobody had any other questions?

MS. MITHAL: I have a gazillion, but I'll just ask one.

MR. CERF: All right, go ahead.

MS. MITHAL: So I think every time we hear that there is a transformative technology taking place, we hear, well, privacy is dead. Get over it. Or we hear that the Fair Information Practice Principles somehow need to be modified or adapted and I just wondered what your views were on that subject.

MR. CERF: So I would not go so far as to simply baldly assert that privacy is dead, although Scott McNealy said that about 15 years ago and I think that was almost an exact quote.

But let me tell you that it will be increasingly difficult for us to achieve privacy. I want you to think for just a minute that privacy may actually be an anomaly. I don't know whether any of you have lived in small towns, but I lived in a little town in Germany of 3,000 people in 1962. The postmaster knew pretty much what everybody was doing because he saw all of the letters going back and forth. And oh, by the way, nobody had telephones at home, you had to go the post office and the postmaster would place the call for you and then send you to a booth to go and talk to whoever the called party was. And on top of that, in the town of 3,000 people, there is no privacy. Everybody knows what everybody is doing.

It's the industrial revolution and the growth of urban concentrations that led to a sense of anonymity, which in some ways leads us to believe that we have privacy because nobody knows who we are.

Now, I'm oversimplifying and I've done terrible damage to what I believe to be a very a fundamental concept of privacy, so I don't want you to go away thinking I'm that shallow about it, but I'd also like to observe that our social behavior also is quite damaging with regard to privacy.

The technology that we use today as far

outraced our social intuition, our headlights. To give you a simple example, let's imagine that you have gone to Egypt and you are standing in front of the Great Pyramid of Giza and you want a photograph of you standing there because you want to put that up on a website somewhere.

So you hand the camera to somebody you don't know and ask them to take a picture. Let's suppose that someone is nearby and is caught in the picture. We'll call this person Joe. You have no idea who Joe is and you don't care, all you want to do is to get the picture of you in front of the great pyramid on your website.

So you put it up on a website or Flickr or Your Tube or what have you. Somebody else is crawling around on the net, looking for pictures of the pyramids and finds this picture and recognizes Joe and tags Joe.

Somebody else is looking for pictures of Joe and discovers that one, except Joe said that he was in London. But that picture shows him in front of the pyramid on June 25th, 1970. Well, 2008. It wouldn't have been 1970, you're right.

So the point here is that Joe is now exposed as having mislead somebody because of a series of innocent-sounding actions. So I use this as kind of a metaphor for our need to develop social conventions that are more respectful of people's privacy. And I think we don't know how to specify that. I think that what happens is that we are going to live through situations where some people get embarrassed, some people end up going to jail, some other people have other problems, as a consequence of some of these experiences. And out of that may come some social practices that will be more respectful of privacy.

But I think this is something we are going to have to live through. I don't think that it is easy to dictate this. So that's where we are, I think, on the privacy question.

MS. MITHAL: Okay. A related question has come in, just a straight-forward question. Should the government seek to regulate security and privacy for Internet of Things, consumers and providers?

MR. CERF: Well, I have to tell you that regulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.

But I also want to argue that, while regulation might be helpful, that an awful lot of the problems that we experience with regard to privacy is a result of our own behavior. Which is not so much an illegality or something, or a violation in a typical regulatory sense, it is really just the fact that we didn't think about the potential hazard.

So before we run off to write regulations, I think we better understand a little more deeply what the risk factors are. I know that I have often wanted to build a congressional comic book that I could make available to our friends in Congress to help them understand, at literally a cartoon level, the way in which the internet works. Because without a reasonable understanding of that, it's hard to write laws, let alone develop regulations for them.

So I need a kind of lightweight, cartoon model which, used as a metaphor, would lead people to the correct understanding of what laws make sense. Otherwise, it is like saying, oh, this network doesn't run fast enough so why don't we just double the speed of light? And then you say, well, that's hard, so we can't do that. Actually, you can do that, believe it or not. The speed of light in an optical fiber is only 90,000 miles per second. If you get rid of the fiber, it will go 180,000 miles a second, so the way to double the speed of light is to get rid of the fiber and do it in an optical free space.

She says we are out of time and you have one more question.

MS. MITHAL: I'd love to do one more question. Why don't we do one more question?

MR. CERF: All right.

MS. MITHAL: So this is coming from more of an industry perspective. So how can industry best continue to innovate, while protecting against privacy and security concerns, not only in the U.S. and western countries, but the abuse of technologies under four regimes that value privacy of their citizens differently?

MR. CERF: So the comments that were made in the panel, and I wasn't here early enough to hear all of it, so I missed the presentations, but the comments about security and rules for who has access for what information and under what conditions, I think, is essential for dealing with that problem.

But it's really, really hard to make security work well, especially if you don't want to or don't believe that the users are going to be security experts and know how to do configuration and everything else.

So figuring out how to make a security system work well, which doesn't require you to be an expert, is a pretty big challenge. I believe we have to face that and try to do it. We really have to try to do it.

SSL, which we all understand can be broken and there is man-in-the-middle attacks and other sorts of things, but it's an example of something that is relatively invisible. You don't have to do something in order to make the exchange happen. So I'm not arguing that's the solution, but it's an example of something that didn't require very much user interaction in order to affect the key distribution. Those sorts of ideas, I think, are going to be important in order to make these systems acceptable in a social sense.

Well, thank you very much for allowing me to --

MS. MITHAL: Thank you.

(Whereupon, there was a recess for lunch.)

AFTERNOON SESSION

MS. JAGIELSKI: Okay, everybody. We are getting ready to start. Everybody take your seat.

I've been asked by the organizers of the event, which really isn't me, that everybody should move towards the middle of the seating and not crowd the aisle seats. I wouldn't, but that's what I've been told to tell you, so. But that's just me, that's just me.

We are going to start our afternoon session now. We have the great privilege of hearing some remarks by FTC Commissioner Maureen Ohlhausen.

MS. OHLHAUSEN: Thanks. Well, welcome everybody to the afternoon session. I am delighted to have the opportunity to set the stage this afternoon for this Internet of Things workshop. And given my particular focus on technology policy, I am very interested in the evolution of the internet.

From its start as basically a one-way conversation where websites provided information to users, to the rise of social media where users not only talk back to websites, but also talk between themselves and create rich conversations.

And now we are looking at the Internet of Things, where our phones and our appliances and our cars and an array of other items will be able to carry on conversations without us and really just fill us in as necessary.

And I believe that the Internet of Things has the potential to transform many fields, including home automation, medicine and transportation, as today's panelists have and will continue to discuss. These new capabilities will clearly offer great benefits to consumers in their day-to-day lives, but we must also be sensitive to the fact that the ability to collect large amounts of information and, in some cases, act on that information also raises important consumer privacy and data security issues, which is one of the topics that our last panel will address today.

So I'm very pleased that the FTC is holding this workshop to get a better understanding of how to achieve the benefits of the Internet of Things, while reducing risks to consumers' privacy.

I consider the Commission's interest in the Internet of Things to be another chapter in our work on consumer privacy and data security issues. It is a particularly interesting chapter to me, however, because it also draws together several hot issues in this space such as data security, mobile privacy, and big data.

On a more philosophical level, it also raises the question of what is the best approach for a government agency, like the FTC, to take with regard to technological and business innovation.

The success of the internet has, in large part, been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competition. It's thus vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, to understand its effects on consumers and the marketplace, to identify benefits as well as likely harms, and if harms do arise, to consider whether existing laws and regulations are sufficient to address them, before assuming that new laws are required.

For the FTC, I believe we can help ensure that the promise of innovations, like the Internet of Things, is realized by using our unique set of policy and enforcement tools. First and foremost, in a new technology or an industry that is rapidly innovating, we should use our policy R&D function to get a better understanding of the technology itself, the new business models it may enable, any existing regulatory structures, including any self-regulation, the market dynamics, and the nature and extent of likely consumer and competitive benefits and risks.

Second, we should use this learning to educate consumers and businesses on how to avoid or minimize any risks that we may identify. Providing consumer tips and suggesting best practices for businesses is one of the FTC's most valuable and cost-effective activities.

Now of course, the FTC is also an enforcement agency and it can, and should, use it's traditional deception and unfairness authority to stop consumer harms that may arise from particular internet connected devices. This not only helps consumers, but also benefits the companies involved in the Internet of Things by policing actors that may tarnish the technology itself.

Likewise, the FTC should use its flexible and fact-intensive approach to antitrust enforcement, to investigate and, where appropriate, challenge competitive harms occurring in the internet space.

For the remainder of my remarks, I will briefly touch on some specific issues, data security and mobile privacy and big data, that have particular relevance to the development of the Internet of Things.

As you know, the FTC, as part of its broad focus on consumer privacy, has an active data security program. The importance of this program will only continue to grow with the Internet of Things, which will sometimes involve the transmission of sensitive data, such as a consumer's health status, or private activities within the home.

You may have heard about a recent FTC case that exemplifies the kinds of data security risks that the Internet of Things may present. So in September, the FTC settled a case against TRENDnet, which sold its interconnected secure view cameras for purposes ranging from home security to baby monitoring.

Although the company claimed that the cameras were secure, they actually had faulty software that allowed unfettered, online viewing by anyone with the camera's internet address. As a result, hackers posted live-feeds of nearly 700 consumer cameras on the internet, showing activities such as babies asleep in their cribs and children playing in their homes.

The type of consumer harm that we saw in the TRENDnet case, surveillance in the home by unauthorized viewers, feeds concerns about the Internet of Things overall. It is thus crucial that companies offering these technologies take the necessary steps to safeguard the privacy of users to avoid giving the technology a bad name while it is still in its infancy.

Now turning to mobile. As we all know, mobile has been a highly disruptive technology that has brought great benefits to consumers and opportunities to businesses and the growth of mobile devices has been astronomical. According to the International Telecommunication Union, the number of mobile subscribers globally rose from 5.4 billion in 2010 to 6.8 billion at the end of 2012.

Mobile devices play an important role in the Internet of Things as they collect, analyze, and share information about users' actions and their environments. From their current location, travel patterns and speeds, to things like surrounding noise levels. This raises the question of how businesses should convey, on a small phone screen, information about what data, sometimes of a sensitive nature, that these devices and apps collect, use, and share.

The Commission has devoted significant resources to addressing the mobile phenomenon. In addition to setting up a dedicated mobile technology unit of tech-savvy folks, we have held workshops, issued reports, conducted research, and developed extensive consumer and business education materials.

The Commission has also been very active on the enforcement front in the mobile space. One case that has implications for the Internet of Things involved an app that collected information from consumers' address books on their mobile phones without the consumers' knowledge or consent.

The FTC settled a complaint against Path, a social networking company, for this activity as well as for alleged violations of the Children's Online Privacy Protection Act. As this case suggests, the collection of personal information from a consumer's mobile phone, without the disclosure or permission, may be deceptive -- may be a deceptive or unfair practice under the FTC Act.

This has obvious implications for other internet-connected devices that collect personal information about users and prudence suggests that such technology should include some way to notify users and obtain their permission.

Now turning finally to big data, according to some reports, 90 percent of the world's data has been generated over the past two years. And the amount of data in the world will only continue to increase with the volume and detail of information collected by new technologies, including the Internet of Things.

Although the ability to collect and analyze large data sets offers benefits in medical, scientific, economic, and other types of knowledge and research, as well as for business innovation, at the same time, the collection of large amounts of data about individual consumers may also raise privacy concerns.

In response to these concerns, the Commission recently began a formal study of the data broker industry. We sent out formal requests for information to nine large data brokers to learn more about their practices, including how they use, share, and secure consumer data. It is vital that we have a good understanding at how data brokers operate because appropriate uses of data can greatly benefit consumers through better services and convenience, while inappropriate use or insecure maintenance of data could cause significant harm to consumers. We will carefully analyze the submissions from the companies and use the information to decide how to proceed in this area.

So just to sum up, the internet has evolved, in one generation, from a network of electronically interlinked research facilities in the United States to one of the most dynamic forces in the global economy. In the process, reshaping entire industries and even changing the way we interact on a personal level.

The Internet of Things offers the promise of even greater things ahead for consumers and competition. The FTCs approach of doing policy R&D to get a good understanding of the technology, educating consumers and businesses about how to maximize its benefits and reduce its risks, and using our traditional enforcement tools to challenge any harms that do arise offers, in my opinion, the best approach.

This type of informed action will allow

free markets and technological innovation to serve the greatest good, while still maintaining a federal role in protecting consumers and ensuring a level playing field for competitors.

Thank you for your attention and I hope you enjoy this afternoon's panels.

PANEL TWO: Connected Health and Fitness

MS. HAN: So thanks everyone. I'm Cora Han and this is Kristen Anderson and we are going to be moderating this next panel up which is on connected health and fitness.

So today we are going to talk about devices ranging from smart pillboxes to connected glucose monitors to wearable devices that allow people to compare their exercise regimens with those of their friends.

As many other folks have mentioned here today, these devices have the significant potential to improve people's lives and also reduce costs. To give just one example that you may have seen in our rotating slides, according to a recent study, patients using a mobile pillbox app that informs friends, families, and caretakers about the patient's pill use reportedly took their medication on time at a rate 31 percent higher than the World Health Organization's estimated average for patients, which is 50 percent.

But these devices also raise serious privacy and security concerns and we are going to dig into those in depth today, as well as what some of the privacy and security consumer protections should be.

So before we get started, we wanted to actually raise one of the issues, which makes this area a little bit unique and that's the regulatory landscape. As many of you are aware, the FTC has the authority to enforce against connected device manufacturers, app developers and others who may be engaging in unfair or deceptive acts or practices.

But there are other regulators in the space as well, like FDA and HHS, who also may play a role in protecting the privacy and security of health data.

So for example, the FDA recently issued draft guidance regarding the management of cyber security in medical devices. The Health Insurance Portability and Accountability Act, or HIPAA Privacy and Security Rules, may also come into play if the device or app creates, transmits, or stores protected health information as part of the information system of the covered entity, such as a physician or hospital or insurance company or one of their contractors.

So for example, if a consumer is using an app on their tablet or phone that tracks their blood pressure levels, this would not necessarily be PHI protected by HIPAA. But on the other hand, if the physician directed the consumer to send this information from the consumer's device back to the physician, then HIPAA privacy and security rules might apply and might require that appropriate safeguards be in place to protect that information.

So while we are really going to focus today on consumer facing devices, from the perspective of the FTC, some of the other panelists may raise -- and it is important to remember that there are other regulators in this space as well.

And so with that, I would like to introduce our panelists and have them spend a few minutes giving you some background about themselves before we get into the discussion.

MS. ANDERSON: Okay, so first we will hear from Scott Peppet. Scott is a professor at the University of Colorado Law School and has written recently about the privacy implications of sensors and other technologies that permit easy self-disclosure and the sharing of information.

MR. PEPPET: Hi and thank you to the facilitators for inviting me onto the panel. This has been great already today. I am going to talk really, really fast because we don't have much time.

But I want to just start by saying I love these sorts of devices. I have a wi-fi connected blood pressure cuff and a Fitbit and I have little waterbugs in my basement that tell me when there is flooding. And I live in Boulder, so that's a very useful thing. And I think there is a great need for a lot more innovation in this space, as much as there has already been innovation in this space.

I write about the effect of technology on markets and, in this health space in particular, in the fitness area, there has just been unbelievable change over the last few years in a bunch of different categories. Countertop devices, wearable devices, what are called intimate contact devices, which are like little stickers or patches that you wear that can monitor things like your temperature or other aspects of your health, adjustables, implantables. All of these different categories of health devices have been moving really, really rapidly.

That said, I want to say a couple of things about privacy and security in particular, kind of tying back to this morning's panel. The first is, as Jeff Hagins said this morning about home devices, these devices still are really siloed and certainly far from perfect. If you've used any of them, you realize that it is not one big seamless cloud of data that tells you everything about yourself, yet.

There are huge gaps between what the -- that prevent the devices from talking to each other. There is also a huge variance in the ways these things are structured. If you read, for example, as I did this summer, the privacy policies of the top 30 health or fitness devices, you see a lot of difference in the way they are owning the data or letting their consumers own the data, what they are saying about sharing the data, et cetera.

And the first point I want to make is this is not just an accident of it being early in the evolution of the Internet of Things. It is, in part, because these companies have not yet all figured out what their business model is. And as they try to figure out what their business model is, some of them think their business model is selling little armbands that you wear around your wrist, but they are not missing the reality that it is really the data that is probably the most valuable. And they are trying to figure out how they are going to use that data.

In the internet space, obviously, we've mostly focused -- most workshops like this have been focusing on behavioral advertising because the model to fuel growth has been behavioral advertising.

In wearables and what we've seen so far in devices like Fitbit and others, that is not the main topic of conversation at the moment. Where are they heading with the data? They are heading in a different direction largely, although I'm sure advertising will also play a role, they are heading towards really core economics or economic functions. Things like credit worthiness, insurance, employability, and the revelation of consumer preferences.

Why? Because these data coming off of sensors are incredibly high quality. I can paint an incredibly detailed and rich picture of who you are based on your Fitbit data or any of this other fitness and health data. And that data is so high quality that I can do things like price insurance premiums or I could probably evaluate your credit score incredibly accurately. The data are going to move towards those economic purposes because they are so useful for that.

So the first thing I want to say is,

number one, we don't have a business model and number two, we can -- one basic principle I think we have to wrestle with is, at some level here, everything reveals everything. And that's what sensors are really -- that's the real challenge of sensors, right? So we can talk about health sensors and say, well, they are really interesting in revealing health. But I can tell whether you are a good credit risk based on your health sensor and I can similarly tell that from how you drive your car and I can probably tell it from whether you leave the stove on at home too often when you go out. These silos of different kinds of sensors don't really work, in the sense that the data will flow, to the extent the law lets it, across the silos.

The second thing I want to say is it is incredibly hard to anonymize any of these sensors' data. I'm not going to argue about that or say too much about it, but I think it is worth focusing on a little bit. Sensor data demonstrate what's called sparsity. It is just very unlikely that you and I have similar Fitbit data coming off of our Fitbits. Why? Because I move completely differently than you do. Ira Hunt, who is the CIO of the CIA said you can be 100 percent identified, as an individual, by your Fitbit data. Why? Because no two persons' gaits or ways of moving are the same. We can almost always figure out who you are based on that kind of incredibly rich detail. Similarly, if you want to read a great study, read the MIT mobile phone study from last year called, "Unique in the Crowd" that talks a lot about sparsity of sensor data. So that's a second aspect of sensors on the Internet of Things that I think we need to talk about.

And the last thing I'll say, just in terms of privacy and security, is just in terms of how poor notice and choice does here. I spent, again, a lot of time this summer looking at privacy policies. It's really odd. I bought a whole bunch of different health sensors, all the different ones we'll probably talk about, and just went through the consumer experience of opening the box.

As a law professor, I went opening the box looking for the privacy policies. I didn't find any of them. They're not in there. They are not in the user guide. You can get the thing on your wrist, and now it's not doing much yet, because it's not hooked up to the website that it's meant to talk to, but even when you sign up for the website it is just striking, when you go through the consumer experience, how not salient it is that you are now about to generate a massive amount of new, incredibly high value data that you've never seen before.

Am I done? I'm done. Thanks.

MS. ANDERSON: Next we'll hear from Stan Crosley. Stan is the Director of the Indiana University Center for Law, Ethics, and Applied Research in Health Information, counsel to Drinker, Biddle, and Reath, and a principal in Crosley Law Offices.

MS. CROSLEY: Thank you. I'm just going to stay right here. I'm a little worried that the CIA will see who I am by the way I walk to the podium. Actually, that also brought up the reference to Monty Python, silly walk. Remember that? It's such a great reference.

So for those of you who actually came to listen to this talk, Indiana University CLEAR is a joint venture between the schools of law, informatics, and medicine at IU and we are really interested in addressing a need at the intersection of health and data. A kind of cross of the healthcare ecosystem, if you will, so privacy, security, ethics, and risk in those assessments and understanding the appropriate use of barriers to the appropriate use of data.

We also believe that this is a timely panel, this is a timely topic. It has always been true that more is known about your product or your service outside of the walls of your entity than inside. And if you think about it, you know, GM makes cars and GE makes refrigerators and the consumers who use those goods certainly know more about whether that product is working for them than GM or GE would. And so it's always been the case.

And it's the case in healthcare as well, as a device or pharma or another company, you know, when consumers are taking your product, you don't have a good closed-loop feedback system. More is known about your products and whether it works or not outside of the walls of your company than in.

We've invented ways, over the decades, to try to figure that out. You know, interventional clinical trials, observational studies, safety data that comes back, and then sales. Sales is a proxy for whether or nota product is good or not. But those are imperfect closed-loop systems, right?

So then enter into now the Internet of Things. And now we have, for the first time, the potential to have a real closed-loop system. And if you think about it as a company, you know, you are faced with looking out at a consumer population or a patient population that is starting to aggregate that knowledge source. Your ability to innovate has relied on the fact that your knowledge is concentrated, the knowledge -- the research that you did to create the products, that's a concentrated knowledge source and you use that, you mine that, you understand it, you assess it. But now that data is getting aggregated outside of the walls of the company, outside of the walls of your entity, outside of the doctor's office.

And so how do you, as an entity try and close that loop to understand what they know? How do you get access to that information? What's the appropriate use that we can make of this information?

You know, if you look at this, 37 billion dollars has been earmarked for data that is created inside the walls of traditional healthcare. But we believe that far more about health has been generated outside the walls of traditional healthcare than inside and zero dollars has been earmarked for understanding this. It is the goodness of the FTC to convene these panels to try to help us understand what these issues are.

So the entities that are playing in this space have a huge responsibility to try to figure this out. And to the entities I've talked to across this space, they are all very interested in understanding what is the appropriate use of information. How do we engage consumers that don't want to be engaged? Let's face it. We've all gone to the doctor's office, we've all gotten the HIPAA notice which, if you get it actually, that's a step up. Really you get to sign the little chart that says, please sign here indicating you've gotten the HIPAA notice.

And if you actually ask for one, they have to scramble a little bit, find it and give it to you. And if you read it, you'll be one of the few who ever has. And then when you hand it back to them, they either throw it in the trash or they put it back on the file for the next person who wants to see it the next month. That's no way to do notice and consent. It's no way to have an informed consumer and an informed public.

And so companies and entities are interested in trying to figure out this gap. How do you close this gap, between the knowledge that you need to innovate, the knowledge to take care of patients, and yet relying on some type of an artifact that exists for notice when the world was a much simpler place and far less connected.

