UNITED STATES DEPARTMENT OF COMMERCE

+ + + + +

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

+ + + + +

WORKSHOP

+ + + + +

FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

+ + + + +

THURSDAY
SEPTEMBER 1, 2016

+ + + + +

The Workshop convened in Madison Hall at the headquarters of the United States Patent and Trademark Office located at 600 Dulaney Street in Alexandria, Virginia, at 9:00 a.m, Travis Hall, Facilitator, presiding.

PRESENT

TRAVIS HALL, Policy Analyst, Office of Policy Analysis and Development, National Telecommunications and Information Administration, Facilitator
HARDIK BHATT, CIO and Secretary-Designate for the Department of Innovation & Technology, State of Illinois
JULIE BRILL, Partner and Co-Director of Privacy and Cybersecurity Practice, Hogan Lovells
HILARY CAIN, Director, Technology and Innovation Policy, Toyota

LEONARD CALI, Senior Vice President, Global Public Policy, AT&T
DAN CAPRIO, Co-Founder and Chairman, The Providence Group
ALAN DAVIDSON, Director of Digital Economy and Senior Advisor to the Secretary of Commerce, US Department of Commerce
MICHELLE De MOOY, Acting Director of Privacy & Data Project, Center for Democracy and Technology
DEAN GARFIELD, President and CEO, Information Technology Industry Council
HARLEY GEIGER, Director of Public Policy, Rapid 7
JOHN GODFREY, Senior Vice President, Public Policy, Samsung Electronics America
AJIT JILLAVENKATESA, Senior Standards Policy Advisor, Standards Coordination Office, National Institute of Standards and Technology, US Department of Commerce
BRIDGET KARLIN, Managing Director, Intel IoT Strategy and Integrated Products
CAMERON F. KERRY, Senior Counsel, Sidley Austin
LINDA KINNEY, Senior Advisor, Internet Policy, NTIA, US Department of Commerce
JOHN KUZIN, Vice President and Regulatory Counsel, Qualcomm
JOHN B. MORRIS, JR., Associate Administrator, OPAD, NTIA, US Department of Commerce
STERLING ROOKE, President, X8
ANGELA SIMPSON, Deputy Assistant Secretary, NTIA, US Department of Commerce
RUSSELL SLIFER, Deputy Undersecretary of Commerce for Intellectual Property and Deputy Director of the United States Patent and Trademark Office
CRAIG SPIEZLE, Executive Director, Founder and President, Online Trust Alliance
LAWRENCE E. STRICKLING, Assistant Secretary for Communications and Information and NTIA Administrator, US Department of Commerce

KENNETH TOBIN, Director, Electrical & Electronics Systems Research Division, Energy & Environmental Sciences Directorate, Oak Ridge National Laboratory
KENYA WILEY, Founder & CEO, Fashion Innovation Alliance

ALSO PRESENT

TREY FORGETY, National Emergency Number Association
CINDY GRADY, Intelsat
SYED ZAEEM HOSAIN, Aeris
RICK LANE, 21st Century Fox
GEORGE MINARDOS, .build
JOSH NEW, Center for Data Innovation
MICHAELA ROSS, Bloomberg BNA
CARL SZABO, NetChoice
RANGAM SUBRAMANIAN, US Department of Commerce
ERIC WENGER, Cisco

A-G-E-N-D-A

P-R-O-C-E-E-D-I-N-G-S

9:07 a.m.

MR. HALL: All right. Thanks everybody for coming. Welcome to the Fostering the Advancement of the Internet of Things Workshop held on behalf of the Department of Commerce.

My name is Travis Hall. I am a telecommunications policy analyst with the National Telecommunications and Information Administration.

And first off, thank you all for coming. This is a really important topic. We've had a great outpouring of interest in terms of the comments from the request for comment.

And we're really excited about today. I think that we've got a really interesting program lined up. And I'm not going to waste too much of your time talking.

So, really quick, just a few logistical things. Restrooms are out the doors straight ahead.

Women's room, you need to go through -- there's like the little dining room. If you go up to the yellow sign and turn right is the ladies' room.

A little bit further along past the glass doors is the men's room.

And exits, there's exits all over the place so in case of emergency there are ways to get out.

First off what I'm going to do is I'm going to introduce our welcoming speakers.

First we have Alan Davidson who is our Director of Digital Economy at the Department of Commerce and senior advisor to the Secretary of Commerce.

For those of you who, just as an FYI, who want more information on the biographies of any of our speakers we do have printed copies of biographies at the welcoming table.

And then second we're going to have Deputy Undersecretary of Commerce for Intellectual

Property and Deputy Director of the U.S. Patent and Trade Office Russell Slifer who provides strategic leadership and oversight to one of the largest intellectual property offices in the world which we are very fortunate to be in. What a beautiful building and facility this is.

So without any further ado I'm going to hand it over to Alan to get us started.

MR. DAVIDSON: Thank you, Travis, and thank you to all of you. Welcome this morning to our workshop on Advancing the Internet of Things.