I think that's where we are all headed. We have to figure this issue out. And so we are, in fact, interested in figuring out what is the appropriate use, the appropriate sharing of information in this Internet of Things, in this connected world, where data will be more impactful. Because we are not just talking about big data. Big data is going to have a huge impact in health care, likely on the back end with the identification of biomarkers or other things like that, but small, daily digital daily, that is where the strides are going to be made in healthcare and that is where the potential is. And that is what we all have to figure out.

MS. ANDERSON: Thank you, Stan. Next up we have Joseph Lorenzo Hall. Joe is the chief technologist at the Center for Democracy and Technology where he focuses on the nexus of technology, law, and policy.

MR. HALL: Thanks a lot. I want to thank

the FTC for having this workshop and for inviting us up here.

The Internet of Things brings granular commercial surveillance into the home. And commercial surveillance, we've seen on the online marketplace quite a bit, but increasingly in retail, physical establishments as well. The capacity here for unintuitive inference, that means ways that people can tell things about you without you being able to figure that out on your own, is really enormous for these kinds of applications.

And as we know, there can be amazing benefits, but at the same time, there is a potential for some serious harm, especially in telehealth and health applications. I consider that sort of the canary in the coalmine for the Internet of Things. If bad things start happening with telehealth and health applications, you are going to see that sort of poison the well, so to speak, for a whole lot of additional kinds of connected applications.

The Privacy Rights Clearinghouse earlier this year did a really neat study of something like 43 apps, 43 health and wellness apps. The sample was constructed relatively well, but anyway, the findings from that were pretty eye-opening to a lot of us.

Some things you would expect, for example, free apps tend to have more advertising. That is not something that is too surprising. But analytics is used by most apps, and in some cases multiple forms of analytics, in some cases ten or so individual analytics companies are seeing some of this granular information, these things that are collected.

They also found that only half of apps that share personal information do so, they share this stuff, in an encrypted manner. So the other half are not encrypting that stuff.

Many send data to third parties, data used for core health functionality of these apps. And they do that, in all cases, over unencrypted connections, they found. And no apps in their sample stored data locally, that's 83 percent of their apps, store data locally. None of them encrypted stuff locally on the device. Half of them had privacy policies and of the half that had privacy policies -- wait. Half of them had privacy policies and only half of those were actually technically accurate as to what they were doing with the data.

So this is an enormous gap in terms of where we have to get to. We have to find a way to bring the market up to the case where we are encrypting things, where we are doing what we say we are doing in privacy policies.

And I would say also, increasingly more end-to-end, especially in health, forms of encryption. So not relying on infrastructural things like SSL and file system encryption, and this gets technical, but ways that only the provider and the patient can actually see that data. Which means you may not be able to monetize in the middle, but there are ways to do stuff on the client side. We've got to recognize there are ways to monetize on the client side without ever seeing this stuff.

And one of the big problems here is a lot of consumer-facing health applications aren't governed by HIPAA. They are not something provided by a covered entity, they are not a PHR, they are not a personal health record, so they may not have to deal with the breach notification rules. They may at the state level, but not the ones that are now in HIPAA via HITECH.

And consumers should be able to do whatever they want with the data. They should be able to share it, they should be able to do willy-nilly things they want. The trick is, the gap between what apps do that help you manage this stuff, that the Privacy Rights Clearinghouse study exposed -- and others, there is other great academic computer science studies along these lines. And that gap is pretty substantial.

And it's clear that we think that there should be some baseline consumer legislation in the U.S. that applies to all personal data, we've said that for many, many years. Not a big surprise. That may not happen soon enough for something like telehealth, to really sort of give us the promise that we would like to see from these kinds of applications.

And so what we are sort of arguing is that the FTC should be given some limited authority in telehealth to regulate. For example, convening a multi-stakeholder group to build a code of conduct, with the incentive being the FTC gets to anoint it as being sufficiently consumer protective and innovative, the promoting of innovation, and then you get the safe harbor from FTC Section 5 enforcement.

The cool thing about our proposal also is that if you can't get people together to make this code of conduct in a sufficient amount of time, maybe like a year, the FTC should have authority to actually write some baseline privacy and security guidelines or rules or something like that.

I'm almost out of time. Anyway, we really think that telehealth is sort of the canary in the coalmine and we should be doing better, the market should be doing better and the FTC definitely has a place to play in helping that.

Thank you.

MS. ANDERSON: Thank you, Joe. Next up, we have Jay Radcliffe. Jay is a senior security analyst for InGuardians and has been working in the computer security field for over 12 years.

MR. RADCLIFFE: So I am a unique member of the panel in that, you've heard today a lot about the great things that we can do with connected devices and the Internet of Things, but you've also heard the potential for the monster being under the bed or the boogie man being in the closet.

My role in the community is I go in and drag the monster out of the bed and show you what he looks like. For the past 20 years, I have been at the front lines of computer security. I started out life as doing email security, and then website security and then finance, but unfortunate for me is that I was diagnosed with type I diabetes at my 22nd birthday. And I have been attached to various medical devices for various amounts of time.

In 2011, I did a presentation at Black Hat where I was able to remotely turn my pump off with my computer. And I was able to change every therapy setting and every setting on that device and make it look like this, which is a pump that does not deliver medicine anymore.

This year, I did the same thing to the pump that replaced this pump from another company. Both companies are very large companies and the issues that I showed this year brought me to almost go to the hospital two times due to problems with connected devices due to software failures and design failures.

These things are not theoretical, these things are real. These things are happening right now, they are happening to devices that you are buying. And it's not something that is publicly well-known. It is not something that consumers are very well-knowledged about. Consumers can't make good decisions because the information they are getting is incomplete. And often times not in a malicious way, but in a way that it hasn't been researched yet. This is really new, cutting edge stuff and it's scary. It is scary to see these devices that we depend upon to keep our children alive, to keep our grandparents alive, to keep our neighbors alive, not working the way we thought they would. Having unintentional consequences from the way they are connected and putting computers in our lives to control our health, to monitor our health.

These features are the things that I end up working on now instead of the internet. I don't secure your website. I don't secure your email anymore. Now I'm securing that meter that they put on the side of your house that has an LCD display on it and tells the power company how much power you are using all the time. It's the device that's attached to my hip right now that tells me my blood glucose value over the last 24 hours. It's the Fitbit that I wear to make sure that I'm doing exercise in order to keep my diabetes in check.

These are all things that I'm actively researching and that people in my field are researching to make sure that we are taking the monster out of the bed. To taking the boogie man and seeing if he is even in there. But if he is, what can we do about it?

And I'm proud to be on the panel here with the FTC because they are looking to do something about it. You know, since 2011, I have struggled to find regulatory agencies that can affect change. Initially when I went to the FDA, they said, I don't know what we should do about this. Probably something.

Two senators ordered the GAO to do an investigation. And what they found was that no regulatory agency was looking at the security of these devices. The FCC said, that's not us. The FCC looks at the way the radio transmits, not what is being transmitted. And the FDA said, it's not us. We look at how the medical part of it works. And it turns out that there is this huge gap, that nobody is looking at the security of these devices from a cyber security perspective, from a connected device perspective.

And that report has prompted a lot of change in the FDA, in different regulatory agencies, in spurring them to look at those events and to look at those things and how we can make the world a safer place, before somebody gets really physically hurt or potentially dies from a connected device failure.

So those are the things I work on. Those are the type of insights that I hope to bring to the FTC, bring to different policy panels to help them get the perspective that they need of what actually is occurring on the ground.

Thank you.

MS. ANDERSON: And finally we have Anand Iyer. Anand is President and Chief Operating Officer of WellDoc Communications, Incorporated, where he oversees the company's mobile and web-based chronic disease management platform and its integration into mainstream health management programs.

MR. IYER: Thanks, guys. I'm going to continue in that same vein of starting to take this discussion, not just about the denominator, which is all about what we need to do from a privacy, security, et cetera perspective, but the numerator, which is really the value proposition.

WellDoc is a company that was founded by an endocrinologist back in 2005. This was before the iPhone existed. It's a concept before the word app was part of our vernacular. And it was born from a simple observation that patients who came into the clinic -- I'm a Type 2 patient myself, I've had diabetes for the last 12 years. You try your best to manage this disease, as Jay knows, you try your best. You do what you have to do with your glucose, your meds, your sleeping, stress, smoking, diet, exercise, everything that is the 360 of diabetes, but there is this little thing called life that gets in the way every now and then and prevents you from doing what you need to do.

At the same time, I consider myself -- you know, I did all my doctorate work in pattern recognition, so I'm a little bit of a data junky, is the honest truth. I would take my stuff in to my doctor and not just give it to him, I'd graph it. Because I'm a little bit of a nerd.

But what's a doctor going to do in the three minute office visit? They don't have the time. The frontline is primary care. They don't know what to do. Because you're not just there for your blood glucose, you're there because you have H1N1 and you have this bump and scratch and itch and, oh, by the way, how's your blood glucose. It's like flossing the day before you go see the dentist, right? You're never as good as the day you see your doctor.

So we asked a simple question. Could we actually convert that lapse, if you would, in not just the data, but the information, knowledge, and action that ensues from that data? And could we do three things. One, could we actually put a piece of software on a patient's cellphone? And this is a good old Nokia 6600 but it still works on those dumb phones, not just smart phones.

So could you use that to actually coach the patient in real time what to do, give them instructions? If they are at a restaurant, they enter their blood glucose and it's high, we tell them how to drop it. Because how I drop it and how Jay drops it are two different things because he's got a different set of comorbidities, I've got a different set of comorbidities. He's on different meds, I'm on different meds. So it's personalized, to a certain extent.

Secondly, can you take all of that data and could you run it through evidence-based medicine and could you show patterns? Could you look for trends, whether they are exercise trends or smoking trends or eating trends? -- that's actually my phone ringing. Very cool.

And then the last thing is, could you give to a doctor, say in a manner that they wanted, once every three months or whenever they want it, really, in the format that they chose, hey, here's where the patient was, here's where they are today. Here's what's changed and here's what you ought to do, but against evidence-based guidelines, but you do what you think is right. You're the expert, it's your patient.

When we did our first clinical trial we dropped A1Cs in diabetes by two points. Just so you know what that means in English, A1C is the average amount of sugar in your blood, for all intents and purposes. The guideline by the ADA is 7 percent, which means 7 percent of your blood volume is sugar. Every one point delta, seven to eight, eight to nine, represents a 43 percent increase in the risk of heart attack, stroke, kidney failure, blindness, amputation, the five big things that diabetes causes.

The FDA heralds a drug if it drops A1C by 0.5 of a point. Look at Januvia, Merck's blockbuster drug, I'm on it, it's a good drug, it drops it by 0.7 of a point. So when they saw a two point reduction, they are like, what the hell are they doing? Swallowing the phone? We said no, they are doing what their doctor has told them to do.

Doctors who received that analysis were five times more likely to make a med change or titrate a medication. So we saw, in a quick swath, with that comes about a 390 to 630 dollar per patient per month cost savings.

So now you say, okay, with that value proposition in the numerator, what do I need to do to ensure privacy, security. And we'll talk about security and when people talk about data security, it's not just about data, it is about the application, the infrastructure, it's about everything in between, it's the full securing or the value chain.

So let me show you, because Cora wanted me to show you how this works, so I'll just give you a quick -- I'll just give you a quick -- good, that's keeping up with me.

So if I go in now and I just make a -- what would an application be in the FTC if it wasn't password protected, so I'm going to put in the password. Here we go, it's now on. Very good.

So if I go in and I actually make a new entry, there's about a two second lag between what I see and what you see, but hopefully it will work.

Let's say I go in and I enter a low blood glucose because I'm feeling shaky or whatever and if I have a pump, that data comes directly into this device, into this software. So let's say I enter 65, it will actually tell me, because we are a Class II regulated FDA device, the FDA considers our software to be a Class II medical device, it says it's low.

And they said, well, you manually entered it, so you better check whether it is true or not, because it's not coming directly from the machine. So they want truth, right? So yep, it's low. So then it says you follow the 15/15 tip. You know, it's the teachable moment. Hey, this is a common way to treat this condition.

It then gives me examples, right at my fingertips, of what I can actually consume and take which is, you know, great because you always don't know what to do.

And it starts a timer and even if the patient shuts the phone off, it will turn the phone back on and remind them in 15 minutes, hey, it's time to recheck. And at that point in time, if I go in and recheck -- I'll save you the 15 minutes, because I don't have it. Let's say I put in a good number, which is 108, it will tell me, hey, you know, great. You get an A+, blah, blah, blah, blah, blah, because it's all about behavior modification and support and making sure that you work with the patient.

Some patients told us, if you give me one more "Way to go!" message I'll throw the bloody phone away. But the next patient says no, I'd like to see a picture of my grandchild when I have a good reading because that's what keeps me motivated. So you get an idea of how it works.

Last thing I'll say is that it is an FDA cleared Class II medical device, but now, for the first time in history, anywhere in the world, we have a prescription code for this. We actually have an NDC drug code for this software. So for the first time, a doctor can prescribe software to their patient, which brings the patient provider, and we'll talk about what that means in terms of security and HIPAA and what not, but this is now a prescribed entity that comes from the doctor, to the patient, with these outcomes.

So that's it.

MS. HAN: Thanks, Anand. Let's get the

discussion started. First, to set the stage, I just want to raise this for all the panelists. How have we seen the marketplace evolve in the past few years, in terms of the products available and their impact on consumers?

MR. RADCLIFFE: All right, I'll go first. As a patient, I'm very keen -- as a diabetic, diabetes is one of the frontrunners of connective devices. Because patients have a lot of control over their disease. It's very interactive, just like he demonstrated. You're doing the medication and testing all the time. I mean, we all know somebody who pricks their finger and tests their blood, you know, be it a family member or friend.

So these devices are coming out. In the last four years, you know, there's been a wealth of devices to really help diabetics and applications, like he demonstrated, to help diabetics do these types of events to help their blood sugars.

And like the studies have shown tremendous amounts of value in that. So it's a very, very good thing, you know. So I'm seeing a lot of things from that perspective.

MR. PEPPET: I'll jump in. I would say one thing over the last five years, you know, on the one hand you had really serious medical devices that, you know, were being developed. On the other hand, you have consumer devices. We've obviously seen consumer devices explode, but they start off as being fairly light in terms of what they could do. So a pedometer, a fancy pedometer, a slightly fancier pedometer. There's been a fairly big gap, even over the last couple of years, between the medical devices on the one hand and the consumer devices on the other. That seems to be narrowing.

You know, you increasingly have consumer devices. I'm thinking, for example, there's a new device called the Scanadu Scout and it's meant to be a consumer device, you hold it up to your forehead for a second, or your kid's forehead, but it is measuring things like heart rate, temperature, respiratory rate, stress levels. A bunch of things that a home, you know, home little digital device couldn't do a year ago.

They're coming out with a Scanadu urinalysis device for home. So you know, you might think to yourself, that's weird, I don't want to do that, but what's happening -- you might want to do it, or you might want to have your kid do it, but what's happening is that that gap is starting to narrow, which is really cool.

You're seeing lots of folks trying to come out with creative places to put sensors or ways to use sensors. So my favorite example is there's now a bra that has a temperature sensor in it. Why would you want to do that? Because it turns out one of the earliest ways to detect breast cancer is very, very slight changes in temperature. So they are playing around with, well, you know, would this work? Answer: Yes, it does seem to work.

So there's a lot of innovation in that consumer health, medical space that is getting attention.

MR. HALL: And reducing the gap even further, in 2014, you are going to see a lot of providers responding to the incentives that are part of what is called the Meaningful Use Program, where patients are going to be able to view, download, and transmit their medical records wherever the heck they want.

And so you're going to see -- and you already see some of these, a ton of really neat apps that compute directly on your medical records. And there's a bunch of companies that are doing this, that are doing it in really neat ways, but I think that is going to further bridge the gap to where all of the sudden you have data on your phone that can be your entire life's medical history. That is undoubtedly sensitive and could be, in addition to being potentially harmful or life-threatening in a physical sense, there is a whole set of -- you know, medical identity theft is a really horrible form of identify theft. And these kinds of data can be used to do exactly that.

MR. IYER: Let me give you just one last thought. And I'll be the controversial one. So I agree with everything that has been said, by the way, but here is where the controversy is and that is, we are seeing an immense amount of innovation from a usability side and user experience.

Things that the gaming industry, entertainment industry, financial services, I mean, you pick up a gaming app and they are fun to use. You pick up a medical device and you throw it away. That's why medication adherence and things like that are where they're at today. I mean, these devices are -- I mean, as a patient, I've got to use them, but if you were to stack their usability against best in class practices for usability whether it's software or hardware, they fail. Miserably. Not just fail, they are bottom of the stack.

And so now the question that all consumers -- because at the end of the day, inside the patient is a person. And everybody talks about the patient, they don't talk about the person. And inside that person, they want to use things the way they want to use things. And why can't I have my data come from Facebook? Why can't I share my -- where do you decrypt the data, FDA asked us? Well, well, wait a minute. You want to send that data and export it to Twitter and Facebook? Where are you decrypting the data?

So we said, okay. We won't do that just yet, because society isn't there yet, you guys aren't there yet, and we're not there yet because we haven't figured it out, but I think that's where we are going to have a huge -- I think, first, you know, clash, is the honest truth. But I think out of that clash is going to come new value. And out of that clash is going to come new ways.

Society is changing, in terms of what they view fundamental privacy as. If somebody wants to know that I'm on Metformin and Januvia, I don't care. Because if I can find 30 other patients that are like me, and I know how they are treating their diabetes and it's working for them, I want to know what they are doing because that's going to help me. So the question is, where do you draw this line then?

And what we are seeing is we are seeing the clash in these innovations, where one is coming at it from a pure usability standpoint and one is coming at it from a regulatory standard, privacy, encryption, you know, AES, blah, blah, blah, and the two are coming together and I think that's where the next five years is going to be -- and where I think the next big step in innovation and value is going to be created.

MS. ANDERSON: Just following up on that Anand, and any of the other of you, if you have any input on this, when consumers do choose to share their data and experiences with others, via social media or in some other way, how does that affect privacy overall?

MR. RADCLIFFE: It eliminates it. It's a -- I get this question all the time. Why can't I make my kid's insulin pump talk to the iPhone and tweet out his values? Well, because I don't want the world knowing what your kid's blood sugar is, that's why.

You know, we had this discussion in our discussion with the panelists before today, which was that there is this element of privacy that you end up -- it's not that privacy has to be pure and that everybody gets 100 percent privacy, but consumers need to be able to make a choice, right? You know you are giving up a piece of your privacy in order to get something else. It's not a zero sum game.

So like he said, he is willing to give up some of his privacy. You can know some of my medical conditions. But if I share that, then I can get something out of it. It's not a question -- and I think that's something that's really important from an FTC perspective is, consumers need to have the information and make the best choice they can. If they believe they have 100 percent privacy, but they can still get all of those things, then they are going to make a bad choice, because they don't know they are giving up that privacy. I think that's something that's really important.

Consumers are willing to give up some of their privacy. We do it all the time when we post where we're at on Facebook, but it helps us. It helps us identify who are friends around in the area and what you're doing and all those things.

So it's something that we're going to have to retrain our mind to how we think about those things, because sometimes it's going to be okay.

MR. CROSLEY: I think this is where you're also getting into the benefits. And I'll take a somewhat contrarian position, but I mean the idea of patient engagement is actually one of the most significant benefits that we have from this connected world.

And the ability to, you know, draw the patients in and engage them in their own care, give them real-time data or sense data or feedback on information from their insulin pumps or their implanted cardiac devices, things like that, is where we are going to have to go next, to pull them in and engage them in that world.

And you're right. There will be the giving of some privacy in that world. You know, security is still the table stakes and I think that -- Jay, you said that at the beginning. I mean, we've got to have security here so that when the sharing is done, it's done with full knowledge and understanding.

But the engaging the patient is clearly, you know, the next frontier. And the devices and the sensors now are going to make it possible to actually engage the patient in some real-time decision-making.

MS. HAN: So Jay, you raise the issue of consumer understanding. I wanted to follow up on that. How much do you think, and this is to all of the panelists, how much do you think consumers who use these devices really understand about what's happening with their information and how it is being used and shared? And does your answer change depending on whether it's a medical device or a more casual wearable fitness device?

MR. HALL: Well, I certainly think that people -- it's very hard to know, even if you're an expert, even if you know how to jailbreak a phone and put a man-in-the-middle proxy to see what's going on, it's very hard to know what any of these apps are doing.

And there's great -- computer science research, for example, Yuvraj Agarwal at CMU has something called "ProtectMyPrivacy" and come ask me if you need a pointer to it, where they've found a number of cases where apps were doing things that the apps didn't even know they were doing. Because they were including like four or five ad libraries that were then going and computing on your contact information and throwing that up.

And I'm certain that that's happening in health, too. Not because of ignorance or willful ignorance or anything like that, but these things can be so easily complex, complex and so easily so, that you end up having a whole set of things that maybe the app developer doesn't even know what's happening.

And that's why it would be nice if there was some mechanism for teaching users and app developers, look, this is where your stuff is going. I know the NTIA Mobile App Transparency Code of Conduct effort made a valiant effort at getting to, you know, a set of screens that mobile app makers would have to show, at some point, that here's what we collect, here's who we share data with.

And I think those kinds of things, to the extent that we can test them, to make sure people know what they're doing, rather than the familiar refrain of, oh, privacy policy means my privacy is protected. No, it means they are trying to explain to you what they do to protect your privacy.

MS. HAN: Scott?

MR. PEPPET: I mean, I think the real answer is we don't know what consumers know and what they don't know about a lot of these devices because there has been very little, so far, to try to find out, although there are some studies.

But I do have some concerns. I mean, my biggest concern is I don't think that consumers have really figured out yet the kinds of inferences that can be drawn from disparate kinds of data.

So for example, one study at the University of Washington showed that consumers were very concerned about location data, about GPS data. They didn't like the idea that they were going to be continuously monitored for location, but they had essentially no concern about 24/7 recording of accelerometer data in the UbiFit health sensor they were wearing.

Well, it turns out if you have 24/7 accelerometer data, you can figure out where someone is pretty easily because if you are driving down the road with an accelerometer, each road on the planet is essentially unique in the accelerometer, in the way it triggers your accelerometer's readings.

So there's just this disconnect, right? They are saying one kind of data I'm really worried about, one kind of data I'm not worried about at all, and yet those two kinds of data support essentially the same inferences. I think we are going to see that increasingly across different kinds of sensors, including health sensors.