Thank you for joining us I should say also, and particularly both to the crowd here and to the folks out on the webcast who are joining us there.

Let me just start by saying today's workshop was really borne of a set of questions that have been posed both within government and outside of government for the last several years that we've been hearing about, what is this Internet of Things.

Is it a distinct phenomena or issue that merits our attention? What are the benefits of the Internet of Things? What kinds of opportunities does it raise? What kinds of policy challenges are we going to be facing?

And particularly for those of us in government thinking about this what is the appropriate approach of government? What is the role of government in the Internet of Things and what should our strategy be for engaging and making sure that we're maximizing those opportunities and also addressing those real challenges that we know are lurking out there.

Today's workshop has been some months in the making and is really designed to explore many of those questions in depth with all of you.

As many of you know the Department of Commerce through NTIA released a request for comments in the spring.

We were really gratified by the response. We got over 130 comments back. They're

up on the internet for those of you -- hopefully many of you have had a chance to look at them.

They came from a diverse, very broad set of stakeholders both in industry, academia, civil society and many of the commenters are here today. So I'd just say thank you for your thoughtful input and counsel that we've gotten and we really appreciate it.

And as we've gone through them certain themes have emerged.

One is that it's clear to us now that the Internet of Things is a technical and business phenom that demands our attention.

The Internet of Things has faced some skeptics, including skeptics within our building. And the question has been raised what's so different now. We've always had an internet that was made up of things.

I think we've been persuaded and the comments make quite clear that the Internet of Things raises some very important differences in

terms of its scale, its scope and the stakes that are at play.

In terms of scale we have over 3 billion people on the internet today. Estimates are that more than 4 times that number of devices are connected online right now, and that number is growing, that ratio is growing.

So, the number of devices that are connected online is rapidly growing and it's going to far outstrip the number of people online.

The scope of it is one of the things that's quite interesting, the breadth of applications we're now seeing in the Internet of Things.

The fact that it's keychains, it's thermostats, it's health devices, it's autonomous vehicles, it's streetlights and connected cars.

It's along the way creating a very broad economic impact with the studies that we've seen talking about trillions of dollars of GDP impact over the next decade. So this is clearly a very

broad phenomenon in its scope.

And the other thing that's quite interesting to us is that it's clear that the stakes are higher, in part due to I think what you'd call the physical or kinetic nature of many of the connected devices that we're seeing.

Twenty years ago a lack of connectivity or functionality online meant you couldn't check your email, or you couldn't get to a website.

In the future that might mean a lack of functionality in that your car doesn't work, or your security system in your home doesn't work, or an implanted medical device doesn't work.

And so we are absolutely going to be entering a new era of consumer and business attention to these devices and to this area.

As a result we see an incredible opportunity. It's clear that the Internet of Things is offering a remarkable set of breathtaking consumer applications and also quite interesting, a remarkable set of applications for the industrial

Internet of Things.

And it's going to be transforming the way we do manufacturing, and it's going to be boosting productivity.

It also as we're going to discuss today raises important challenges including issues like privacy and security, but also how we achieve the best technical building blocks, how we make sure that we have good broadband spectrum, interoperability, standards, issues around international competitiveness.

And we know that if we don't address those issues, if we don't address those challenges and ensure that the proper building blocks are in place we won't be able to realize the full potential and promise of the Internet of Things.

In our comments we also saw I think a desire at least on the part of some commenters for a clearer engagement by government.

Some people are actually calling for a national strategy around the Internet of Things,

and that's something else we want to explore today.

What is the right shape for government engagement? How do we best coordinate not just within the federal government and all the agencies involved, but among policymakers at the state and local level who will be engaged, and among international policymakers.

And this is important I think particularly for the Department of Commerce and our digital economy work.

We have two decades now of experience at least honing a policy approach to the internet and to digital technologies.

It's an approach that's been grounded in principles like openness, freedom to innovate, multi-stakeholder participation, and a very careful approach to regulation that I think shows a humility and a respect for the rapid pace of technical change.

As Internet of Things moves into areas of traditional regulation ranging from healthcare

to automotive safety how do we ensure some consistency and fidelity to the approach that we've taken that has made the internet and our digital technologies so successful? That's a question we really want to explore with you today.

The Internet of Things and this workshop are also an example of a broader question we have about how government engages with new and emerging technologies.

It's quite clear that the pace of technical change remains incredibly high. You just look around. Every week, every month some new and interesting area of development just even within the areas of digital technology.

And this poses huge challenges, not just for business and for consumers, but for government as we think about how as a society we grapple with the kinds of rapid change and dislocation that can sometimes come from new technology.

And so part of our focus at the Commerce

Department and particularly within our digital economy agenda has been to think about how government can thoughtfully engage. How can we make sure we have the right talent. How can we use the expertise that we know we have in-house.

How can we engage with industry and stakeholders to be thinking about the hard issues ahead of time, to be a booster of new technologies and to make sure we're heading off the hard problems before they become real problems.