MR. RADCLIFFE: I mean to me, the question about consumers and their privacy, I actually think you need to -- I agree with Joe in that's almost a question you need to go a higher level up. The companies producing these devices don't even know what the privacy issues are.

You know, the implications of what they're recording and how it can be used -- and the example I'll give is I'm working with a customer that uses medical devices and he's like, what about connecting the medical device to the car, over Bluetooth? And I'm like, okay, what are you thinking? And he's like, well, it would be really helpful because you could see your medical stats, you know, like while you're driving. You won't have to look down for them.

And I said, "okay." And I'm like -- I'm thinking, you could also do other things. And you're going to hear on the next panel about all the crazy things that are being done with my research skills with cars. So if your blood glucose gets too low, why not just turn the car off? What if I surreptitiously told the car that your blood sugar was low? And he went, never mind.

So you know, thinking through some of these things, thinking through the privacy and security measures, consumers want everything to be connected and companies want to give their consumers and their customers everything that they want, but that's not what we need to do, you know? And then we need to take a second and think about the implications of that, from a security perspective, from a privacy perspective. We can't just connect everything to everything and everything will be great. We have to think about how these things are going to play out and how they are going to be used, you know?

So it's a very good question. We are going really, really fast, from a technology perspective, and just now we are starting to see some of the danger of things for a medical device, for a car. And now we want to mix these things together? Maybe not a great idea.

MR. IYER: So I'll share with you kind of our last six years of observation of several thousands of patients and kind of, for me, the answer lies in, it's an evolution. And it's an evolution that involves transparency and it's an evolution that involves education for the customer.

And the customer could be the health plan, it could be the doctor, it could be the patient, it could be a caregiver, it could be anybody who is a stakeholder.

So if you look at data and you look at two dimensions of data, there is one dimension of the actual presence or absence of data, so presence and absence, and then this vertical dimension is, I know my analysis intent and I don't. So just play out those four quadrants.

The bottom quadrant says, I have data and I know what I'm looking for. That's what we call informative, that's basic 101. Patients want to know that stuff. Hey, show me how many times I was in range, show me how many times I was out of range, show me how many times I skipped my meds. Those are the things they know you're capturing and they know you are going to report on because it's fundamental, it's 101.

Now go to the right. I know my analysis intent, but I don't have the data. We call that discovery. It's the realm of predictive modeling, for all of the mathematicians in the crowd, it's, you know, Bayesian, Markov, that kind of stuff, okay?

And the value proposition there is, I'd like to be able to tell a patient next week, to the nearest day and the nearest hour, when they are going to go hypoglycemic. Why? The biggest cost of hospitalization in the United States today with type 2 diabetes is unnecessary hospitalizations due to hypoglycemia. And if I can actually predict that -- for those of you who follow WellDoc, we had a press announcement last week where we actually published a paper where I can predict it now to 93 percent, which is pretty damn good. It's better than not knowing at all, right?

And so that descriptive says, okay, you don't have the data but you are going to tell me something of value to me. Some people may find that valuable, some people may say, you know what, I don't need to know that. Okay, that's fine.

Play this quadrant out. This quadrant says, I have data but I have no idea what I'm looking for. Do you know how many patients we found in our last six years who were on Byetta. Byetta is an injectable drug, you've got to take it -- but it only works when you eat.

So the doctor writes a prescription, take it at breakfast and dinner. So the patient is religiously taking their Byetta at breakfast, but they are a breakfast skipper. Because they put into the system, I skipped my breakfast.

So doctors wondered, why the hell is this drug not working on this patient? It should. Well, let me put you on something else. Meanwhile, the third day this happens, the system wakes up and says, hmm, rule. Taking Byetta but not recording their carbs? Did you know now that Byetta only works when you eat? Talk to your doctor about switching.

Doctor says, well, I wrote the prescription "At breakfast and dinner" and I meant with breakfast and dinner. There's 18,000 articles in the last ten years written about patient/physician discordance. So that quadrant of data says, you should use that data to catch -- all of the sudden, the patients are taking their Byetta and it's working. Huh.

Fraud, abuse, and waste? Think of what the value proposition is to CMS and the Medicare population for that.

And of course, the last one is adaptive. You don't have the data and you don't know what you're looking for, but you collect it over time. And I think it's an evolution. And for all intents and purposes today, we are still in that bottom left-hand quadrant. And we are slowly starting to push the envelope in these three directions and I think we'll learn as we go along.

MS. ANDERSON: Okay, thank you. We've heard several people now mention limitations of notice and choice and we know that those are a significant privacy concern in this area. What are some of the other significant privacy and security concerns that you all are seeing in the health and fitness realm?

MR. CROSLEY: I mean, I think one of the risks that we have is that more is going to be known about your health by others than by you. And how they use the information about you is a risk, right? That's a concern.

And so if there is no norm on, you know, what use can be made of data, other than that consent form that you might sign that can be very broad, then what others know about your health can have an impact on you, if you're not aware of it.

MR. HALL: I guess, something else I've mentioned just briefly is, there's a lot you can do with that sort of raw, granular stuff. You can keep that on the device, calculate some aggregate statistic and share that with the provider and that can help you move away from a place where you know so much about someone that you can put them in danger, for whatever reason.

And I'd like to see more -- so I guess that's an opportunity rather than another of a litany of problems we see today, which I think we've covered pretty well. I think there is an opportunity for doing client-side stuff and doing aggregate stuff. And some of the devices have to do that because they don't have enough power to do more complicated kinds of stuff.

But increasingly, you have more power on these devices, which means you can collect it all and send it all, which I think we should think about that and be careful about how much you need and how much you're sending and how much you're collecting.

MR. PEPPET: I think there's a couple different things. I mean, one is, and it may seem trivial but I don't think it is trivial, one of the biggest concerns for consumers at the moment is, they just want a copy of the data. So, you know, a 2013 study by (inaudible) who was trying to figure out all of the consumer concerns about fitness devices, the number one concern is, I can't get the data. I want to see my own data.

It turns out, again, if you take the time to read a bunch of these privacy policies, some of them say it's your data, some of them say it's our data, as the firm, some of them don't say anything about whose data it is or what kind of access you'll have, and often these siloed consumer companies are giving consumers access to sort of aggregated, analyzed data of, you know, this was sort of your heart rate and the number of steps you took yesterday or whatever, but not access to the actual raw information.

And if you want to import it to some other platform or if you want to just analyze it or you want to share it with someone, that's just one basic concern.

Another one is, you know, I think that if we are going to -- you said other than notice and choice. I think one of the biggest ones is just use. Drawing some lines around acceptable use, which we are very uncomfortable talking about in a lot of the privacy world. But for example, can an insurer require, as a condition of car insurance, that if you have an accident in the future, they have access to the blackbox data coming out of your car? The answer is, well, it depends where you live.

In a few states, the answer is no. States have said an insurer cannot do that as a condition of your insurance. Most of the states have said nothing, the feds have said nothing. That's a really hard question.

And you can extrapolate from that question to other kinds of insurance where you could start to see a home insurer, for example -- I mean, I love the General Electric example this morning of leaving your -- you know, your stove telling you you are leaving your stove on. Well, I'm pretty sure my home insurer would love to know that, if I was routinely doing that. Could they, as a condition of my insurance, require me to have my appliances share that information with them?

Now, you know, that's not General Electric's problem, but it is a policy problem that is really quite real and that we just have not wrestled with, I don't think. And again, we may not see it as a privacy problem, per se, you may see it as an economic power question.

And the last thing I'll say is that Commissioner Brill, I think, asked the question this morning of Vint Cerf about the economic divide, how is this going to play out, right? I'm not sure -- I sort of agree with him, I'm not sure this is really a problem of an economic divide, like the poor aren't going to be able to get enough sensors. I think the poor are likely to have sensors imposed on them, far more than everybody else.

So the people in this room, I doubt most of you, even if you have an employer, which many of you don't because you are fun, internet freelancers, but the ones who do, I doubt you are in a job where your employer is likely to impose that they want you to wear a sensor or else you are going to get fired. But there are lots of jobs where that's increasingly happening.

If you doubt that, read a new article in The Atlantic that came out like yesterday about truckers who are increasingly being monitored, long-haul truckers increasingly being monitored. Watch the person who cleans your grocery store and who, every time they get to the end of the aisle, they have to swipe their wrist against the end of the aisle where there's a scanner.

This kind of monitoring is very uncomfortable for people in the employment context, but it's here and getting more and more developed. So those kinds of privacy questions, I think, are hard and we are going to have to deal with them.

MR. CROSLEY: I mean, I love the idea of the appropriate use of the context because it really is the only way that we are going to be able to manage all of the enormous amounts of data that are coming in from all kinds of different areas.

And so, you know, we have regulatory models now that are based on this. The FCRA certainly is based on that. It sets a ring fence up, it says, you know, these people are appropriate, they have gone through security criteria, they can access the data, it is for these defined uses and these uses over here are impermissible. There is access to the information on how your data was used. I mean, it's a model that's workable and it's based on accepted uses that were determined, you know, dealing with experts. So I do think that what Scott suggests is a model that we are going to have to seriously engage in.

MS. HAN: What do the rest of you think about use restrictions? Any other thoughts?

MR. RADCLIFFE: That they're good.

MR. HALL: I was going to say, one of my colleagues is here in the room, Guautam Hans, and Justin Brookman, one of my bosses, wrote a paper recently about things -- privacy implications before any use is made. So once collection has happened, no one has touched it, there are still some -- there are some implications of having access to that stuff.

And so that's where I get to before I even talk about use restrictions. Use restrictions, as long as they have teeth. That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body. The FTC is a good -- for this application is, you know, they have history of doing consumer-based actions. They have a growing technical expertise.

Anyway, so I think that as long as it has teeth and it doesn't stifle things too much, to the extent that people can accept it and that folks like us can say, yeah, it promotes innovation, to a certain extent. It's not a free-for-all, but at the same time, it puts some real restrictions that mean something and has real teeth behind it, that would make me happy.

MS. ANDERSON: We've got one question from the audience. The EU is considering narrowing rules around consent and compatible uses. What effect would a move to explicit consent for each use of data have on healthcare and research?

MR. HALL: Can we ask the questioner some clarifying questions?

So the consent stuff is not necessarily in the health -- actually, they're scaling back some of the consent for public health uses, so maybe they are talking about the consumer stuff.

MS. ANDERSON: Why don't we go based on that assumption?

MR. HALL: Okay. That was just me clarifying, I don't have an actual answer.

People are mad about bringing back or taking consent away in the health context, that's something I don't have a response for. Sorry.

MR. PEPPET: No, I was just going to say, I mean, this is one of the conundrums, right, in this space. If you've got a bunch of different sensors on a bunch of different devices, on your home, your car, your body, that are measuring all sorts of things, there is just no practical way that you can consent every time one of those sensors reports something about you or else they are not going to be useful.

So that's what just tactically and pragmatically puts pressure on consent as the solution here.

MR. HALL: There may be technical solutions. I'm sorry, I'll be really quick.

Something that I would like to see exist is something I put on my home network before my cable router, DSL modem, or whatever, that allows me, in bulk, to anoint certain kinds of data that flows forth from my house. So that's a way of sort of aggregating consent-like stuff. It sounds a lot like DuoTrack, it sounds like other things like ad identifiers and things like that.

And you would need some basic standard so that telehealth companies that do anything related to the Internet of Things could mark certain packets as, here's the thing, here's what it is trying to do, so that you could then preclude certain data from flowing forward. It's not a perfect solution, but it might help.

And I mean, I think explicit consent for every use would be catastrophic. I mean, it would basically shut down innovation, it would shut down treatment. It's just, beyond practical, it's also unethical, right? Art Caplan, Eric Meslin and a host of others have looked at consent and they said, look, if this is the vanguard, if this is going to keep impermissible use from occurring, this isn't an ethical construct, right? To expect that the patient understands the full scope of use, the full scope of risk, and they are determining, based on their limited understanding, whether the use is appropriate or not. You know, they're going to trust the doctor and they are almost always going to say yes. In many circumstances where their answer, if they knew the risks, should be no.

So the idea that consent in health care is really, for a data use, is really the only thing we are going to stand on is just not an ethical construct.

MR. RADCLIFFE: You know, one of the things, when I think of that, is we don't have to go very far backwards to see how user agreements and acceptable licensing has really just been ignored.

Like okay, agree to this license. I mean, how many of you have read the iTunes license when you reinstalled it? Really? Nobody. I mean, it's pretty limited, right? If you have insomnia, I mean, go for it.

But another example would be that when I brought the issue to Animas about the software bug, they were like, oh, it's not a bug, it's a feature. It's on your manual. And I said, are you kidding me? And I pulled out the 472 page manual and, sure enough, there was a sentence on page 74 about this. And I was like, but really. It's a 472 page manual that I guarantee you 98 percent of all these users haven't read.

And that's what user agreements and licenses have become, it's a joke. I mean, if you want explicit permission, yeah, yeah, yeah, whatever. I accept. Just install the damn thing so I can get what I need to get out of it.

So it's really kind of a false solution. And you need to look at what's been tried before and say, if we don't want to go down that path, we've got to come up with something new, not to recycle bad ideas that have been used before.

MR. PEPPET: Before we get off of notice

and consent, or just consent, two things. One, as opposed to the 400 and some-odd page manuals, privacy policies on most of the fitness devices that I've played with, at least, or looked at are unbelievably short and leave out huge amounts of information that I, as a consumer, would want to know.

For example, half of the ones I surveyed didn't say anything about the actual health -- well, I can't say it's health data, the actual data about physical state that the device was recording or capturing. They just said things about use of the website, which is a totally different kind of data and not necessarily what the consumer would actually want to know about.

So we are a very early stage in just the norm creation around what would those privacy policies talk about.

The other thing I'll say, and I just have to inject this, because otherwise I'm not going to have a chance. I don't see how consumers could be consenting, in the sense of understanding the risk they are up against at the moment, when if one of these companies is hacked, which we've heard all day, they can be in almost all of the -- almost all of the devices I know about, when a good security has tried to hack them, they've been able to. If any of these consumer devices are hacked, then none of these are subject to the state or federal data breach disclosure laws.

So I looked at every state data breach disclosure law this summer and, guess what, none of them applies. Maybe Texas, maybe Nebraska, to the data coming off of your Fitbit. I think if Fitbit gets hacked and they steal 100,000 users Fitbit data, the public should know that.

So if I had a magic wand, the first thing I would do is I would just amend the definitions in all of those state data breach disclosure laws and say, hey, consumers have a right to know when this information gets out so at least their consent means a little bit if they know the risk that they are, you know, doing business with a company that has lax security and has been breached.

MR. HALL: Scott, have you written this yet? Can we read this?

MR. PEPPET: February. It's a cool paper called "Sensor Privacy."

MR. RADCLIFFE: I will say one thing about the breach notification, because I've dealt with that for a very long time. We've started to see some fatigue in that, from that perspective. People initially were like, oh my God, my data has been breached. The bank sent me a letter. Now they're like, they don't even open it. I mean, it's become alert fatigue of like, yeah, whatever. I mean, you're sending me these every three months because banks are getting popped all over the place. That information is pervasive all over.

So it's a problem from that perspective. You have to kind of take that into account. Not saying that it doesn't work, because I think breach notification laws, I know that they have caused businesses to change, from the legal liability standpoint. But from a consumer standpoint, I don't think they've had the impact long-term that we would like to think.

MS. HAN: Okay. So I know we've talked about appropriate use restrictions, but I wanted to get into some of the other privacy and security consumer protections that might exist.

Anand, why don't we start with you, as you've been developing your product so we can get your insights first.

MR. IYER: I think that -- so we have a

framework. It is actually, for those who are interested, check the Diabetes Technology Society publication in April of this year, there's a nice white paper that we did with the Air Force on this architecture.

Security is a multilayer -- it's multilayered and it all starts with the user. So there's a user layer of security, there's an application layer of security, there's an environment layer, there's a device layer, a network layer, a services layer, and then an integration layer. And I'll talk about each one of these briefly.

Users, when you think about it, in many ways the number one source of breach and things like that are users. We always say that there are three ways of ensuring user security, right? Must have, must know, and must be, right? Think about it. We're all violators. I forgot my thing in my jacket in my office, can I borrow your pass to get back into the building?

We don't do that as much with passwords, must know. So must be is the last one, which is retinal scan, thumbprint, whatever. But we have to educate people and employees, especially in

HIPAA-covered entities, about what security really means. And that's not a small task. So there's user security.

There's application security. I mean, it's interesting. We've gone through several external audits and security firms coming in and doing penetration testing and all the things they should do and writing the reports and looking at vulnerabilities and the software coding practices. And where people open ports and leave ports open that are vulnerable to attacks and phishing and hacking and what not, it's amazing. And for us, this is software 101. You don't code that way. You just don't. But 90 percent of people code software that way. 90 percent of the applications in iTunes and Google, if you would -- they would miserably fail security tests. So it has to be secure at the application layer.

The environment is interesting. We all have data centers, but how many people actually have best practices for physical, electronic, human, et cetera security at the data center? They don't.

Devices. We encrypt on the device, we encrypt on the link, we encrypt on the server, we encrypt -- and encryption means it's 256-bit AES, you know, it's -- good stuff, right? When we had the chief security officer from the Air Force, we did a project with them at Wilford Hall, said we like your security architecture, that's pretty good. But it's got to be encrypted there, because if I lose my phone, I ought not to have vulnerabilities for data loss because somebody has my phone.

The network is the network. That is something we are all familiar with. There's all kinds of security ways to secure networks, some better than others.

And then at the service layer, every touch-point with the customer, whether it's customer care, help desk, has to follow all of the proper security methods and procedures. And so for us, it's really a collection of all of these things that define how you fundamentally architect your security, the measures against which you monitor and then you publish and then you continuously improve to say, you know what, we've got to reduce vulnerabilities here. We've got to improve, you know, protection there. But that's kind of how we've evolved it over time.

MS. HAN: Thanks. Anybody else?

MS. ANDERSON: I think we have one more

question from the audience and then I'm going to have a slight variation on this. So the question was, what's the top security concern that you think doctors should be aware of as they rely on these devices? And I'll expand that to speak beyond doctors, also what is the top security concern you think consumers should be aware of as they decide whether or not to use devices?

And to the extent you can, speak to any precautions that those doctors or consumers could take.

MR. HALL: So most of these things don't encrypt on the device, they don't encrypt when you're sending. You don't have to know what that means, but buying a simple VPN, something that, if you are at an open wi-fi at a coffee shop or something, you could fire-up as soon as you connect to the wi-fi network, that will at least protect your information from other people snooping locally. That's something that people don't often realize.

It's hard to give prescriptive things. You know, unfortunately one of the most -- one of the hardest things about security these days is people's devices are riddled with crap, you know. Especially desktops. Some to a lesser extent, you know, your gated mobile platforms, but even then, there are various things that can do pretty promiscuous stuff. It can do things without your knowing and that, if you really appreciated the consequences, you wouldn't let them do.

And maybe, this is where I was -- the Privacy Rights Clearinghouse study that I was talking about was so neat because they actually went and did some pretty cool forensic stuff, only on 43 apps, but it would be neat if you could put bounties up to -- and say, what is this app that I care a lot about? Like my password management app, you know. I have to use a really boutique one that I don't know is very sound and I would like to know that, but I can't pay someone else enough to do that. Maybe I could -- money to do that, especially -- and that would happen very quickly for some of the top apps.

MR. RADCLIFFE: For me, I think that consumers need to understand that the thing that they're using is probably not secure. I think that a lot of users just have the assumption that it is. And they're like, oh, well I'm on the internet and it's going to be fine. Or why would a hacker attack me? I'm a 35-year-old white male at Starbucks. You know, I don't have any money, I don't have any power, whatever. And that's just simply not true.

You know, attacks use those types of people as a steppingstone or use large quantities of those types of people. Where they are not attacking you, but it's leverage against something else, it's a way to hide.

So getting consumers to stop and think for a moment, I'm in a Starbucks. Should I log into my bank that's totally not encrypted right now? Maybe not, right?

So in some cases, we are getting there with the financial industry, right? You know, I go to the ATM machine and now it's -- there's a little hovel that you have to get into and there's things that protect your fingers. You can't see what is being typed and people are aware of that now. And I think we need to bring that awareness to the next step, which is I'm wearing this device that's collecting all this data, where's my little hovel? Where's my keypad? I had to pick a password more than three characters. You know, like things that will help do that.

And some of the consumer device manufacturers are starting to do some of that, but doctors need to make their patients aware or companies need to make their patients aware that, like, you're getting something that is connected here. Let's think about that. Let's think about that in a larger construct. And that's hard to do.

MR. CROSLEY: Building off of what Jay has said, I think that data integrity is really the -- in healthcare, that's what we are worried more about probably more than anything else, right? Data integrity. Is the doctor going to act on data that may not be accurate, that may not accurately reflect the information collected.

Taking a cue from being an analytics company though, the answer isn't less data, the answer is more, right? And so it's what I think we are going to get into with health care is I think we are going to have multiple sensors. I think we are going to have multiple different applications measuring blood pressure. I think they are going to be aggregated and sifted and we are going to find out the confounding variables and then come out with clean data. And that data will be assessed and have integrity.

You know, data security is going to undergird all of that somehow that I think that, you know, we are going to evolve into a place where we will be able to detect when the data doesn't have the integrity that we are used to seeing and we will be able to hopefully treat along those lines.

MR. IYER: I agree with everything you said, Stan. And just one interesting observation, where I go back to my earlier point about the clash. In one of our larger clinical studies, you know, we observed many things. University of Maryland was our principle investigator and so it was an academic study and so we had the luxury to observe all kinds of stuff. Just to observe, right, because it was academic. And then figure out if there is any value in it.

And it was interesting to see -- you saw how I password protected my application? I actually had to enter a four digit password to get into the application. We made that optional. We know from FDA we have to -- there is a PHR on the phone that has their meds, their doses and all that. That's password protected, and it has to be, inside the application. There is a second layer.

But the one for the application, there's no real data or PHR stuff so we said let's make it optional, right? And what was interesting is, doctors came to us and told us, I think you should take that away. We said, why? And they said because people who actually do that aren't using the system. It's one more hurdle for them to go into. Usability.

And so therein comes the clash, right? So it's very interesting. Take away the four digit thing and we said, huh, interesting. Because at the end of the day, the doctors prescribing Lipitor to their patient, they improved their -- bad example with statins and what's been happening the last couple of days. But doctors have been prescribing Lipitor to help improve the cholesterol management for the patient. They're going to prescribe BlueStar to help them manage their diabetes. They want them to get better. I mean, it's an altruistic reason they went into medicine, right? They are not just doing this for money. They want their patients to be better.

And so any hurdle you can remove to have a patient adopt and manage, that's where we are going to get the clash in. Now if I have -- now I've got to consent to everything and privacy and this and that, patients will throw the bloody thing away. They won't use it. So that's where we are going to have the -- it's going to be interesting how that plays out.

MS. HAN: Okay, thanks. So we are just about out of time, but I wanted to give each of our panelists maybe 30 seconds or less to just answer the last question.

What do you see as the most valuable role the FTC could play in this space? Let's start with Scott.

MR. PEPPET: Two things. One, apply the existing laws, which could be better, but things like FCRA, for example. So the FCC this year, in January, looked at an app that was making criminal records available to employers. I think you are going to see other kinds of sensor data, health data, trying to migrate out of the health space and into things like employment. And you've gotta watch that line.

The second thing is, I would look really hard at the privacy policies of a bunch of these consumer products already and ask whether they are enough or are accurate or are -- potentially, you could say here are the things we think that these consumer sensor devices should at least talk about in a privacy policy.

MS. HAN: Thanks. Stan.

MR. CROSLEY: Use your station as you have here to convene stakeholders and have meaningful conversations like this, but I think also to begin the path down an appropriate use conversation, just recognizing that, you know, notice and deception isn't going to get you very far down this path.

MS. HAN: Thanks. Joe.

MR. HALL: Maybe some very specific, I don't know how specific you can get, guidelines about best practices, in terms of device privacy and security. More enforcement that fills the sort of gap that HIPAA has left, like the LabMD case. You know, which would help -- the other side of that is having things to point to to say, here's what you should be doing, here's what ran afoul in these cases. But that will come in time.

MS. HAN: Jay.

MR. RADCLIFFE: We have to have somebody that holds companies accountable for the statements they make. We have too many companies saying, oh yeah, we're totally secure and then, you know, somebody like me comes around and pulls the monster out of the bed and shows what's really there. I can't slay the monster though. I mean, I keep pulling them out and I can't do anything with them.

So there needs to be some conjunction there over making some accountability that you can't do that. You have to be accountable for your actions.

MS. HAN: Thanks. And Anand.

MR. IYER: I'd say continue to do this, but continue to collaborate with the other agencies. At the end of the day, it's not just you. It's the FDA, it's the FCC, in this connected health space.

And rather than recreating something and trying to start something on your own, kudos to Commissioner Hamburg at the FDA for the guidance document and Bakul Patel who put it out, great work. There's holes in that, everybody knows it. There's pieces that you have expertise in that you can help plug some of those holes.

I think it shows a tremendous amount of national leadership to stitch these perspectives and agencies together to come up with the requirements for what a solution should do and then let industry go and innovate the way they should innovate and compete on the basis of competition. And then you guys can help accelerate the adoption of these things by partnering with those agencies.

MS. HAN: Okay, well thanks to all of you for joining us here.

PANEL THREE: Connected Cars

MS. JAGIELSKI: Okay, we are going to get started. This is Panel 3. This is on Connected Cars. I am Karen Jagielski and I am joined by my co-moderator.

MR. BANKS: I'm Lerone Banks.

MS. JAGIELSKI: And we're going to introduce panelists in just a minute. We have -- this is a short panel, we only have an hour. So we are going to quickly get through introductions and then get to the heart of the situation.

So with that, I'd ask my panelists to introduce themselves and tell us just a little bit about yourselves.

MR. KOHNO: Hi, my name is Yoshi Kohno and I am an associate professor in the Department of Computer Science and Engineering at the University of Washington.

My area of expertise and specialty is computer security. One of the focuses that we look at is computer security for cyber-physical systems. And so in our lab, we have done a lot of work on security and privacy for medical devices, for home automation systems, for children's toys, and for the purposes of today, talking about the work we've been doing in the security and privacy for the modern automobile.

MR. WOLF: I'm Chris Wolf. I'm the founder and co-chair of the Future of Privacy Forum. I also lead the privacy practice at Hogan Lovells. At FPF, Future Privacy Forum, we've been doing a lot of work in the five years we've been around, on the Internet of Things, starting with our efforts for a code of conduct on the smart grid. More recently dealing with retail location standards and we also have a connected car project that is going on at FPF.

Today, we published a paper called an, "Updated Privacy Paradigm for the Internet of Things" and I guess I'll talk a little bit about that during the panel.

MS. JAGIELSKI: And that's also available up front. There's copies there.

MR. NIELSEN: I'm John Nielsen with AAA. I'm Director of Automotive Engineering and Repair. AAA's interest in the connected car really centers around the motorist's opportunity to use this new technology, to understand what it can do, to understand the implications of it and make sure that what they receive is all that it can be, without distracting -- without distraction and without loss of privacy as they use it.

MR. POWELL: Hi, my name is Wayne Powell. I work at Toyota, specifically in the -- we have an R&D Center in Ann Arbor, Michigan and I am the general manager for the group that is responsible for multimedia and telematics development, primarily for the North American market.

As I suppose is obvious, we make cars. It is our responsibility to deliver these systems to our customers, both on the vehicle side as well as the cloud connectivity. It is our responsibility to design and validate.

MS. JAGIELSKI: Okay, thank you. And just for purposes, just so we understand again, we have a short period of time, just in terms of defining the scope of our conversation, we are going to limit this to consumer-facing technology. We will not be talking about V-to-V, vehicle-to-vehicle, information transmission or vehicle-to infrastructure, V-to-I, technologies.

So with that --

MR. BANKS: Let's get started. So we heard earlier that a BMW has five computers that it uses to unlock the car doors. And so I don't own a

BMW unfortunately, but I've been in a few and I didn't know that there were that many computers at work.

And so that gives us a good starting point. What are some of the technologies that exist currently in cars? How many computers? What types of computers and systems are available in vehicles today?

MR. POWELL: I guess I could start that one. Quantity of computers, I don't have a number off of the top of my head, but at one time the automobile was the single largest consumer of CPUs from a single device point of view. There are dozens and dozens. Of course, the more complex the car, the more we have.

And the idea of using multiple devices distributed across the car to do a function is very typical for issues like that.

Specific to this particular topic of connected vehicle, maybe I can clarify some things of what a connected car is and what it's not. First, I'll start with what it is not.

Most of what Toyota has done in the connected car space has been to connect the users in the car with information that they want and they need. That has, for a very long time, has been satisfied through broadcast media. We are downloading from either satellite or terrestrial-based systems.

So the majority of what people actually say they want and actually do consume, based on prior testing and our surveying, can be serviced by broadcast media. Meaning we can send traffic, weather, lots of information down to the car, the car can grab it, store it, and the consumer can consume it with no bi-directionality of the data.

So for many years, that's been most of our connected car space in the data space. So in that sense, that is not connected car, since it's one direction.

Another area I want to clarify that is not connected car, and I think this has come up in some questions, is the EDR, the event data record. As far as -- I think there is some fear that we have the ability to connect that to the network. We do not. That is a stand-alone device in the car that has to be -- the car has to be accessed directly through wired devices to actually get that data out of it. So the EDR is not part of our lexicon of connected car discussions.

Having said that, let me talk about some of the things that we do do with connected vehicles. There is two basic pipes into our cars, one is through embedded modems we call DCM data, data communication modules. They go by a variety of names that people -- General Motors uses OnStar, those kinds of things. That's an embedded modem, a phone, embedded to the car. It has a secure connection to, in the case of Toyota, our server networks. It is a one-to-one communication and the data flow is managed from the vehicle to the center directly and through secure links. And that is a subscription-based service and the customer can opt out at any time.

The second one, and the more recent one you see a lot more about, is the smart phone-based connectivity of cars. In Toyota we call that Lexus Enform/Toyota Entune systems. Those are more -- the ones you hear a lot more about. They are more the app type environment where consumers can do things like such as they can listen to Pandora audio stream sources, they can also conduct some queries for movie tickets or restaurants, things like that.

That's the second pipe into the car and that's largely through the consumer's phone and connected to data through Bluetooth or USB into the car itself.

I think it's important to recognize that those systems are, by design, segregated in the vehicle where they are not connected to the entire vehicle data bus and have access to the entire car's data network.

So those are the two primary paths that we address when we talk about connected vehicles.

MS. JAGIELSKI: I'm sorry, I don't mean to interrupt. What you just described, is that unique to Toyota's model or is that across the industry?

MR. POWELL: Well, it's certainly Toyota's model. I think, by-and-large, I can't speak for everyone but that is basically the methods that I -- there's some short-range communication wireless devices like -- you could consider Bluetooth, I suppose, wireless or wi-fi, but the majority of the long haul wireless communications, bidirectional in the car, is through those two means, yes.

MS. JAGIELSKI: And I can tell Yoshi had something he wanted to add.

MR. KOHNO: I was just going to chime in a little bit. So I clearly don't have the same level of expertise that Wayne has with regard to, you know, working at Toyota, but I would say that we have, as part of our lab, we actually purchased, in corporation with UC San Diego, purchased two modern automobiles and studied them from a security privacy perspective.

I won't get into the security and privacy just yet, but I do want to say that the modern automobile is pervasively computerized. The one we had, you know, dozens of computers in it. I've talked with manufacturers that have more than 100 computers inside their vehicle. And they are all connected to each other and the fact that there is a lot of concern about having so much cabling inside the car is really weighing down from a physical weight perspective.

There are several points that I wanted to make to follow-up on Wayne's. One is, in case you aren't already in the automotive space, is that the connection -- the computers that are within the car are incredibly value from a safety perspective.

And to give you an example of the safety value and also the connectivity within the car, some modern automobiles have a sensor on each wheel that detects how fast each wheel is spinning. They will send this sensor to another computer in the car that will determine if one wheel is spinning faster than the other, and if it is, that's a sign that you might be getting into a skid. And then so it will send a message to the brake controller and say brake controller, please slow down the back left wheel. And it will apply more break pressure to the back left wheel and that provides traction control. So there's a huge value in the computers and the connectivity within the vehicle.

The second follow-up point that I would make is that, you know, I think there's lots -- when we think about connectivity, there's lots of different definitions we can have in mind. I really like Wayne's definition of connectivity from the perspective of, you know, this is some sort of capability that we are providing toward the consumer or toward the, you know, the person using the vehicle.

But one thing that I will point out, when we are dealing with these new technologies, is trying to understand the unexpected consequences. Mainly, there is connectivity by design and then there is also connectivity by a hacker. This is where a hacker figures out some way to bridge multiple networks or some way to leverage the connectivity in unexpected ways, and so that is something that, you know, we in our lab also try to think about.

MS. JAGIELSKI: And specifically as to connectivity by attacker, that specifically goes to some of the work you and your colleagues did. Can you talk a little bit about that?

MR. KOHNO: Yeah. So there's a number of things that my colleagues and I did with the vehicles that we purchased. The first set of things that we wanted to do, just to, again, ground you in the context.

Within the market automobile, there are dozens of computers and these computers are connected to each other for valuable safety purposes. The first set of experiments we tried to figure out was what might an attacker be able to do if they could connect to that car's internal computer network.

And we found out the attacker could do a large number of things. The attacker could control the brakes, he or she could control all the vehicle lighting. And we tested this actually on a decommissioned airport runway, for safety, where we had a test person driving the vehicle and then we sent an adversarially-crafted packet over this car's network, making it impossible for the driver to actually stop the car. And we did a number of other tests as well.

The second set of experiments, we said how might an attacker be able to gain access to the car's internal computer network without ever physically touching the car. And we actually found several ways to do this.

And one of the cute ways that we did it was that we found that we could actually, you know, I could email you a WMA file that would play perfectly fine on your music file and would play perfectly fine on your computer, but if you burn it to a CD and put it into your car, a CD of Beethoven's Ninth, you put that into the car, it unlocks the car doors. We can do a whole bunch of other things as well.

But perhaps even more interesting was our car had a built-in telematics unit. Wayne already mentioned the BCN. We found that -- what this means is that, when we buy the car off of the lot, it basically had the built-in cell phone in the vehicle. You know, we didn't have to do anything. We didn't even activate our service and we were able to call this car's phone number, play the appropriate tone to switch it to an inbound modem, play the appropriate, you know, bypass an authentication vulnerability in the vehicle, and then load our own software on to the car.

So basically by calling the car's phone number, we were able to do this. Because the car had a built-in cell phone, it actually had 3G data, and so once we had this little small bit of code on the car, it actually opened up an internet connection to our servers at the University of Washington where it downloaded additional code. Basically, if you are a computer scientist, it's an IRC client.

And so we have, you know, we basically put the cars on our command and control system at UW. From that point, we can do anything with the vehicle. We can locate its GPS coordinates, we can start the engine, we can disengage the brakes, we could bypass the mobilizer so that -- the thing that is designed to prevent theft.

The car also has Bluetooth hands-free calling, which means that it has in-cabin microphones. So we could turn on the microphones within the car and listen in on everything that is going on inside the car without any visual indicators. And that's kind of maybe a little longish summary, but.

MS. JAGIELSKI: No, I think that's quite enough. Thank you.

MR. BANKS: So given the depth of those risks, it sort of begs the question of, aside from some safety benefits, what are the actual other additional benefits of having connected cars or why do we --

MR. WOLF: So maybe I can talk about that. And I'd be interested to hear from Yoshi whether or not his experiments have ever been revealed actually -- whether there have been examples of this in the real world.

But yeah, I do think it is important, as one of your previous panelists talked about, you need to know what the numerator is as well as the denominator. And the benefits for connected cars are really quite significant for people who have it, you may have experienced it.

For example, if a driver is in an emergency situation, they can literally just push a button and call on first responders. Or even if they are not able to themselves, first responders can be called by the car. These systems can alert drivers to hazardous road conditions and navigate the drivers around them. There are on-board sensors and analytics that can work together to detect dangerous malfunctions and to alert drivers of the dangers.

And they even can be used for parents to ensure that their kids are using the car responsibly. I have an app for my car that shows a map that will actually show where the car is riding and how fast. And I'll know that it is a family member that I've loaned the car to and I can see how they're driving.

I also have a car that can have software updated wirelessly, with my permission. They notify me every time it happens. And one of the conditions in the car currently is that it has such a low clearance that apparently it's been striking objects in the road and causing fires.

And so today, the manufacturer announced that they were going to send an update to raise the suspension. I won't have to go to the shop to have that done, the car will do it for me.

In terms of public safety, connected car companies may be able to disable or slow down vehicles to help reduce the number of high-speed pursuits. We've actually seen videos about this on some of the TV crime shows, where if there's a car jacking or some other incident going on from a remote location, the car can be slowed down, the four-way flashers put on, and the car can be stopped.

Obviously stolen cars can be recovered more easily with this kind of technology. And location services can help ensure that good Samaritan calls result in first responders being directed exactly to the scene.

And then there are simple convenience factors. And my car, if it is 116 degrees in the interior, which sometimes it is here in Washington during the summer, I can turn the air conditioning on from my app and make the car cooler inside.

The NAS system is connected to a lot of information, we heard about Ways this morning, from Vint, that might help me avoid traffic jams, maybe even avoid speed cameras, if that's on -- I think Ways offers that opportunity as well.

MS. JAGIELSKI: Not that you ever speed.

MR. WOLF: No, not that I ever speed. Find parking and other things. And so coming along will be things like offers from mechanics, restaurants, retailers, entertainment venues and more that I might want to have provided to me through the apps in the car.

Infotainment systems can allow me to, at appropriate times and places, access social media or have a passenger access it. We heard about apps today that can make sure your garage door is shut. It can also open your garage door. I've used my app more than a few times to remember where I've parked. It provides a map and directions back to the car.

And I mentioned that the software not only, on the suspension issue, but the software can be updated to provide additional features and also safety enhancements without having to take the car to a repair shop.

MR. NIELSEN: And maybe just building on that a little bit, in addition to what it can do today, when you think of the car having computers on almost every system that exists, either from a standpoint of monitoring what it's doing or causing it to accentuate and do something else, it also provides the ability to identify things that could be failing, that could be going wrong.

And so if you play this out in some of the newer systems, they are now actually capturing data and saying, wait a minute, this system is a little bit out of spec, it's time to come in for service.

So the potential with all of this technology is to simplify our lives. I mean, it sounds counterintuitive to talk about all of this complex stuff, but applied properly, it really does simplify life for motorists, provides new insight that can keep them safer, it can help save some money, and it gives them an insight that otherwise they wouldn't have. So there's a lot of pluses to it.

I would just say, the other side of the technology is obviously we think of distraction and looking down at something and manually moving a knob, the cognitive distraction. There are so many things going on and work overload is real issue. The AAA Foundation for Traffic Safety has done some research that shows there are some limits. And as we get more and more and more into the car, the opportunity for distraction, if the data isn't displayed properly and controlled in a good way, is a seriously growing risk.

MR. WOLF: So John's point is really critical because if we talk about the pros and cons of having these technologies in the car, we have to understand, drivers are going to have them. They are probable going to have them on mobile device. And so it's an issue of whether you want them looking down with their iPhone in their lap -- how many times have we been behind drivers that are driving very, very slowly and they are obviously interacting with an app and then you honk at them or flash your lights and then they speed up very, very fast.

They're going to do that, whether or not it is provided by the OEM or it's in the car, so why not provide it in a way that is presented so that their head is up and perhaps there are access controls on what is available when the car is moving or not and is presented in a way that is both user friendly and safe. And I know that's beyond the jurisdiction of the FTC, it's more a NTSA issue, but it's obviously relevant to flesh-out this discussion.

MR. BANKS: But it's still really interesting and it begs the question of when is there too much technology? So we heard earlier about the different things that you can do, say, with fitness devices. And so if you take those devices that you've heard about previously and integrate those into vehicles, how much distraction does that create and how to we start to assess when there's too much technology?

Because one thing I guess we can be sure of is, if it's possible to build it, there are innovative people that will try to build it, but does that necessarily mean that it's appropriate, actually, for a car?

And so how do we start to determine or -- I'd be interested in your thoughts about how do we start to determine where the line is in terms of what technology we should actually consider integrating into vehicles.

MR. NIELSEN: Building on the previous point, I think the technology itself is of benefit. And information or data, there's not a downside to that. I think that something that is produced by the car, the more that the owner can access and use that, there's just nothing but upside.

I think the issue really centers around how it's used, how it's displayed. Not whether they have too much or too little. I think it's, how do you put it to use? Do you need that while you're driving down the road or is that something that you want to access at home or share with someone else?

MS. JAGIELSKI: Well, in terms of -- so this data, these services are being provided and they sound great, but in terms of the other side, and I know Wayne you talked a little bit -- the model I think you were talking about is a little different, because it is sort of self-contained, but in terms of data that is being collected by all of this technology in the car, you know, the question arises, well, what is happening with all of that data? Where is it being stored? How is it being used? Who has access to it? Do third parties have access to it? Can you talk a little bit about those issues?

MR. WOLF: Maybe I can start because the Chairwoman this morning used this example, she said connected cars may direct emergency responders to an accident, but will the data transmitted be shared with your insurer, who may raise your rates or cancel your policy.

And I actually tweeted that this is a hypothetical that sounds scary, but there is no factual predicate for it. In fact, the closest thing we know is that there are insurance companies that provide you the opportunity to have monitors in your car to evaluate your speed and location to affect your rates and also maybe make conclusions about your safe driving, to also affect your rates or your coverage. But believe me, those are done with absolute disclosure and purely a choice on the part of the insured motorist. I don't think we've seen anything close to the hypothetical that the chairwoman raised.

And with respect to the OEMs, I think we've seen pretty good disclosure about the collection and use and access to data. And to the extent that there hasn't been, you know, granular disclosure, I think context says a lot. I think a lot of motorists would understand that, when they push the button to have an emergency responder come rescue them, their data is being shared with the emergency responder.

MS. JAGIELSKI: Well, what about in terms of, say -- and when you talked a little bit about this, I believe, vehicles that say, you know, you can take your smart phone, you can plug it into your car, run whatever apps you want to run -- so the OEMs may have a particular policy regarding the vehicle itself, but once you start introducing, say, these third-party apps or your smart phone or whatever, at that point, who becomes responsible, or is there anybody responsible for what data is collected and how that data is used?

MR. POWELL: As far as the data itself, we have a basic -- the technology is available to do almost anything, as has been described both up and down here.

To another -- the first thing we say is, what do we need? What is the necessary functions that meet the litmus test of what is necessary in a car. And these gentlemen already described it, basically safety-related functionality that Chris described regarding airbag deployment and things like that. So the need, what is the value proposition in the car to the customer.

And also the improvement to driver awareness. Things like traffic and weather and incidents on the road makes drivers not just not distracted, but more aware and better drivers and more capable dealings with complicated traffic structures and things like that.

We also have another litmus test that says driver distraction, which John was talking about as well, driver distraction is an enormous issue. We do -- Toyota has policies in place, internal, self-imposed policies in place, that we restrict access to things when vehicles are in motion. Toyota has been working with others, other car consortiums to develop those. But even before that, Toyota had these policies in place for years before that. And we've taken a beating in the marketplace over that. I mean, there are customers who consistently complain about the fact that, why can't I do this while I'm -- or why can't my passenger do this while I'm in traffic.

They're good questions, but the Toyota policy is conservative there and we block things out, we don't allow certain things to happen, because we don't think it's appropriate to do in a car. So layer on, we learn the functionality to what's appropriate.

To the issue of security, this is kind of the essence of the issue today, I think. Toyota takes a layered approach. First, what I mentioned of the limiting what we actually have available in the car. Security by design, we -- Yoshi described a large number of microprocessors that are all connected. Well, generally that is basically true, but that is not perfectly true in each case.

All networks, all vehicles, our products, the CPUs in the cars are not connected to all networks. There is some level of segregation in the vehicle and we engineer those things in.

We also have a second realm where the pipes that go out of the car are not just wide-open pipes that can -- both our DCM or built-in modem based systems as well as our smart phone-based systems have dedicated links, by design, to Toyota secure data centers. And then the third parties, if you will, access the cars through those centers, not directly at the car.

The third layer that we use to improve security is an evaluation itself. We test our cars, we actually go after this stuff. We look for holes in our systems.

And the fourth way is we engage third-parties outside to do the same thing. People such as Yoshi, people with these kinds of skills, these kinds of deep knowledge of how systems and how hackers can get inside. We erase that. And we hire them and we work with them and we take their input and we make their systems better.

Having said all of those things and putting in all of those layers, it is still not a perfect world and there is no such thing as a perfectly secure device and I don't believe there ever will be. But the number of layers and effort that we put in place, and the continuum that we are doing, to continue to watch for new threats, new points of attack, is an unending endeavor.

MR. WOLF: And can I just add that, having worked -- with my law practice hat on, having worked with a number of OEMs addressing these issues, they understand that the second they lose consumer trust because of undue concern over security or sharing or privacy issues, that this technology will not realize its potential. And it has huge potential, I think particularly, as we see new model years, we are going to see unbelievable evolution in this technology.

And so at least, based on my experience, these companies are taking these issues extremely seriously and are giving the security and privacy issues the highest level of attention.

MR. BANKS: This question is directed, I guess, mostly to Chris and John, but anybody else feel free to chime in, and it's about consumer attitudes about privacy.

So in terms of your interactions or research with consumers, what things have they been sort of squeamish about in terms of technology and access to their information and the amount of sharing that is possible in vehicles and just their attitudes about that?

MR. WOLF: Well, we have a couple of studies that we looked at at the Future Privacy Forum. There was a recent study by Covisint that found that consumers are really eager to see these maps and parking and traffic and other transfer information brought into their vehicles. They really see the value in being able to update software remotely to bring more entertainment options into the vehicle, to monitor their kids' driving habits and to transfer personal settings from one car to another, which is not something we've talked about yet.

In 2011, the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies, which goes to my earlier point about why these companies are taking it so seriously. And then that was followed by driver distraction, driver complacency, cost, and privacy sort of brought up the rear, which was kind of an interesting finding.

And a recent study by Capgemini showed that over 75 percent of global respondents who were willing to share their connected car data with OEMs or dealers, 20 percent would share the data with no restrictions, 27 percent would share it in exchange for incentive or services, and 28 would share anonymous data for research. And we really haven't talked about that much here, but there is a lot of this data that is being collected that is being anonymized and combined with other data to do traffic and other public policy kind of research.

MR. NIELSEN: Maybe to come back down to some obvious things. Consumers obviously are excited about the technology and that's -- as we heard, that's something they want and they want more of it. I think it's new, I'm not sure that they fully understand it, and this is anecdotal, that they fully understand what the capabilities are, what data is transmitted or gathered, and are there any risks for privacy. That's unclear.

But I think certainly they are interested, they like this. It is -- I think the auto industry as a whole would say that the connected car is the future. It's the way things are going and I think there is a strong concern for safety, for security for privacy.

And I would just say that, you know, there are a number of different car companies and each have different practices, different policies. I mean, everybody is concerned about privacy, but the way the data is collected, what's done with it, is diverse. And I don't pretend to know every car company, but what I know is we go into terms of service for a number of them and they vary substantially. And I think consumers, and this is anecdotal, consumers need to be better aware. And I think that one of the things that AAA will work on in the future, you'll see some research from us that really talks about what are they, you know, what do consumers think, what do they want, what are their concerns related to this technology.

MS. JAGIELSKI: Yoshi, in your work, I know your focus generally has been in the security angle of it. What made you decide to look at these kinds of things? Why did you decide to challenge the security systems of vehicles?

MR. KOHNO: Yeah, so the question, I guess everyone heard, why did we decide to analyze the security systems?

One of the things that my lab has been

doing for a very long time is trying to figure out what is going to be the next hot new technology over the next 5, 10, or 15 years and what might the interesting security and privacy challenges be with those type of technologies.

That is why -- and Keith Marzullo talked about it and Kevin Foo and I and a bunch of colleagues, we got the implantable defibrillator back in 2006 and started to say, well, what are the security and privacy vulnerabilities with this implantable defibrillator. That's why we are looking at home automation systems.

And it's actually for that same reason that we started looking at the modern automobile, because we saw this as being a very emerging technology and wanted to understand what the issues might be.

Over the course of all of our research in these areas, one of the things that we have observed is that very often, and I'm not saying this is all the time, but very often what we see is we see sectors of the broader industry that are not consumer science experts, start to integrate computers into their systems and then start to integrate networks into those systems.

And because they don't have the same past experience of actually being attacked by a real attacker, such as Microsoft and so on, their kind of level of security awareness often, and again not always, but often appears to be kind of dated.

So for the system that we analyzed for this automobile, the system fell to a number of vulnerabilities that are straight out from the 1990s that Microsoft and others were having to address.

MS. JAGIELSKI: I think that I -- that, I think, goes along with what some of the other panelists have been saying, that there is this consumer demand, or you're seeing a consumer demand for connectivity, but at the same time, is there the technological understanding and sophistication of the people implementing this connectivity and is this something that is a problem?

MR. KOHNO: So what I would actually say is that I feel like much of our work has already been done in the automotive space, in the sense that we now see auto manufacturers really very focused on consumer security and privacy issues.

The U.S. Society of Automotive Engineers, they have a task force on security for automobiles. U.S. Car also has a group focused on automobiles, and I think there is now a lot of awareness, both within the government and in the industry, on security and privacy for these technologies.

What I would say that actually worries me more is what is going to be the next technology in five years from now that we aren't discussing, but you know, in some laboratory somewhere, there is a lot of innovation happening and then that product emerges to the market in five years and, you know, will they have thought about security and privacy proactively.

MR. WOLF: But you know, I give Yoshi a lot of credit because he and his colleagues have made this an issue that, as he indicated, was a wake-up call. And I think if there is one takeaway from this panel that consumers ought to have is that these companies are taking the issue seriously. And I think if there were any substantial flaws or vulnerabilities that existed today in the cars that people are driving, we would have heard about it. And we haven't.

MS. JAGIELSKI: Well, we have a question -- I'm sorry. We have a question from email and I guess this is primarily to Yoshi.

And the question is, what can/should you do if your vehicle is hacked when you are driving?

MR. KOHNO: I think that's a very, very tough question and I think it raises -- I believe it actually connects to a question that Chris asked earlier. We haven't really seen anything like this in the wild yet. And I actually think that the risk to car owners today is incredibly small for a number of reasons.

One is that, to pull off the full set of attacks that we did requires a significant amount of technical sophistication. Second, all the automotive manufacturers that I know of are proactively trying to address these things.

You know, I don't want to speculate on what to do if this situation were to arrive in practice, but I would say that I feel like the risks today, because people are addressing it, are small. With that said, I don't want -- you know, I don't think anyone plans to become complacent and it is very nice to see that, you know, we are having this discussion here today and that all of the industry and manufacturer representatives and so on are looking at the issue.

MR. BANKS: I think you made a really good point earlier, Yoshi, about consideration of future issues and it would be interesting to hear what the industry has in place currently to be forward thinking and proactive about yet unidentified potential issues.

MR. WOLF: So to set the stage for that discussion, and then I'll turn to the experts who are actually doing this work, but I wrote a blog entry for the IPP Privacy Perspectives earlier this week as a preview to this workshop and I said, do we need the law of the connected horse. And for those of you who remember, Judge Easterbrook and Larry Lessig had this debate over whether or not we needed "The Law of the Horse" to govern the internet. And the debate was over whether or not existing law was sufficient or whether we needed to evolve some new rules.

You know, I come out in taking a really moderate approach and seeing whether and when there are problems rather than trying to innovate or legislate in advance, which could really stymie innovation.

MR. POWELL: I think we've touched on some of the things that both Toyota and other OEMs do to prevent those kinds of attack, but you asked what's the next frontier.

One of the frontiers we see is not just our electronics in the car, but a lot of brought-in devices. The smart phone is a brought-in device, it has a lot of capability, but you are seeing additional ones beyond that. Things like insurance company dongles plugging into the OED connector that have their own modems built right into them. And there are a lot of devices that are coming to the car.

We also have non-OEM competitors, well they're not competitors, new entrants to the space, like the Googles and the Apples, who want to take over the in-car experience with their device and they just simply want a want to interact with it in the car.

We don't have any real control what they are doing and that's probably one of the areas, going forward, that we'll see some areas of unclarity there. As I said, the insurance companies are pulling both position and various driving behavior patterns that don't go through any of our systems in the car at all. They just -- they are taking data off of the regulated OBD port output and then taking it away.

And so we are seeing more of that and

there will be more to come.

MR. BANKS: That's really interesting. To a related question that I have on that point is, your perspectives, Yoshi in particular, open versus closed systems. So systems that actually allow or encourage app developers or non-OEM parties to contribute, either applications or collect data from the devices, as opposed to completely closed proprietary systems that restrict access.

Are there benefits to one approach or the other or does one provide more security or more protection? Can you just sort of talk about what those issues are?

MR. KOHNO: Okay, my name was called out, so I guess I might as well be the person to reply.

I think there are benefits, you know advantages and disadvantages, of both open and closed models. And I honestly don't know what is the right solution in each individual case without looking at it in more depth. I know that computer security researchers often times talk about the risks with closed systems, being that, you know, if they are using proprietary security mechanisms, maybe there is no way for the public to really know are these security methods secure or not.

And you know, there are also risks with open systems, in the sense that it gives people more liberty to actually inject code into the system. And there's been indications of trojan or malicious behavior being injected into open systems.

So I don't know if I have a, you know, one is right and one is wrong answer, but I do believe there are trade-offs in both directions.

MR. WOLF: Yoshi, is that also a risk with access to data in open systems? So if the consumer is given access to the data, is there a security risk there?

MR. KOHNO: Consumers getting access to the data, I think that opens another set of issues that we haven't really talked too much about, but whose data does the system belong to?

So I'm thinking about some of these applications where, you know, it might be kind of profiling information about the driver, but the interesting thing to me about the driver is that there might actually be multiple people who legitimately drive the car. And so does -- how do we actually know whose data belongs to whom?

MR. POWELL: I think one thing we need to be careful of when we say open versus closed, we probably should be defining that a little more carefully.

Related to security itself, in the case of Toyota, we use closed systems in the sense of the way we -- we don't expose them to third-party developers. However, we don't use closed security standards. We are using open security standards that have been peer reviewed and are fully scrubbed in the space to make sure we are the most robust we can be there.

So when we say closed systems, what we are talking about is closed development systems and closed software systems that have some more modicum of control to them. It's certainly no panacea, it's not a guarantee, but it's just another layer in the layer of defenses that we have. Obviously, the benefit to that is we have another layer. The downside, of course, is it can stifle innovation. We don't open up -- I mean, Toyota is different from some of the other OEMs in we do not actively promote third-parties to, here's our APIs, come on in. You've got access to our car data, please develop around it. Toyota hasn't done that, partially because of this risk. Exposing this critical vehicle data, without knowing what people are going to do with it, or the ability to control what they do with it, we consider it as a risk. So at this time, we are choosing not to do that.

MR. BANKS: John, do you have any insight on what consumers have said they wanted, to any degree, as it relates to open or closed systems?

MR. NIELSEN: I think that open and closed is something that most consumers wouldn't fully understand. But what we looked at is, when you talk about choice, what can you do with the data? Can you repurpose it, do you have access to it?

I think, over a number of issues, motorists at large, AAA members, have made it pretty clear that they would like to have access, they'd like to have control over it and be able to determine how it's used, if it's used at all.

And I think that's an important -- as we think about where this moves in the future, not just today, it's very difficult to say what it will be, but the fact is that this device that the consumer owns is producing data from their use. And they should have some say it what happens and how it's used and where it goes and how it makes their life better.

So I think security is always an issue,

but choice is huge.

MR. WOLF: I think we are conflating some issues. I think John, I agree with you completely, if we are talking about sharing that data with third-parties in ways that the consumer might not expect contextually, or did not consent to either generally or expressly, but if you are talking about the combination of consumer data with the proprietary algorithm or systems, and so it really is combined with proprietary data as well as other motorists' data, I'm not sure we want to have a system where consumers have access to that, both for security reasons and also because of ownership and incentivization reasons.

MR. NIELSEN: I think that's a fine point. And you're right, so there is certainly proprietary software and intellectual property in a car. And that's clearly, from my perspective, the realm of the manufacturer.

But the data that is produced by how I use my car, I think, ultimately is mine and I should be able to determine what happens. And I agree, there is some benefit in anonymous data being used to track trends and so on, increase vehicle safety, and that's important.

MR. WOLF: And in fact, you don't want to give an incentive to de-anonymize or to keep the data identified, when the trend is very much towards privacy through anonymization in connected cars.

MR. NIELSEN: Well, I would still say the choice, ultimately the choice would come down to the consumer.

MS. JAGIELSKI: Well, I think that raises an interesting question. Because if we are talking about consumer data and who has access to the data, how do you provide information or notice and choice, or can you provide notice and choice to consumers in this space? That's part one of the question.

And part two of the question is, we are talking about cars. You know, we're not talking about, say, a smart phone that has, you know, a shelf-life of two to three years. We are talking about something that conceivably, in the case of fine automobiles like Toyota, could be on the road for 20 years, conceivably, or more and that can have multiple owners over time.

And if the data is being collected by "the car" yet nonetheless, could potentially have multiple owners over time, how do we deal with that? How do we deal with data about multiple users/owners? Not just simply, you know, drivers in the same family, for example. How do we do that? How do we provide the information to consumers so that they know what information of theirs is being collected and how it is being used?

MR. WOLF: So you are really asking two questions.

MS. JAGIELSKI: Yes.

MR. WOLF: One is how do we provide notice and choice generally in a connected car. And then what --

MS. JAGIELSKI: Or can we?

MR. WOLF: Or can we. And then the question of what do you do with multiple users. Well, we have multiple users of devices all the time, it's not just restricted to cars. And we don't typically put the burden on the manufacturer of the device, of a laptop or a desktop or even a mobile device, to find out who is using it at that particular time. There really is a consumer responsibility to protect their own data and also to inform other users. That's why we often see, when we are on websites, if you are at a public computer, don't save your password on this computer.

So we need to think hard before we impose an obligation on the creator of the equipment, or even the provider of the service, to anticipate who various users might be. I don't think it's an easy question. I understand the concern.

MS. JAGIELSKI: Yeah, but cars are different though, aren't they, John?

MR. NIELSEN: I think maybe there is two ways to look at it. So right, the cars are tremendously complex. The most basic function is typically monitored. Almost everything that the car does is controlled by a computer, but that's a lot of data that really has almost no value to a third party. If you drove your car one way, I'd really not have any purpose, couldn't make any value out of that data.

What I could do is the contacts that are in your phone often populate into the dash, so the ability to clear that out is important. I think the data the car produces is probably not the concern, when you think of reselling a car.

The services that go along with that, so what data has been captured off of the vehicle, I think, is the one that needs to be addressed. And typically, your service would change with a change in ownership, so you'd have to have a new contract.

But I don't think the car produces so much -- it certainly doesn't store so much over a period of time, that a consumer should be really concerned about what's happening.

MR. WOLF: But to answer your first question on notice and choice, we have to remember that some of these systems don't have screens. The head-ins are simply devices with a button to allow you to call for emergency assistance or will detect when there is an emergency.

So we are so used to notice and choice in a world of screens, whether they are big or small. And also, I'm not sure we can port over directly what we are used to with respect to multiple devices, which is when we try to do a new app or it is about to engage in a new function, it pops up a screen and it says, would you like us to collect your data, yes/no. When you're going 60 miles an hour, it's not a good idea to have that screen pop up.

And so we're going to have to think about new ways to provide notice and choice and hope that, first of all, context will solve a lot of these issues, where there really isn't a need for those specific choices at the moment that the data is being collected.

MR. POWELL: If you want to -- regarding Toyota's feeling, Toyota's basic position is the consumer owns the data. That's the driving policy behind what we do. We collect very little information, either on the car or off-board. As John mentioned, it's not that -- it's not as rich as many people may think.

But having said that, we have very clear opt-in standards at the time the consumer buys the car. Plain language and multiple choices of levels where they can opt-in or opt-out. We do -- you don't want to be putting up, is it okay to use my position, while you're driving in the car, while you're driving down the road in the car, but we do offer a very clear way for people to opt-out if they choose to, in a very simple, easy-to-understand way.

When the car is sold to the next person, any off-board data from that car, as soon as the owner closes out those accounts, either their Entune account or their Inform account or any of those telematics or infotainment-based off-board systems, as soon as the accounts are closed, the data is gone. It cannot be retrieved. The devices, in the case of the modem in the car, the modem is shut-off and we cannot turn that modem back on unless the owner of the car, the new owner of the car, takes physical action to do it. We can't wake a car up remotely. Once a car is asleep, it cannot be woken remotely --

MS. JAGIELSKI: Yoshi probably could wake it.

MR. KOHNO: I don't know. It all depends on different manufacturers. I don't want to say anything about Toyotas, but --

I think Karen's question is very interesting. And I don't have an answer, but I liked all of the stuff that I heard the other panelists say.

A few things that I want to chime in on. You know, there are some comparisons between, you know, apps on the car and apps on the phone. I think it is important to note that maybe what we have for the phone isn't actually the right thing, even for the phone. You know, there's actually a lot of research that's been going on today at, like, what's the right way to handle notice and consent on the phone. And so maybe we need something different for a car, but we shouldn't begin by the assumption that the phone is actually the right strategy.

I would also say that it is very interesting to hear what happens when a car is sold. You know, I think that there are a lot of challenges in this space. I think all of the panelists realize that there are these challenges. You know, a new owner, renting a car, you know having someone else's child -- you know, someone else drive the car. These are all very interesting challenges.

And just to kind of point you to the complexity of this space, I will mention that there are apps that you can buy to download on your spouse's phone so you can track them. And so, you know, there is the potential for trying to figure out -- there is potential risk and also opportunities to try to address those risks.

And then lastly I would say that, and I forget the exact details of the study, so I'm sorry I'm not going to be able to quote it, but even very minimal driving data, you know, basically data about how you are maneuvering the car, it is possible to learn things like, you know, is this person an aggressive driver, a passive driver, and this and that. And whether sharing that information is a risk, I don't know, but there is a lot of potential uses for data that we may not think of off of the top of our head.

MS. JAGIELSKI: Okay, we're going to -- because we are running out of time here, we are going to move to -- because we have questions, although a couple of them I can't read the handwriting, so we'll do our best. We'll do our best.

Okay, so the first question is for Yoshi. What is the number one security issue you think the industry needs to address? Only one.

MR. KOHNO: I would say that the number one security issue the industry needs to address is awareness early on in the design cycle of a technology. And by that, I mean going back to the very beginning where you are figuring out the requirements for the technology, what are the potential issues and how can we mitigate them?

And maybe this is an opportunity to say that we actually developed a tool kit, a security and privacy threat discovery cards, that we designed to help people who are not computer security experts, brainstorm about consumer security threats, and they are available outside if you want one.

MS. JAGIELSKI: Yes, there are several available outside if you want them, generously donated by Yoshi.

MR. BANKS: One thing you didn't mention Yoshi, what about guidelines from the FTC? Do you think there would be useful security guidelines or to what degree?

MR. KOHNO: That's a good question and I would say that I probably shouldn't answer that for a number of reasons.

One is that I'm not a legal expert and a policy expert and so on, but I would love to have that conversation some other time.

MR. BANKS: That was a general question for the panel, so anybody that has perspective about it.

MR. WOLF: Well, I think the FTC has done a pretty good job at not prescribing prescriptive security suggestions for particular technologies because technologies change so quickly.

Obviously, the process recommendations that the FTC makes and its enforcement actions that identifies insufficiencies in the application of security steps serves an incredibly useful purpose, but I would not like to see the mission of the FTC to become the granular technology prescriber.

MR. NIELSEN: I think it's fantastic that the FTC is engaging with this topic now. It's early in the process and I think, just understanding what's happening and monitoring it as it develops, it will become increasingly apparent what needs to be done, if anything, in the future. So I think it's just -- this is a great first step to start understanding what is and what could be.

MR. POWELL: I guess to just add, I think we prefer any kind of self-regulation or this kind of discussion, open discussion, with all players.

And just as a reminder from my previous comment. If we are going to do this, we really should venture to open it up to the entire space of people who are in the automobile industry. Not just the carmakers themselves, but all of the people who are playing in this space.

MR. WOLF: This week in Los Angeles at the L.A. Auto Show, they actually had a hack-a-thon where they came up with these new privacy and security-enhancing technologies. I saw a couple of blogs reporting on them today, so we should all take a look at what they came up with. I think they announced them today at noon time.

MS. JAGIELSKI: Another question asked if the panelists can note areas that are unique to connected cars from any other connection. So what is unique about the connections involving automobiles as opposed to other kinds of connections?

MR. POWELL: Well --

MS. JAGIELSKI: If any. The answer could be none.

MR. WOLF: They move very, very fast.

MR. POWELL: There is, of course, a lot of similarity. I mean, the risks of data use -- of exposure of data and misuse of data. That's, I think, pretty common.

The fact that it is an automobile moving down the road, it's working in a riskier environment.

John mentioned the issue of distraction. The one thing that is very clear is that, one of the biggest problems with bringing in all of this technology, the real world applications and the studies that other people like AAA have done and we've seen as well is that the level of distraction that these features bring to the car is extraordinary. It's an order of magnitude more distracting to deal with some of these in a suboptimal way, like on a phone, than for tuning your radio or even eating in the car.

So we think that the distracted driving element of it is probably a really unique domain space that we absolutely have to address. And we can't just separate it from the -- we're not talking about data security, but we have a responsibility, if you will, to provide the right information, limiting it to the right uses, to make drivers more aware and not more distracted.

MR. WOLF: But I will say that, on that point, you see a lot of innovation and experimentation going on. I remember a couple of years ago when technology first started in the car -- dials that you had to look at, interactions on the screen. And one car I owned it took like five steps to change the radio station with this dial.

And now you're seeing -- I kind of joked a couple of years ago when I spoke at the North American Auto Show, I had a picture of an iPad strapped to a steering wheel. And the guy from NTSA was furiously taking notes and I said, this is just a joke. Well, it's not a joke. And in fact, big screens actually may be safer because the icons are bigger, it's easier to interact with it more quickly, and it just may be a better interface. And we are seeing experimentation that I think could be useful in that issue.

MR. NIELSEN: Just to build on that, coming back to what's different, first off, I think when you talk about a cell phone, most consumers know, it's asking you all the time, do you want to share my location? Can I do this? I'm not sure that consumer awareness is nearly as high with the capabilities of the car and what can be done with it. So I think that's a difference.

And then I think secondly, it's the automobile and there's a different passion around the car than there is for a cell phone or another device. And when you think that somebody could know how fast you're driving or what you're doing, where you are, typically the car represents some freedom, and that can be quickly compromised with technology. So I think that's a huge difference.

MR. BANKS: Are there any significant issues related to updates? So I think Chris, you mentioned the ability to update vehicles remotely, but there's an expectation of lifespan for, say, cell phones and laptops that I think is different at least. I have a car that was from like '87, so --

MR. WOLF: You need to update it.

MR. BANKS: I need to update the car. So when there are expectations for a long-lasting ownership, are there any unique issues about maintaining support for the onboard systems, in that case?

MR. POWELL: I guess that would be me.

Well, we certainly know how to do it. It's not a new idea or a new concept. The question is, what are the benefits versus the risks. And where we are right now is we are very -- we don't do over-the-air updates to most of our systems. Our Entune apps, we can push apps, you know -- to a phone, which is more an interaction with the infotainment system, but we don't currently do over-the-air software updates. We can, but we choose not to at this time because we really don't think it's well understood. I mean, to the point that five or ten years from now, that car that we built tomorrow is going to be out there, and perhaps it is outdated in its ability to -- you know, we don't want people attacking ten year old cars either, not just the new ones. So it's an area we need to proceed with caution on.

MS. JAGIELSKI: So in terms of -- so for something -- when you have a vehicle that can last

10, 15, 20 years, how do you ensure that data is updated? I mean, is that something that would require, you know, the person would have to go to their dealer or to an auto repair shop? Because if it's not getting pushed --

MR. POWELL: Well, what we do now is, either through a dealer portal update or, for example, making a USB-type dongle, a USB-stick available, but that is mostly limited infotainment systems. Critical systems are all done at the dealer, updates are all done at the dealer.

MS. JAGIELSKI: Which brings me --

MR. WOLF: Since February, I've had I think five updates. And the one that they announced today was the first safety-related update. This --

MR. POWELL: Well, this was not a Toyota.

MR. WOLF: Not a Toyota. All of the others were convenience and enhancement-related.

MS. JAGIELSKI: Well, I drive a stick, so you know, anyway.

But this leads into one of the questions, which is auto manufacturers can download data from cars during maintenance visits. What kinds of privacy protections should be applied to this data? So maybe we need to clarify, when you do visit your dealer and you are getting these updates, what kind of information are they collecting?

MR. NIELSEN: Maybe I can touch on that. So the data -- when you think of going to get your vehicle serviced, first off, if you are going in because the light is on, it's telling you something is wrong and you want to get that fixed.

What the data -- it doesn't keep a record of what you did this week. Most of the data is pretty volatile and it only saves it in terms of what turned on the light. So what's the throttle position sensor and a mass overflow sensor, that's really not very exciting data. Well, maybe to me, but that's me.

So really what you're talking about is really a diagnostic. And this --

MR. WOLF: It's not a record of everywhere you've been and how fast you've driven.

MR. NIELSEN: Yeah. Most everything is volatile and tracks out in 30 or 40 seconds.

MS. JAGIELSKI: Okay. Oh --

MR. BANKS: No, no. I was actually going to say that I think we are running out of time, so I guess with the last few minutes that we have, we can give each panelist an opportunity to share a parting thought that they think is really important about this area. So you're first, Yoshi.

MR. KOHNO: Okay, I don't have much time to think.

I think that parting thoughts are, continue to enjoy the automobiles that you have, but at the same time, again, I think my parting thought is that for everyone who is thinking about a future technology, whether it is the next generation automobile, the next generation medical device, the next generation home or whatever, trying to think about security and privacy issues proactively. It's probably a lot better for everyone in the long run.

MR. WOLF: So I just recommend that people take a look at the FPF paper on it, the Updated Privacy Paradigm, because we do need to think about FIPPs in new ways when we are dealing with technologies like the connected car.

Mr. NIELSEN: I think just what we've talked about today is how exciting the automotive industry is, what's changing, and I think just having these dialogues are critical and I really applaud the opportunity to talk about this and look forward to continuing the conversations in the future.

MR. POWELL: Thank you for having us. I think that, in addition to what these guys said, from Toyota's point of view, the number one item, the number one thing we have is the trust of our consumers. And we are not going to do thing to violate that trust.

MS. JAGIELSKI: Well, thank you very much. There's going to be a very quick change here, so don't move.

PANEL FOUR: Privacy and Security in a Connected World

MR. DAVIDSON: Hello, I'm Ben Davidson, an attorney with the Division of Marketing Practices and with me is Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection.

Our fourth panel today is going to focus on the broader privacy and security issues raised by the Internet of Things. It's going to be structured as a discussion around a series of scenarios that Maneesha and I will raise.

Before we start, I want to introduce our panelists. To my left is Ryan Calo. He is an Assistant Professor of Law at the University of Washington. Ryan has done research on the intersection of law and emerging technology.

Next to him is Dan Caprio, the Senior Strategic Advisor and Independent Consultant for McKenna, Long & Aldridge. Dan has served as a subject matter expert to the European Commission Expert Group on the Internet of Things and advises on the Transatlantic Computing Continuum policy.

Next to Dan is Michelle Chibba, who oversees the Policy Department and Special Projects at the Office of Information and Privacy Commissioner of Ontario. Her office conducts research and analysis to support the Commissioner's rule in proactively addressing privacy issues affecting the public.

Next is Drew Hickerson, the Assistant General Counsel and Senior Director of Business development at Happtique, a mobile solutions company that aims to help patients and providers integrate mobile health into clinical care and daily life. Happtique has a program that will review and certify health apps that comply with standards for privacy and security that Happtique has designed.

Next to him, David Jacobs is the Consumer Protection Counsel at the Electronic Privacy Information Center. David focuses on representing consumers' privacy interests before Congress, in the courts, and federal agencies.

Finally, last is Marc Rogers, who is the Principal Security Researcher at Lookout, Inc., a mobile security company. Marc's core expertise is as a whitehat hacker, who alert and publish security issues and communicates them to consumers and the industry in a responsible way. Marc has recently hacked Apple's Touch ID and also Google Glass.

So let's get started with our first scenario. Sue is tech savvy and has always been interested in new gadgets. In her home, she has several interconnected devices like a smart oven, smart lights, smart thermostat, and a smart alarm system. She enjoys the convenience that these devices, but she is frustrated at having separate controls for each device, so she decides to come up with a single system that can integrate these devices and add controls.

She decides to run the -- sorry about that. Sue's innovation is to use a single smart phone app to control all of the smart devices in her home. Sue will be able to automatically lock and unlock her front door, turn on and off her alarm system as she approaches, and control the lights in her bedroom so that they turn on before her alarm wakes her up.

We'll start with Michelle. At what stage should Sue start thinking about privacy issues?

MS. CHIBBA: Well, first of all, thank you for being, you know, the Ontario visitor here in the U.S. And I'm here because of my Commissioner, who is a regulator -- she is the Information and Privacy Commissioner of Ontario, Toronto. And it's not because of Rob Ford.

But I'm going to say, I'm going to say

that Sue knows that privacy is good for her business. And she also knows about the privacy by design principles, which is really taking a proactive, sort of privacy by default approach to any kind of technology that involves personally identifiable information.

So when is she supposed to be starting? She is going to be really smart and savvy, so she is going to say, gee, these technologies collect personally identifiable information. So as soon as she conceives of this concept, right, this idea, she is going to start thinking about how can I protect that data without the consumer having to do a lot of heavy lifting.

MR. DAVIDSON: And what should that process look like, more specifically? David, what do you think?

MR. JACOBS: Yeah. Well, I'll echo a lot of what Michelle said. You know, I think she's, in general terms, just thinking about what data do I need to collect, how is it going to be used, and what third parties, if any, is it going to be shared with.

And you know, there are various ways to break it down. Maybe she thinks about, you know, front end versus back end. Am I using any sort of anonymization or data minimization techniques? What is the interface going to look like? Those kinds of issues.

MR. DAVIDSON: And Marc, what should she be thinking about security issues, from the outside?

MR. JACOBS: So the important thing when designing a connected thing is that security has to be baked into it from the very beginning.

What I'm finding in breaking things is that generally they fall into two camps. That is, things that are designed by people who are aware of the kinds of flaws you would find on the internet, in which case they have a robust design and they address most of the issues and they are quite forward-thinking in terms of what issues you are likely to encounter that haven't cropped up yet.

And companies that haven't got the experience, that are coming perhaps from a different industry where they maybe, for example, a medical device manufacturer, where they are aware of the issues that you would encounter in the medical device, but are not aware of the issues that they will encounter as an internet thing. And as a result, they miss a lot of the issues.

And so understanding these issues and looking to expertise and looking to best practice is really important. Because one of the most important things about the Internet of Things is, there are a lot of things on the internet and many of the issues that we're seeing have been sought before. So the lessons are out there, we just need to guide these companies towards those answers.

MR. DAVIDSON: Drew, who should Sue hire in her company?

MR. HICKERSON: So I know that Sue is a tech savvy individual, but we don't know if she is a technologist by trade. I think it's important that she engages someone who understands the technological ramifications, in terms of how that may implicate or impact her business model or strategy.

So to give you an example, she needs to figure out how she plans to monetize her application, her product, over time. So how does she build that into her application, in terms of say, for instance, she wants a freemium model and that freemium model incorporates an ad network. Well, she is going to want to have an outside consultant, counsel, security architect, come in with the right sort of structure, in terms of how she builds or designs her product so that she's not left retrofitting it after the fact.

MR. DAVIDSON: And Dan, how is this process different since she is making an interconnected device, versus saying making say a restaurant recommendation app or a weather app?

MR. CAPRIO: First of all, I'd like to thank you for having me, to the FTC to holding the workshop and thank you for inviting me to participate.

I think this is a good example to sort of begin, as was said earlier, to bake privacy and security in. But in addition to that, to think about, you know, what we connect to the internet and why, sort of as a general principle.

And then the other, you know, general principle that applies here is that there is no such thing as perfect security. She's, in this example, I mean -- with the Internet of Things, it's a transformative technology. Really, the future of the internet itself. And so her challenge is how to protect privacy and security and still enable innovation in a practical way.

That being said, there are a lot of

guidelines for applications that she could follow and that, you know, she needs to think this through from the beginning and get the security right at the outset.

MS. MITHAL: Can I just follow-up? I think Drew and Marc both raised the idea that she may be tech savvy, but she may not have the right technical expertise. And there was discussion about the fact that she should hire a security expert or might want to hire somebody who knows about ad networks and that sort of thing.

So I guess I'd like the panelists to discuss a little bit more about the costs and the benefits. So are you saying that it depends on the sensitivity of the data? Are we saying that, you know, in all events Sue can't just go out there and put up a shingle, so to speak, in the virtual world and do this herself? Does anybody have any thoughts on that?

And I was also going to say, you know, for the questions that we are addressing to all of the panelists, you might just raise your name tent if you would like to answer.

MS. CHIBBA: Can I answer?

MS. MITHAL: Yes.

MS. CHIBBA: So we did, in reality, we recently published a paper for smart meter app developers. And what we found was that this space, much like, you know, you heard it raised in earlier panels, much of this space, they are not sophisticated, huge corporations with large IT departments or even a chief privacy officer, right? They are small, independent, maybe one or two individuals.

And so for us, for our office, one of the sort of -- the M.O. that we operate on are the three Cs. We do a lot of communication, collaboration and consultation. So we really started to target the small and medium-sized organization to sort of put out some essential guidance for app developers.

So some of these things were things like, you know, don't -- if you don't need the data, then don't collect it. So we call that data minimization, right?

Is there a way to pseudonymize or anonymize the data? Give the individual the choice, in terms of whether to have the GPS feature on or off, right? Retain as much of the data on the device as possible, in terms of control. Don't use a single ID as a default, if you can stop it from being persistent. You know, being much more dynamic.

So it's these small things that will help these individuals. There are a lot of resources out there as well, in terms of what we call a privacy impact assessment. There are some simple, basic questions that a developer or an owner of an organization can ask themselves and go through a series of questions.

They can also get companies to do a threat-risk assessment. That's much more on the security side that Marc and David and Drew could probably talk about.

MS. MITHAL: I think Ryan and then Dan and then Marc.

MR. CALO: So thanks so much for having me. Actually, having two people from the University of Washington in successive panels, we appreciate the other Washington for expertise and so forth. And I am especially happy to being among so many interesting and great panels.

Somehow Joe Hall was able to favorite one of my tweets while he was on the panel, which I thought was particularly amazing. I don't know how he did that. I didn't see you do it.

So I would say that we want to start even earlier, I'm going to out Privacy by Design, you know, right --

MS. CHIBBA: Yay!

MR. CALO: I think the place to start thinking about privacy is when you are thinking about your business model, right?

So I spent some time in China a couple of years ago. I went on behalf of a delegation for Stanford Law School and I gave my usual speil about this is how we do privacy and this is what matters. This is conflict between innovation on the one hand and people's privacy on the other and I got a lot of sort of blank looks. And I don't think it was the very good translator, right?

And so when I talked to some folks about it from the industry there they were like, well, you know, look, we don't really face this problem in this way. And I said, well, what do you mean you don't face the problem this way? And they said, well, because all of our stuff is fee-based, you know what I mean? So we don't try to monetize people's data in ways that they wouldn't anticipate.

Now, China has other problems, right? But they didn't -- at least these companies I spoke to didn't perceive that essential conflict. So I think what Sue should be asking herself is this. What am I doing? What am I selling? Am I selling something that just joins a bunch of devices together and customers pay me money and I serve the customer this way? Or am I building a data engine that clever people can then later monetize? Because that's going to drive so much else in terms of decisions on whether to put in on the client, in the cloud, who to bring in and when, and so forth.

And so I just wanted to argue that the life cycle starts at your business plan.

MS. MITHAL: Dan?

MR. CAPRIO: I just wanted to add a quick point related to security or Sue's problem and that's there's so much innovation and it's low cost. Michelle mentioned some of the ways that Sue could secure that data and that reasonable data security doesn't need to break the bank.

I mean, we've talked all day about context and I think context is important. And I agree with Ryan, she needs to think of it at the inception, to bake it in.

But there are certainly tools and technologies that she should keep in mind, you know, that might not cost an arm and a leg.

MS. MITHAL: Marc and then Drew and then David.

MR. ROGERS: I think it's important also to note that there are two other things driving this and that's that innovation isn't just in the product space. There's innovation in the attack space as well. The threat landscape is not static, it moves very quickly. And when we connect things, we fundamentally change their value to some of these aggressors.

Take for example a thermostat. A thermostat on the wall has very little value, the only real security you can think about is physical, to make sure maybe your kid doesn't turn off the temperature in your house.

But on the other hand, a connected thermostat is something of a device that can provide intel of what's going on inside your house, when your house is empty and, if harnessed into a large community of things, can even be used as a weapon to attack critical infrastructure.

So it's a full-time job to really keep on top of all of this stuff. And so for a small company, it may be much more economic to turn to an expert in the field, a security company, to provide them with guidance, expertise and assessments to ensure that they are doing the right thing. However, there should always be someone in the organization who is responsible for ensuring that that happens and they look after the business side of it.

MR. HICKERSON: I think the biggest issue is education. So to date, we have extremely innovative, bright, sophisticated technologists, but when it comes to the regulatory regime in which they are developing technology, they are not necessarily up to speed. They don't know what the ramifications are. And their whole idea is to build it now, collect as much data as possible, and then worry about those issues later.

But fortunately, I think we are seeing a lot of start-up incubators provide education. You know, they are having sorts of folks, you know, spend their time, attorneys, privacy security experts, come in and educate these folks early on so they're not left, after the fact, worrying about how to fix the solution, you know, post hoc.

MR. DAVIDSON: So another question for you Drew. Sue sets up her system and she is trying to decide which smart devices in the home she wants to make compatible with her system. How much should she know about those devices and their data collection and their security? And how can she go about figuring that out?

MR. HICKERSON: Sure. So I think first and foremost she needs to now what platforms are they running on, what devices are they intending to integrate or reside on. She needs to know what market she wants to essential market her solution for. Is it strictly for the U.S. or does she eventually want to scale and go international?

She needs to know, are these devices utilizing IOS are they using Android? Are they building HTML5? She needs to know what sort of user experience, user interface that she wants to essentially offer to her customers.

She also needs to know, are they utilizing open source or proprietary APIs? How are they storing that data? What sort of security policies, procedures, and protocols are they currently leveraging? Do they have privacy policies in place? Are they accurate? Do they actually reflect the policies that are being instituted through the application?

She needs to know whether or not those applications are collecting sensitive information. If any of the information is health-related, is HIPAA involved? Are any of the devices she's thinking about connecting to medical devices? Because by virtue of her connecting to an existing regulated medical device, you know, she essentially then becomes subject, under the recent FDA guidance proposed in the final guidance as a mobile medical application.

So there are certain ramifications in that area, so she needs to do her due diligence on the applications and devices that she wants to connect to. Because it then essentially creates a chain in her own infrastructure.

MR. DAVIDSON: Another question for Dan. Sue decides that the cost of securing the data transmitted by her product exceeds her budget. What does she do? What are her options?

MR. CAPRIO: I was trying to get at that earlier. I think she looks for resources, as I said, that are sort of online or sort of existing best practices that are considered innovative. I mean, security can be very, very expensive. You can spend a lot on it, depending on your context awareness, but it doesn't have to necessarily, you know, break the bank or break the business model.

She still has to figure out a way, even if she is over budget, she has to figure out a way to secure it and I think there are resources available that she could take advantage of.

MR. DAVIDSON: Michelle.

MS. CHIBBA: I can tell you that our Commissioner is cochairing a technical committee under OASIS and it's sole purpose is to look at ways to translate the Privacy by Design principles into technical requirements.

But more than that, it's looking at what kind of documentation can software engineers -- what should the standard be for that documentation to do exactly that? To be able to document, and if they have a breach, to be able to go in front of a regulator to say yes, we made this business decision for this reason and to take that accountability.

So that's what I would suggest Sue would have to do. She better make a good business case as to why she made that trade-off.

MR. DAVIDSON: And Marc.

MR. ROGERS: I just to go on to say that I struggle to see how that element of security would end up costing a lot of money. I think if it is designed right, it doesn't have to cost a lot of money. They are plenty of open standards out there that can be adopted that will allow this to work well.

And that ultimately the cost of not doing it right could end up being far more serious to the business when she has a breach or when she ends up with a massive loss of trust in confidence because customer data is suddenly out in the wind.

MS. MITHAL: Actually, I think that leads to a follow-up question, which is something that was eluded to in earlier panels about incentives.

So I think, you know, as Sue is creating her product, you know, she is looking at selling it to the public and she wants to show them that it can do all the nifty things that she says it can do. And I think people said before, you know, consumers don't really have a window into security. They don't -- security is not one of the bases on which they may buy a product.

And so how do we get the incentives right? How do we make sure that Sue has the incentives to bake security into her product, even though consumers aren't necessarily clamoring for it?

MR. CALO: I can -- do you want me to go ahead?

MR. CAPRIO: Go ahead.

MR. CALO: I don't know how to do this. If you don't do this? Okay.

MS. MITHAL: It's easier for us.

MR. CALO: I'm talking. I'm talking right now.

All right, so I think that we are overstating a little bit the risk to Sue, right? So I'm not your attorney and if you are a start-up don't cite to what I just said to, you know, I'm not even licensed to practice. Actually, I am. I'm barred in D.C., it turns out, but anyway. I'm not your lawyer.

But Sue doesn't have to worry about this yet. If you look at the FTC enforcement pattern, it is very clear that the FTC really waits for awhile until you have a lot of customers before it starts to kick the tires on your security. And properly so, right?

So if you look at the consent decrees around security, I mean a lot of them, not every single one, pretty sophisticated companies that have grown to a size where the FTC looks at it and says, you know, look. Shame on you for having this many people and not doing it, right?

So let's not -- I mean, I think that if you get those structures in place early, if you think about your business model, you are going to be well-positioned, right, to efficiently move to a proportionate security amount when it comes time to.

And a related answer to your question about what do we do about consumers and security, security is something that the FTC, I think, is doing a really good job on, right? I mean, if you don't have adequate security, irrespective of whether you represented it in a way, the FTC, at one point, is going to have some scrutiny against you. And that's something that I think we do really well. I mean, that's just my own view.

MS. MITHAL: Okay, David and then Marc and then Michelle and then we'll move on to the next scenario.

MR. JACOBS: You know, I also think that FTC enforcement and enforcement by the state AGs is also a great incentivizer. And now it's not just big companies that the FTC looks at, I think really small companies that are doing egregious, engaged in egregious misconduct -- I don't think Sue falls into this, but that's another case.

MR. ROGERS: I don't think fear of regulation should be the only incentive here. There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence.

And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they've done well. And they've gone on to push out products where there have been no issues. Those companies are always going to do better than the companies fail to deliver what consumers want, because consumers are very good at voting with their feet. And I would argue that that's potentially more damaging to a company than any fine a regulator can draw.

MS. MITHAL: Michelle.

MS. CHIBBA: Yeah, I was going to -- I mean, it's along the same line. There was a survey recently by a trustee that said, you know, I've always talked about governments, where individuals are required to give their personal data to governments, and therefore governments tend to be more conservative, in terms of their approach, right, as custodians.

But in terms of business, they actually said that 89 percent of individuals will go to another business right away if they do not feel comfortable or have any trust in that company's ability to protect their data. So that's a telling figure.

I think the other one is, the average citizen understands ID theft. I think each one of us has probably had one incident where either our online banking had been hacked or whatever, right? And so the average citizen will know about security.

And so what we say to businesses, use that as your competitive advantage. Whether it's your security policy or your privacy stance, use it as a competitive advantage. Get out there as a leader of the pack and do that.

MS. MITHAL: I am going to just ask one last question on this scenario. And Ben eluded to this earlier, so let's say you are advising Sue on building and privacy of data security. Is your advice to Sue different from what it would be to a company that is creating a restaurant app or a weather app? What about the connectiveness makes this unique?

MR. ROGERS: I think the connectiveness just changes sort of the things that need to be looked at. Security needs to be taken seriously across the board for all applications. Obviously, the more intimate the application, the greater impact it can have on a consumer, so maybe the more vigilant it needs to be.

But one of the other things that people sometimes forget to take into account is that there can be unforeseen effects from things. A good example, I think, is the IP-connected lightbulb. People stated earlier in this conference that perhaps the only concern that people should be concerned about with IP-connected lightbulb is that you may be a victim of a drive-by attack when someone comes by and turns your lights on and off.

But I would argue that there are other potential effects that could take place that you may not have even thought about. For example, what if the lightbulb gets used with millions of other lightbulbs to attack something else?

So don't underestimate what could be done with your app, no matter how simple you think it is.

Security should be taken seriously, right from the get go.

MS. MITHAL: Thank you. Why don't we move on to the next scenario. Ben will put that up on the screen.

So here's the scenario. Now we have Jane. She wants to start training for a marathon and she learns about a new watch that can automate her training. The watch can connect to Jane's online calendar to schedule times for runs, calibrate an optimal training program based on Jane's heart rate, recommend particular running routes, based on other runners' patterns, and design a course that will simulate the marathon Jane is going to run.

The watch also contains some optitional features like automatically posting Jane's progress on her social network, helping Jane find other people to run with, and even offering Jane discounts on her medical insurance based on her improved health.

So the watch is advertised as "a connected watch to help you train for a marathon." The package insert contains terms and conditions, which includes product specifications and functionality information. And the terms and conditions say nothing specifically about data collection and sharing.

Okay, so let's take the simple scenario where it is just a one-to-one sharing. So Jane is using the watch, it transmits data back to the manufacturer and it helps her improve her running times and her, you know, run courses and so forth.

So the first question is, does the advertisement -- this is a connected watch to help you train for a marathon, does that advertisement put Jane on notice as to whether the watch manufacturer will obtain her personal information?

So why don't we start with Ryan.

MR. CALO: Okay. So it's a truism about American privacy laws that a lot of it has to do with notice and choice, right? We all know that, everybody in this room understands that.

And you know what I like to say about notice as a regulatory mechanism is sort of like what Winston Churchill said about democracy, right? So notice is the worst form of regulation, except for all of the alternatives. I thought I'd get more of a laugh out of that. Are you with me?

MR. CAPRIO: I'm feeling you.

MR. CALO: Dan's feeling me and I'm so

glad to have his energy next to me.

So the point of the matter is that, you know, think about this, right? Think about the fact that there are people in this room, at least one I know for a fact, has a device that we learned earlier allows a blind person, who speaks English, to communicate with a German-speaking person. That's the state of the technology we are dealing with today. And yet, we are using Gutenberg-era communications for terms of service and privacy policies. That disconnect is so profound that it has led to just an avalanche of commentary. And everybody knows that no one reads privacy policies or terms of service et cetera, et cetera, et cetera.

So do we abandon notice though? This best/worst thing? I mean, we don't. I think we need to innovate around notice. We need to drag notice into the 21st century finally. And I think that the Internet of Things, interestingly, is a forcing mechanism. Because it doesn't have that screen that can sort of allow you to lazily just lay out what California law requires you to do about what you are collecting and so forth.

So ideas include things like having some standardization so that Jane's device permits you to understand, not just what data is being collected, but how it is being shared. I can get into some examples of how we might do notice better. And if you're interested, I have an article about this called "Against Notice Skepticism."

So I do think that there is some role for the very experience of the watch to put you on notice of something, I think that's appropriate, and I think maybe that's what's happened here, but I wouldn't just limit it to that. I think there is a real opportunity to do notice right, to do it well.

I mean, Facebook organizes information, a lot of information, for a living. That's what they do for a living, right? Like, we need to innovate around privacy notices the way that we do around the other products.

MS. MITHAL: So I think, Ryan, we started with the simple scenario where it is just the one-to-one between the consumer and the manufacturer. And I think you eluded to the fact that, you know, maybe the watch itself is enough to communicate that one-to-one value proposition.

But let's say that -- let's complicate the scenario a little bit and say that the watch manufacturer starts, you know, selling your data for advertising purposes. So we all agree that the terms and conditions may not be the best approach for, you know, putting that disclosure in.

We know from the Future of Privacy Forum paper and from a lot of what has been discussed here is that the watch has too small of a screen to be able to provide that disclosure.

So what should we do in the case where the watch manufacturer says, you can take this watch for free and I'm going to sell your data to a third-party, third-party advertisers? How does that get communicated to consumers? Is that something that is even appropriate? How should somebody go about doing that?

MR. CALO: Okay, so I'll quickly respond to that. So --

MS. MITHAL: I'm sure you have the answer.

MR. CALO: No, I'm going to give the answer, I mean, I just have a sort of frenetic way of talking about it.

So basically if you think about the thing that really, really bothers the privacy community, you can see this for instance in ethics comments about the, you know, the Internet of Things, right? It's when you do this bait-and-switch.

You say, I'm going to sell you OnStar and OnStar is going to help you when you are in trouble and tell you where to go and rescue you. And then all of the sudden, someone very clever says gosh, that's a lot of interesting data. We could monetize that data, right? And so then -- you're not really giving the consumer the gist of the transaction. I sell you this helpful thing for a money.

If what you do is you say look, this wristwatch, you are not going to pay a thing, we are going to use it to advertise, right? Well, fine. That doesn't create an essential problem. I don't see why consumers shouldn't be able -- smart enough to do that. Maybe you want to do an update, the thing blinks, and you go and you realize that you have a message and you go into your console and you see what the change might be. You know, creative thinking about that. That's a little long, but --

MS. MITHAL: And actually I wanted to turn to Michelle also because I know that, in Canada, the laws are somewhat different in terms of there is, you know, requirements for privacy policies and choice.

So maybe you would answer the first question differently. If it is a one-to-one relationship where it is just the manufacturer is getting the data and maybe using it to do first-party marketing back to the consumer, how would you think notice or choice should be made in that situation?

MS. CHIBBA: See, we go for control, the individual control of the data. So in Canada, it would be, you know, if the individual understands, right, buys the watch and understands that, you know, the manufacturer has to collect a certain amount of personal information, then that's fine. He or she has a choice whether or not they want to engage.

What we'd like though, however, is to say that if there are any, I guess, features built-in to the watch, right, that would perhaps enable the communication that, in fact, it shouldn't be the default is on. The default should be off, to enable the individual the choice to opt-in.

MS. MITHAL: Right. Marc.

MR. ROGERS: I just wanted to say this is actually a scenario where we already are running into some difficulties. Because if you take a look at some of the mobile advertisers and the kinds of data that they collect, it's very varied and, in some cases, incredibly intrusive.

And what we have found as an organization is that there is a lack of a code of conduct to tell them what they should do. And so we've been working quite heavily in this space, pushing out ground rules to say to advertisers, it's okay to collect this kind of information, but it's not okay to collect this kind of information.

And that, I think, helps. And so I think this needs to be a part of the Internet of Things as well. I think opt-in is important. I come from the U.K. and opt-in is an important part of the way the U.K. handles data protection.

The other thing is also to make sure the consumer understands what data is being collected. It's one thing to say that data is being collected, but it's another thing to say that actually we are collecting your telephone number, we are collecting your birthdate, we are collecting your sex. You have to be very clear about it so that they can understand what the implications of that data being shared are.

MS. MITHAL: You know, we keep using the term notice and choice, and I think that's slightly outdated. You know, we talked in our most recent privacy report about simplified choice and just-in-time choices. And I'm hearing that, you know, even that is complicated when you don't have a screen or you have a small screen.

So we've got a question from the audience. Is there a role for privacy security seals for IoT devices? And the questioner goes on to add, the proposed EU data protection regulation contemplates these seals in a big way.

So is there a role for this and is it ripe for this kind of innovation or self-regulation?

MS. CHIBBA: Well, I can answer from the smart meter, smart grid point of view and it is something that the industry, as well as the utilities, really called for.

You know, organizations are looking for a means to have some sort of a filtering process, some sort of an acknowledgment of an organization's privacy practices, so definitely.

In Europe, they have the particular seal and I think there is one through the trustee for smart meter organizations.

MS. MITHAL: Drew.

MR. HICKERSON: Sure. So I think it's very important to the consumer, and even to certain professionals, that they have a level of credibility and trustworthiness in the types of applications and devices that they are utilizing.

I think often times we associate, you know, high ratings and high reviews and high user adoption with trustworthiness or credibility. And I think there's a difference between user experience, and how susceptible someone is to adhere to any particular app, whether they like it or not, to actually a correlation in terms of how that app or how that app publisher or developer is actually handling the information that they are collecting, storing, transmitting, sharing. How much notice are they giving to the user? How much access to the user's information are they giving to the user? Things of that nature.

And I think there needs to be some sort of bar, so to speak, when it comes to these applications. And I think a seal is appropriate. I mean, that was essentially the impetus for my company's certification program, specifically with respect to health mobile applications.

Because quite frankly, providers and hospitals and patients wanted to use applications for purposes of the provision of care or to self-manage, but they just could not take a level of confidence in any given application. And I think they needed some sort of vetting and they knew the FDA was coming out with guidance; however, they knew it was only going to cover a small subset of the marketplace.

So roughly -- you know, the final guidance is actually even smaller than was anticipated and it probably will only cover less than 20 percent of the health care mobile application marketplace. And we are talking over 40,000 applications.

So you know, that's why we saw, from our customers, our physicians, our nurses, our providers and other health care entities, that they needed that level of confidence, which is exactly the reason why we concocted that program.

MS. MITHAL: Okay, Dan.

MR. CAPRIO: It's a good question and I think seals are certainly part of the solution. But I think we need to -- we've been talking about this all day, but maybe just take a step back when we think about the FIPPs. I mean, the FIPPs is a framework. And I think you heard, from the outset of the day where Chairwoman Ramirez talked about, you know, the need to adapt notice and choice.

And so I think it's important, as we have this discussion, that we recognize with the Internet of Things, I mean, we are at the beginning of the beginning. And we are seeing business, as we've heard all day, business models are rapidly evolving.

And I think part of our, you know, discussion today or sort of our work going forward is, what's the problem we are trying to solve and what do we need to do to solve it. And I think part of what we've talked about, that this is going to be the challenge, the recognition that, you know, consumers don't read privacy policies and that notice and choice is not working so well with the transformative technology, like the Internet of Things is, you know, to begin to think about moving away from siloed approaches around collection and start thinking about, you know, focusing more on use cases. Thinking in sort of real world harms and practical solutions.

And certainly I'm not advocating for abandoning the FIPPs, but instead we really need to rethink and update and evolve the FIPPs for greater emphasis and interpretation.

And just one quick data point I think Ryan mentioned, you know, industrial-era regulation. I mean, let's keep in mind that the FIPPs grew up in the seventies, you know, in an era of centralized data bases, you know, with a lot of structured data.

When I started at the FTC 15 years ago, it's hard to believe, but we actually measured -- we measured progress of how we were doing on the internet by surveying 100 websites. And you know, we really were -- it was, the internet back then was one-to-one, it was discrete, it wasn't transactional.

Today, you know, it's transactional, there are many layers, it's one-to-many social media, there is a lot of unstructured data and, you know, probably 50 or more different players. So it's much more complicated.

And I think, you know, the challenge or the opportunity going forward is to roll up our sleeves and to work together between industry, civil society, and government to be respectful of the FIPPs, but adapt, you know, into more of those -- and thinking through some of the use cases.

MS. MITHAL: So Dan, that was really interesting. I think there are a couple of things from your remarks, and I think they have echoed themes that we've heard throughout the day.

So we've heard, you know, some variation of, you know, the Fair Information Practice Principles are, you know, not dead but, you know, are dying, need to be adapted, not well-suited for this technology. We've also heard some people talk about the importance and relevance of a use-based model.

And I guess I just wanted to ask the panelists if they think that those two are fundamentally inconsistent. So one of the things that I'm hearing is, okay, when you have the one-to-one relationship, maybe the choice is kind of embedded in the transaction. When you have a relationship where you have the manufacturer sharing with third-party advertisers, well that choice needs to be a higher level.

So is it that we are doing away with concepts like choice in favor of use-based restrictions or are they compatible? Or is this semantics or do we need to think about this a different way? David.

MR. JACOBS: Well, I think there's compatibility there. I mean, the one thing about the FIPPs is that, you know, they're flexible and it's not just all about choice or notice or consent.

You have transparency and accountability and access and they've been part of the Fair Information Practices from the beginning.

And so, you know, I don't think you need to do away with the FIPPs, even if you emphasize transparency or access more. And certainly I think the Internet of Things gives you greater opportunity to do so, but you know, the FIPPs are still fundamentally sound.

MS. MITHAL: Michelle.

MS. CHIBBA: Yeah, I was going to say, and you know, coming from Ontario, Canada, I guess I can say this, but one of the things that we -- one of the exercises that we did when the Commissioner developed the seven Privacy by Design Principles, was to map it to the FIPPs. And so we agreed that they are longstanding and solid principles.

Perhaps what Privacy by Design did, and remember and recall that, in 2010, it was unanimously approved by the Global Data Commissioners in Jerusalem, and the areas where perhaps Privacy by Design has advanced, you know, beyond the FIPPs is in the fact that you are being proactive about privacy. You are looking at it very early and you are using mechanisms and tools to do that. And you are embedding privacy into the design of technologies or businesses processes or network infrastructures.

And then there's the other one that has been very attractive and what it speaks to is it speaks to getting rid of this zero sum, like it's privacy versus security or privacy versus innovation or privacy versus marketing.

And rather saying no, no. You can have both, but you have to be innovative. It may take some time, it may take some discussion and understanding of all of the objectives that need to be met, but there should be. Because what we don't want is to have that situation where, invariably, then privacy is given the short shrift.

MS. MITHAL: Dan, last comment and then I want to move on to a different question.

MR. CAPRIO: I just wanted to say, I think that the -- and it's been mentioned earlier today. You know, the first-party of the relationship, the one-to-one, that's really where trust and confidence, I mean, for the business opportunity of the Internet of Things to takeoff, I mean, we've got to get the policy framework, the privacy and security, right. And it's all about trust and confidence.

And the incentive, you know, obviously is to create or develop or differentiate on that trust and confidence. But it's that third-party relationship, it is different. And that's, I think, an area that we really need to think through much more carefully.

MS. MITHAL: Okay. So while we're on the question of choice, I am going to take a question from the audience. So the question is, throughout the day, panelists have suggested that we need a central ecosystem-wide, platform-level mechanism for user choice for the IoT.

So I guess what I'm envisioning is, you go to one place and you maybe set your preferences. For all of my connected devices, I'm okay sharing with the manufacturer, but you don't want to share with third-parties. Or I don't want to get the insurance discounts or I do want to get the insurance discounts.

Okay, so that may be good or not for privacy, but won't this give too much power and a huge competitive advantage to the entity that controls the mechanism or consumer interface?

MR. CALO: I mean, I think with any of

these questions, you know, you need to ask yourself a few questions as, I don't know, not necessarily for purposes of regulation, but just for purposes of what industries to sweep and what to look for, right?

Ask yourself, you know, sort of who built the underlying mechanism, who controls the data flow, and who pays, right? I mean, and the consumer is none of those things, right? If there's no control, if they didn't build it, if they don't pay especially, then that's the kind of place you want to sort of be scratching around and looking for potential for abuse.

I would say that our lodestar here should be to empower the consumer to understand and effectuate choices. I'm not sure that that needs to happen in the Internet of Things -- I mean, that makes me uncomfortable, in part because I just wonder precisely the gist of the question, which is how would you then -- when you have standards, how do you get an upstart to sort of be able to get into the mix? I worry about that.

But what about by household or by a consumer-by-consumer basis? What about requiring at least an interoperability so that a third-party provider can come in and create a hub that allows you to effectuate choice and see what's going on, right?

But again, I think it is about sort of sitting down and looking at the space with incentives, especially monetary incentives, in mind.

MS. MITHAL: Okay, Marc.

MR. ROGERS: I just want to say that I find it unlikely that such a scenario would come about. I think you've got too many different things coming from too many different areas for all of the manufacturers to want to cooperate in such a way. Some of them may have some advantage in doing that, but not all of them will have advantage.

There are also a significant number of already closed systems out there which aren't talking to other elements horizontally inside your house network. So I don't see practically how something like that would work.

I also don't think that level of control is necessary. Instead, what we should have is a standardized approach for doing this. I agree that we don't want the users to have millions of different interfaces that they have to go to regularly to deal with things, but if they standardize it and reduce it, I think it becomes a much more manageable solution. And at that point, I think the consumer is going to be a lot better off.

MS. MITHAL: Two more points that I want to hit before we move to the next scenario. So one is that we heard earlier today that one of the unique benefits of the Internet of Things is, you know, the data it can provide to improve our lives. You know, lower traffic congestion and improve medical outcomes. And a lot of what I think we heard today was about the idea of people using analytics from the IoT devices to improve outcomes in particular areas.

So let's say the data is shared beyond the consumer and the manufacturer, but the data is shared in aggregate or anonymous form. What sort of choice should there be for the consumer? Should there be a choice? Should companies be allowed or able to share the data on an anonymous aggregate basis? What does that mean?

I had some people down to call on if nobody raised their hand.

MR. CALO: Quickly, I think there is a big difference between anonymized and aggregate, first of all. I just -- it's like I don't really care if

-- I mean, imagine a consumer who says, I hate advertising so much that I don't want any of my data to go towards those advertisers and so that's a sticking point for them, right.

So apart from that rare person, anonymized, does that really matter? Does that really matter if they know who you are? I never sort of -- I mean, I understand the importance of anonymization, of course. And I've read Paul Ohm's excellent work like everyone else, but at the end of the day, like -- let's say that after you have a 12 mile run, that's sort of one of the scenarios. You have a 12 mile run and you are on this app and what it does it is tells Snickers that you just completed a 12 mile run.

And Snickers then is able to send you a text to your phone saying here's a coupon for Snickers, here's the closest place to get Snickers, right? And here you have run, you're so good, you've run and burned off all those calories and then all of the sudden, oh, you're susceptible. And this is when you get the Snickers ad, right? I mean -- think about the New York Times --

MS. MITHAL: But is that really anonymized or aggregate?

MR. CALO: Well, that's just what I'm saying. So does it matter if they know who I am? It could be utterly anonymized. It could just be device 124 went for a 12 mile run, do you know what I mean?

MS. MITHAL: Yeah.

MR. CALO: It doesn't matter who it is. And so for me, those are different threat scenarios.

MS. MITHAL: Right, right. So one scenario is, they don't know that you are Ryan Calo, but they know that you are device 1234.

Another scenario is Snickers gets the information of a 1,000 runners and says here's where we need to place our billboards. So those are two separate scenarios.

MR. CALO: But related. Interesting, yeah.

MS. MITHAL: Michelle, you had your --

MS. CHIBBA: So I was going to say, as a regulator, let's say if we do have a breach. I mean, the first question we always ask is, is it personally identifiable information. And for the most part, if it's anonymous, it's not. It's not. If it's aggregated, it's not. So the privacy, you know, the privacy issue doesn't come into play at that point.

I can tell you that, in terms of health research, it is very critical so we are always looking at ways -- and sometimes, for example, aggregated data is not effective in terms of the research, in terms of longitudinal research.

So we are doing a lot of work with academics around effective ways to de-identify data to be able to meet the research objectives, some granularity of the data, without specifically identifying the individuals.

So I think that's an area that one should be exploring as well and I know the FTC now has Professor Latanya Sweeney on staff, so it is an areas that, you know, certainly you will build your expertise. But this is an important aspect because health research is so vital and we don't want to -- you know, we don't want to put privacy towards a barrier towards that type of progress.

MS. MITHAL: Dan.

MR. CAPRIO: You know, I think that the example, if it is anonymous and de-identified, sort of gets to a larger question that we've got to think through as sort of, what's the harm? I mean, we might not like the scenario, you know, of running a marathon and then getting a Snickers bar, but in the overall scheme of things, is that really harmful as a consequential -- I mean, we've had a lot of discussion today about medical information or we protect financial information or kids' information.

I think we need to think through some of the consequences, but if it's anonymous and de-identified, then that's an industry best practice and I don't necessarily see the harm.

MS. MITHAL: And actually related to that, one of the things that we heard earlier today was that companies in this space can get all of this data, you know, we should be talking about use limitations, not necessarily about collection.

So does data minimization have a role here? It's one of the FIPPs, we can see Privacy by Design is having an element of data minimization and, on the one hand, we heard that companies use data in ways that are unexpected the consumers like. And what's wrong with that?

And on the other hand, we've heard that, well, you know, data minimization is important as a way of maintaining data hygiene so that you don't have these unexpected and unwelcome uses.

So where do we stand on data minimization in the Internet of Things space?

MR. CAPRIO: I think data minimization is important. I think, you know, Stan Crosley put it well, I think it was two panels ago, where he said what we need is we need more data, not less.

I mean, the data minimization is important, but there is so much -- as was said earlier, there is so much innovation and there are so many business models that are still developing, sometimes it is almost impossible to predict, you know, at the beginning what data needs to be minimized. And would you be, you know, minimizing the wrong data or sort of choking off potential benefits and innovation or sort of the value of the data if you were forced to predict that at the beginning.

MS. MITHAL: So that sounded like a case against data minimization.

MR. CAPRIO: Well, it's kind of a yes and no. I mean, I think in certain circumstances, data minimization is an important principle, but again, it is part of that, you know, the adaptation that we are seeing with the evolution of the Internet of Things. It's not black and white.

MS. MITHAL: Okay. Anybody else have a

view on data minimization and whether it is still relevant in an Internet of Things era? Yes, Michelle.

MS. CHIBBA: I would tend to agree that data minimization is still critical, even if it is de-identifying the data.

You know, we've done some big data analysis as well and what we always say is, you know, personal information are assets, right? It's very valuable information. So therefore, the more assets you collect and you hold, the higher your risk or your liability.

And you know, we can hear from Mark and everyone about security. The more data you hold, the higher, you know, security level you'll need. You'll need to encrypt very carefully because it's at risk, the more data you have.

So what we always say, if you don't have to collect it -- it's the first principle of data minimization. If don't have to collect the personal information, don't do it. But if you have to, then do it in as minimal possible way as is feasible.

And there are creative ways and one example that we always get when we're talking to institutions who come to us, for example, to say,

oh, we want this detailed voters list, right? They
want the date of birth. And we'll say, well, why?
Well, we have to know whether they are eligible or
not. Well, then just ask the question are they over
18 or under 18. Why do you need the date of birth?
Simple.

MS. MITHAL: That is a great segue into our third scenario, which Ben will introduce.

MR. DAVIDSON: This one is about a security breach. So Sue's system for controlling interconnected devices via the smart phone is extremely successful.

One day, she gets a call from her friend Tom, in California, who runs the home security system that is compatible with Sue's system. Tom tells Sue that the log-in credentials for his system were compromised and the criminal has posted live video feeds of some of Sue's customers on the internet.

Tom also tells Sue that he's not sure how to go about updating his alarm system software to remove the access to the user's system. The consumers are located throughout the U.S.

Marc, how should Tom have designed his system to provide better security and any initial thoughts about what might have gone wrong?

MR. ROGERS: So it's kind of difficult to say what went wrong with that amount of information. And I don't necessarily think that we should dive too deep into that. Rather we should look at some of the best practices that should have been followed that would protect against these kinds of breaches.

One of the first ones, and probably the most obvious, is to ensure that there is adequate compartmentalization between customer data and customer systems. You shouldn't be able to move from one customer's system into another customer's system without any difficulty.

Likewise, there should be care that the credentials are adequate, that they are strong, that passwords are changed, meet recommended standards. Things like two-factor authentication should be considered, but also the broad-based access control should be considered. It shouldn't be possible to take credentials from one subscriber and then go and access another subscriber's account, which is sort of vaguely what it sounds like went on here.

This isn't a new problem. This is a design issue that has been solved in many systems. It just gets more complicated because you're bringing in another popular word at the moment which is cloud. And with these cloud systems, it is a little bit more fuzzy to see who owns and who is in control of the data and sort of the access control systems.

But if security had been baked in at the start, and there had been a proper -- an adequate security assessment where a skilled assessor had evaluated the entire attack surface of the platform, looked at common vulnerabilities and issues, tested what you could do with legitimate credentials, tested what you could do with staff credentials, this kind of issue can be avoided easily.

MR. DAVIDSON: To follow-up on that, we've heard a couple of conflicting, or at least in tension themes throughout the day, one of which is that these vulnerabilities aren't that technically sophisticated. They are things that have been around in computer programs for years. Another, and I think you said this earlier, Dan, is that it's not too expensive to fix these problems, but at the same time, we've heard that just about every interconnected device has had these problems.

So I guess, what's going on? Is it a lack of incentive? Is it a lack of knowledge? Should we all be in the computer hacking business because it's so easy? Marc.

MR. ROGERS: I think it's the rush to get things to market. A lot of companies overlook the fact that they aren't necessarily the most skilled in these areas. They just are completely unaware of the issues because they are coming from a different field.

If you take a look at the issues with the Trend webcams. Default passwords are something that should never pass through into production space. It's an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren't often doing this kind of assessment -- so they see it as a hinderance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer's desk which, at the end of the day, the consumers aren't capable of setting that level of security, nor should they have to.

These products should be secure by design so that if a consumer wants to turn on an additional service, they turn it on, but it's not there unless they actually actively turn it on, understanding what the risks are.

MR. DAVIDSON: So in our hypo, who should be responsible for the poor security? Is it Sue or Tom or both of them?

MR. ROGERS: That's a difficult question to answer. I would say it's both of them. There are two systems there that have integrated and they both should have looked at the security.

Sue, at the start, should have ensured that anyone who integrates their system with her system didn't cause any unforeseen effects that then compromised data security. But the other system should have then been tested when it was integrated to be sure that something unforeseen hadn't happened.

MR. DAVIDSON: Michelle?

MS. CHIBBA: Yeah. We always say you can outsource services, but you can't outsource accountability. So I think it was Sue's responsibility to ensure because she's the first point of contact to the consumer, that any service that she contracts had better meet the same standard as Sue is, you know, advertising to her clients.

The other thing I think Tom and Sue should have had was a breach protocol. You know, as much as you want to design things in, you know, you have to face the fact that there could be a breach. So the question would be, you know, do they shut the system down right away from the network? What should the actions be?

I can tell you that we had a similar situation with a video camera and a backup camera on a car. I don't want to take up too much time, but it was a similar situation, it was a breach. It was a Methadone clinic and individuals in the clinic who are eligible to receive Methadone must demonstrate that, and have a witness, with respect to a urine sample.

So it was the best of the worst in terms of a privacy approach, so the clinic decided to put up a webcam in the washroom. And they were convinced -- they got the recommendation from a law enforcement service that they could install a wireless CCTV. You know, the receptionist could view it and, you know, no problem. It's wireless, it's just from the washroom to the receptionist.

What happens? Somebody with, you know, going in has a backup camera, we have the smart, you know, panel just before this, has a backup panel and then sees that it is fuzzy and then see someone urinating and had picked up the signal. Because this is not a secure signal that they use.

So in this case, as soon as we found out -- and of course it is always the media that finds out, right? The first point was, shut the system down. Shut it down. Try to, you know, at least reduce the harm that is being produced by this particular breach. And they did, they followed through.

But what is interesting is, and I know I'm going a little bit off-topic, but it's the fact that the Internet of Things is going to broaden, and I think another panel talked about this, our definition of what is personally identifiable information.

Because in this particular order or investigation that our commissioner found, you see the clinic said, oh, but it wasn't recorded. It was just a transmission, we were just monitoring. But our commissioner said no, no, no. You got expert advice. She said the pixels that were going across the particular airwave, if they were intercepted, which they were, could in fact become a record. These were pixels. The fact that they were picked up in this insecure band, radio frequency band, the fact that a backup camera could, you know, intercept that and take a record, she concluded that, in fact, these pixels were a record.

MR. DAVIDSON: Okay, Marc and then Dan.

MR. ROGERS: I just wanted to add one thing to that and that is shutting it down isn't necessarily always the answer. Or rather, if it is going to be an answer, there has to be some consideration in terms of what the consequences of that happening are.

When you're talking about a service like a streaming content service, shutting it down, you know, there's only the consequence of taking that service off-line. But when you are talking about something like an internet-connected lock, there could be some fairly significant consequences to the person who is relying on that lock in order to get into their house, relying on that security.

And at that point, the design should take into account what happens when the service does get shut down or when the internet is unavailable. If the internet is unavailable, you shouldn't be locked out of your house. Consequently, if the internet is unavailable, your lock shouldn't fail open, and therefore people would be able to walk into your house.

MR. CAPRIO: So I think in this instance, I mean, Sue should have -- we've talked about it, she should have built security into her products. But I mean at a very global level, there are some -- and TRENDnet is an important case, but there are some very high level principles that can apply which is, for instance, stop using hardcoded passwords and accounts and devices that will connect to networks. So common sense. And then quit using insecure protocols for device configuration and management. But it's sort of thinking these things through at the beginning and not after the fact.

MR. DAVIDSON: I was going to ask a question from the audience. What are some examples of Internet of Things projects that exist today that have done a good job of addressing privacy and security and what specifically is good about them?

Drew, why don't you start us off because hopefully you've seen some health apps that you think are good examples.

MR. HICKERSON: Yeah, certainly. So you know, one of the things that we test applications for, in addition to content, operability, privacy and security, is essentially the extent to which they take their data seriously, in terms of the privacy and security parameters they put in place.

And I think one of the important things that they do, especially cloud-based technology, is that they engage reputable, premier, well-known hosting providers. And fortunately, a lot of providers such as Firehose and now Amazon will sign what is called a business associate agreement. And essentially that is their promise, which they are obviously contractually bound by, to uphold the data with respect to certain privacy parameters, security measures, to make sure that they are essentially on the hook and they take the information as seriously as the consumer does with respect to their own information.

So a lot of the developers that we are working with, who actually aren't even subject to HIPAA, are engaging and utilizing some of these service providers who are, in fact, HIPAA compliant. So it's nice to see people go above and beyond, in terms of the types of vendors that they want to engage with, because they want that clout in the marketplace. They think it certainly distinguishes them from their competitors, but more importantly, it is essentially their promise to their users, in terms of what level they hold their user's information.

MR. DAVIDSON: Any other examples? Anyone else?

MR. ROGERS: I'd actually like to say that Google Glass is a pretty good example of a well-designed Internet of Things thing. It's got significant challenges, there is a lot of contention around its use, but if you look at the actual model behind it, Google has done a very good job.

The security, yes I was able to compromise the security on it and other people have compromised it in other ways, but Google has been very quick to respond and fix those vulnerabilities in an average turnaround of about two weeks, which is phenomenal compared to any of the other devices out there.

I mean, if you take a look, for example, at handsets. Huawei handsets have a half-life, in terms of fixing vulnerabilities, of infinite because many of the vulnerabilities don't get fixed. So I think Google has done a great job in developing a system where people can tell them about vulnerabilities, they can take those vulnerabilities, fix them, and push it out the user in a way that the user doesn't have to do anything.

Their device just gets secured. And that's a good way of doing it.

And also, they've shown that they are very responsive in terms of understanding concerns that people have with the kinds of content that should be displayed on Glass. They've been very, very clear in displaying the kinds of data that is going to be shared back and forth on Glass and how it is integrated. So I think that's a phenomenal product.

Another one I want to mention is the Nest thermostat, because I haven't been able to break it.

MS. MITHAL: If I could just follow-up with one question on a specific scenario, this talks about home security systems and the fact that hackers were able to access the live video feeds.

And this may be a bit of a technical question, but we know that companies like Google and Facebook fairly recently started encrypting email communications and communications on Facebook. In 2013, do people think that it is -- that live video feeds that come through Internet of Things products should be encrypted? Maybe that's a question for Marc.

MR. ROGERS: I think any kind of sensitive data that passes through an untrusted zone, such as the internet, should be secured with encryption. And it's questionable whether or not it should be encrypted in, say, semi-trust zones like DMZs.

We have the technology, we have the capability. It's kind of a no-brainer to me. As to whether or not it should be encrypted inside networks, that's a difficult question because there are other things to consider. For example, there is a lot of manipulation of content and aggregation that goes on inside the network and enforcing that all of this type of data must be encrypted could become very restrictive to companies and cause problems with a lot of services they run.

So yeah. In terms of internet video feeds, I think they should be encrypted.

MS. MITHAL: Okay, why don't we quickly move on to scenario four. I think we've covered most of this, but let's take -- so I think we've -- in past scenarios, we've talked about product as marketed.

And now let's say Sue decides to make a modification to her product. So before it was a one-on-one product, she developed disclosures, let's assume she got all the consents, and now she has decided to change her data sharing. And she now wants to share data with third-parties, either for medical discounts or insurance discounts, for advertising, whatever it may be.

I think, Ryan, you started to address this a little bit so maybe like a beeper goes off on your device and it says go look at the website, we have an important announcement to make.

So for something that the device has changed or the functionality or the data sharing has changed, we've talked to the FTC about the principle that, if there is a material retroactive change to a privacy policy, there should be opt-in consent.

So as a practical matter, how would these companies go about getting consumer's consent if they would decide to change their share? Dan.

MR. CAPRIO: Oh, I thought you said Ryan.

MR. CALO: Go, go, go.

MR. CAPRIO: Do you want to go?

MR. CALO: That's fine. I'll go. No, you go. Go ahead.

I'll just answer quickly. We can't even get consent among two of us, much less -- so I mean, there was an earlier question here which is, should that raise alarm bells in and of itself, right?

I mean, you know what drives me nuts, I've got to say, the FTC should investigate this, remember the first time that you went to a movie theater and you paid like nine dollars, and now it's much more, but this was like a couple of years ago, and you were sitting there and you paid your money and you got your popcorn or whatever, and then all of the sudden you see ads for Coca-Cola for like ten minutes, right?

I mean, that is exactly -- that is just, that is something where it is sort of that value proposition, just of that transaction, has shifted on you, right? I think that should set-off alarm bells. I'm not saying that you need to necessarily -- I understand the counterarguments, oh, you know, it would be even more than 10 or 11 dollars if we didn't have these ads beforehand and you can always come late. You know, I understand these things. But alarm bells should be going off when that happens. When OnStar starts to use the information for marketing, that's a real change of the gist of the transaction and that's what I'm trying to get at.

We should be looking for -- because, by the way, I'm not a data minimization proponent. I think the data should be promiscuous, it should be value additive, I see a tremendous upside to the data being, you know, really promiscuous. It's just that when we see these secondary, non-beneficial uses, it should trigger alarm bells. And it should trigger having to sit down and talk about that transaction again in a fundamental way, not just having some update on a policy somewhere, right?

So precisely how we do that, I'm not 100 percent clear, I have some ideas. But you know watching for that change in the nature of the transaction in a way that does not benefit the consumer.

MR. CAPRIO: I would say that I have sort of two reactions to the scenario. First, I am not sure theoretically that, in the Internet of Things environment at present, that the information is being exchanged for, you know medical information for a discount. So I think we do sort of have to deal with the here and now and the current and the practical.

That being said, if Sue is turning around and selling PII, that's a problem. And sort of whether that is in the theoretical world of the scenario or in the -- you know, if she is turning around and selling it to a data broker, that's a big problem. And I think that's part of, you know, the emphasis the FTC has put on the 6(b) study. But the secondary use issue is certainly very important.

MR. CALO: I just want to quickly respond and say that's why portability and sub-standardization is helpful, right? So the scenario is you buy something, you buy a product, it does something cool and you get to use it and so forth and then all of the sudden they are going to be selling your data to a third-party or marketing or whatever or giving you a discount. And we can read Scott Peppet's work about how you can frame anything as a discount. All you do is you raise the price to everybody else and then you give them a discount if they give up their data.

So you know, if your data is portable, right, then you can pick up and go to another provider. If it's not, then you are sort of locked in, right? So one nice thing about standardization and portability to police this area is that if there is an essential change in the nature of the transaction -- you know, that's why there should be movie theaters that don't show ads right beforehand, so I can go to those movie theaters.

MS. MITHAL: David, I wanted to ask you

about the scenario of the kind of modification to the original contract, so to speak, and what your views are on that and what you think the practical advice should be to companies that want to engage in this practice.

MR. JACOBS: Right. Well, you know I think it could be material because materiality is sort a fact-intensive inquiry and you have to look at how much does this affect the consumer's decision to use the product or not. And was Sue making some sort of implied claim when she was originally offering the product without selling consumer data?

And as far as how to obtain consent, I think that there are a lot of possibilities and it sort of depends on the particular situation that Sue finds herself in with the consumer and, in this case, it's an app, so you might have a just-in-time notice that pops up? Maybe there is registration and so she would also reach out to them through email and so on.

And so there are definitely connections that she formed with the consumer when she established this relationship and one of those should work for consent.

MS. MITHAL: So we have just a few minutes left and so I wanted to just go down the line and ask the panelists one question, which is if you were the FTC, what would you do next? So we can start with -- which way do you want to start? We can start with Marc.

MR. ROGERS: I think one of the challenges here is how wide the Internet of Things is and how fast it's moving. So I'm not sure whether we fully understand all the questions right now, let alone move on towards proposing some answers.

So I think we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing. And I think we should be light on the enforcement at this point, but there is a huge role to be played in pointing these companies toward the right answers that are out there. Because as we've heard, time and time after again, a lot of these design problems have been solved. They were solved in the earlier version of the internet.

And by following the best practice that already exists and addressing the problems that have already been solved, 90 percent of the issues can be addressed. That then leaves us with the kind of remaining problem set of what about these unique issues that arise as a result of the Internet of Things.

But like I said, softly, softly I think. We don't want to stifle this.

MS. MITHAL: Okay, David.

MR. JACOBS: I think that one thing that the FTC can do is enforcement. And in fact the Commission has already done this with the TRENDnet case. Joe mentioned on the other panel that there is no Federal omnibus privacy legislation and so, in the meantime, there are regulatory gaps the FTC can kind of step in with enforcement.

I'd also like to see more work done on the meaning of context. You know, we began with context today and it's come up in every panel, trying to talk about what types of collection and usage is consistent with the context of a technology or a relationship. And so I think there's opportunity there for the FTC to either, you know, come up with guidance or revisions to the privacy report, specifically addressing context.

MR. HICKERSON: So I think the first thing is to continue to educate. I think these sessions, you know, have been extremely helpful. The conversations have been very provocative and I think it all comes down to educating consumers, educating industry, educating the technologists that are building all of these solutions that we are utilizing on a daily basis.

I think, you know, the FTC can also work with the industry to partner up, because I think we are looking at an emerging market that is growing exponentially and there's too much volume to be able to really navigate and be able to enforce effectively alone.

And lastly, I think it's partnering with the other agencies. So I think, you know, the FCC, FDA, ONC, you name it, I think it is about coming up with non-duplicative standards or rules where it can be risk-based, so that also essentially minimizes the toll on the agencies themselves. But really work together and cohesively.

MS. MITHAL: Michelle.

MS. CHIBBA: I don't know, do you want a Canadians perspective of telling you what to do?

MS. MITHAL: Sure.

MS. CHIBBA: Anyway, so I am just going to talk about our experience. I think what has worked for us is certainly the Privacy by Design framework. So we are really pleased that the FTC has taken this on as a core value.

What we see next is really the fact that this is really a huge ecosystem that needs a lot of players at the table. So in terms of partnerships, what you're doing. The other partnership is with the academic community. They know what technologies are coming into the pipeline, they know what the vulnerabilities are, so I think there has to be a means to bridge what's going on in the academic world to what is practical and what can be sort of encouraged, in terms of technology development.

MS. MITHAL: Dan.

MR. CAPRIO: Thanks, Maneesha. I've actually been very encouraged by what I've heard today. I mean from government, civil society, industry, sort of all recognizing the opportunities and challenges related to the Internet of Things, particularly privacy and security.

And just a couple of things just to sort of need to keep in mind. First is, I mean, one size doesn't fit all. You can't -- I mean, this is an evolution that really requires, I think, a new way of thinking and a flexible framework to adapt to the 21st century. So as always, as the FTC thinks about this, it needs to be in a technology neutral way.

And I think that there's agreement that, you know, any sort of move toward regulation at this point is premature. We just don't know enough about the models and everything and where this is going.

So I think the opportunity is let's, you know, roll up our sleeves and get to work. But one final thing, sort of as a -- we've talked a lot about societal benefits and competitiveness, but I mean there is a lot at stake here. So to achieve the benefits of the Internet of Things, the country that gets this right will lead the world. And I think the United States has certainly led the world, you know, keeping the internet free and open and I hope that they work that we do together, we will be able to continue that leadership.

MR. CALO: I'll be really fast. So Commissioner Ohlhausen said something really interesting in her earlier remarks about how the Internet of Things is a kind of a -- it has two functions, right? First of all, it collects information, but also in many instances, it gives information back to the consumer, right?

And we've been talking quite a lot today about it's collection of information and if that's secure and so forth. But we should be keeping our eye, I think, also on the ability of now corporations to be able to reach people in their homes anytime, anywhere. I mean, won't some of the information that comes to consumers be advertisements? How does the ability to reach a consumer in the consumer's own home, in a nonmarket context, how will that change marketing dynamics, possibly for the worst?

Now again, I'm not saying this is happening today, but it would surprise me if we had this entire multi-billion, you know, enumerated Internet of Things and no effort were made for your refrigerator to maybe suggest that you should get some ice cream with the milk that you've just run out of.

So that's what I've said, to keep our eye on that. And I'm with the panel largely about wait and see.

MS. MITHAL: Okay, all right. So if panelists could stay in their seats, I'd now like to introduce the Director of the Bureau of Consumer Protection, Jessica Rich, who will make some closing remarks.

CLOSING REMARKS

MS. RICH: Great, hello. This is one of those podiums I can barely see over, so I'll try to be loud.

So this has been an incredible day, but also a long day so I'll also be short and loud. First, I'd like to thank all of our panelists for taking time out of their busy days, and there are many panelists still in the audience, to educate us about what's emerging in this area.

I'd also like to thank staff who worked really hard to make this event a success. Karen Jagielski, Ruth Yodaiken, Cora Han, Ben Davidson, and Kristen Anderson, and of course Maneesha Mithal and Marc Eichorn, who is out there somewhere. I think he was controlling the fan. He went out to turn that monstrous fan off.

So I'd also like to offer a few brief observations about some of the things we learned today and also talk about where we are going next. We did read that this workshop is a prelude to regulation, so I'll leave you in suspense and address at the end whether that's true. And Dan did mention regulation, so I'll just leave you in suspense and wait and address that in a few minutes.

In our first panel, we heard about smart items and services that are already appearing in homes across the country. From window sensors to ovens and energy meters, the array of connections brings many business partners into homes, but there are challenges including balancing convenience and innovation with privacy and security.

And there are those rolling up their sleeves to address those challenges, such as this multi-stakeholder effort to develop a voluntary code of conduct for energy usage data.

Looking forward, we want to ensure that companies that bring innovation into the home are nailing down privacy and security before opening the door.

In panel two, we heard about connected health and fitness devices ranging from casual, wearable fitness devices to connected medical devices such as insulin pumps that have the potential to save lives, enhance care and reduce costs. As our panelists recognized, however, privacy and security are essential to enabling consumers, doctors, and researchers to take full advantages of the benefits brought about by connected health and fitness devices, particularly given the sensitivity of the information involved.

These protections include encryption, compartmentalization, and appropriate use restrictions. Those will help ensure that consumers' health information will not unexpectedly be used in ways that consumers don't want them to be used.

In the connected car world, we heard about data that is currently collected, although not necessarily transmitted, by vehicles. We talked about the challenges of security and privacy in this space, such as the feasibility of notice and consent, the trade-offs between utility and safety. We talked about platform management and security by design in an industry that hasn't really focused on these issues before.

Finally, in our last panel, we learned that many of the privacy challenges involving interconnected devices are, in some ways, not new ones, but in other ways present specific challenges. For example, when it comes to the Internet of Things, how can we provide effective notice, particularly with interconnected devices that don't have screens, and when data is being collected passively, perhaps without a consumer's knowledge.

We also discussed the broader questions about whether the privacy issues raised by the Internet of Things will require rethinking some of the traditional frameworks we've had for protecting privacy.

What is clear, however, is that whether we are talking about home automation systems, connected fitness devices, cars or other things in this increasingly connected world, industry must step up to ensure that privacy and security safeguards are baked into the products and services that we talked about today.

These protections include privacy and security by design, I think there's lots of agreement about that, and also transparency and choice in some form. Although we are definitely still grappling with exactly when and how to provide these values in this context.

This is the beginning of our conversation with consumers and industry on the implications of the Internet of Things. As you might have guessed, our next step will not be to propose regulations, the suspense is done, I guess, but to do a report, which we like to do, to capture all of the great things that we learned today, including the recommendations we heard about different types of best practices that could be effective in this space as we move forward.

With that in mind, we invite everyone, who hasn't already, to submit public comments to us at iot@ftc.gov. We are keeping that open until January 10th, 2014, obviously. Not 2015. The more informed we are, the more helpful we can be in continuing this conversation in supporting sensible privacy and security protections that are compatible with innovation. We will post your comments on the Workshop page at FTC.gov.

Thank you so much for coming.

(Whereupon, the proceedings ended at 5:30 p.m.)

State of Maryland, County of Harford, to wit:

I STEPHANIE M. GILLEY, a Notary Public of the State of Maryland, County of Harford, do hereby certify that the within-named witness did appear at the time and place herein set out.

I further certify that the proceedings were recorded verbatim by me and this transcript is a true and accurate record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _____ day of ____________________, 2013.

____

STEPHANIE M. GILLEY

NOTARY PUBLIC

My Commission expires on February 25, 2017.