And so this is an area where I think you'll be seeing more from us. And the Internet of Things is a terrific example of what we're trying to do.

So, just to give you a little preview of the day hopefully folks here have got the agenda. It's up online as well.

Our workshop today is designed to mirror these themes and questions that have been raised.

To give a little preview, as a start

we'll hear more about the promise of the Internet of Things. And we'll kick off both the morning and afternoon sessions with short, real-world stories from people in the field about the possibilities and the promise that IoT offers.

We'll also explore the technical building blocks for the Internet of Things including issues like interoperability, spectrum, broadband access.

We'll have a panel that will then explore the policy opportunities and the challenges with issues like privacy, security, innovation and inclusion.

And as I said we're keenly interested through all of this in thinking about our mission which is what is the appropriate government role in all of it.

This morning we'll have an armchair conversation led by NTIA's Assistant Secretary Larry Strickling to explore one major effort in industry to craft a potential national strategy.

This afternoon we'll hear from an all-star panel to explore the role of government and think more deeply about this question of the national strategy.

All through this I have to say a real word of thanks to all of our speakers and participants today. We are just delighted to have such a deep bench of expertise from across the IoT ecosystem and from diverse perspective including industry, academia, the non-profit community, public interest groups. So thank you all for participating.

In conclusion I would just say it's clear that the Internet of Things is a business and technical phenomenon that we need to take seriously and that demands our attention.

We need to get the policy side of this right as well to make sure that the Internet of Things realizes its full potential.

We're excited to get this day started. We look forward to your input on ideas and thank

you once again for joining us.

Now, I'll very quickly turn to our next speaker, and as I do I want to just say thank you to the Patent and Trademark Office for hosting us today. They do have a beautiful facility here. We're delighted to be in Alexandria.

And please join me in welcoming Russ Slifer who's the Deputy Director of PTO. And thanks.

(Applause.)

MR. SLIFER: Thank you, Alan, and welcome everybody here to the USPTO. We're really happy to have you with us today.

Like many of you perhaps I had no idea what the term "Internet of Things" meant when I first heard it. Was it simply talking about all of the things that I see on the internet? And then I realized what the general definition was.

But it makes more sense that we need a term to describe the many ways our lives are touched by interconnected things, from the smartphones in

our pockets to the buildings that we live in, to the vehicles we drive, to lifesaving medical devices.

Now, I'll be honest, some things are not as life-changing as others. I was looking last night and I saw dog bowls where I could control it and feed a treat to my dog while I'm watching him from work, or an egg tray that miraculously tells me when I'm low on eggs so if I'm at the store I know to buy more eggs.

We all need to check our slow cookers throughout the day, right? To make sure that they're cooking right.

I'm only making fun a little bit of some of the things. I live using the Internet of Things every day.

My home is in Boise, Idaho. I've got it connected so that I can look at my security cameras. I can control my lights and the temperature in my house, the irrigation in my yard. So these kind of things are touching everybody. As

Alan said, there are millions and millions and millions of devices every day that are connected and being controlled.

But besides the name of what we call this and the underlying technology that is being controlled by it are policy challenges that require public and private collaboration, especially in the realm of intellectual property.

Similar to the Internet of Things is the subject of copyright in the digital age. And that's a very important topic recently we tackled at USPTO partnering with NTIA as co-leads of the Department of Commerce's Internet Policy Task Force.

We published a white paper this past January which was the fruit of that collaboration.

In it we recommended among other things amending the Copyright Act to provide more guidance and greater flexibility to courts in awarding statutory damages.

We also made several recommendations to

make it easier for remixers to understand when a use is fair, and to obtain licenses from the owners when they need to.

We also recommended the development of best practices by stakeholders to improve consumers' understanding of the terms of online transactions involving creative works.

In making those recommendations and others the task force was mindful of the need to protect copyright effectively while promoting innovation on the internet.

That same spirit is very much behind the task force work on the Internet of Things. And for that matter, the work of the USPTO.

Our mission here at the USPTO is rooted in the Commerce Clause of the U.S. Constitution that Congress set forth to promote science and the useful arts by securing for limited times to authors and inventors the exclusive use of their writings and discoveries.

This clause provides incentives to

innovate in exchange for the dedication of those innovations to the great corpus of human knowledge, and to the benefit of all mankind.

Without these incentives there would be little motivation for anyone to share their new ideas, and arguably plenty of incentives not to share.

Such ideas and innovation play an important role in our nation's economy. As Alan pointed out we have smart cities that are going up.

We've got new innovations that are used to improve access to public services, making workers safer and allowing consumers to upgrade their homes.

The importance of innovation in our nation's economy has never been more important or greater, frankly.

According to a forthcoming Industries in Focus report, IP-intensive industries directly or indirectly support 45 million jobs, nearly one-third of the U.S. employment.

The share of total U.S. GDP attributed to IP-intensive industries was over 38 percent in 2014.

Private wage and salary workers in IP-intensive industries continue to earn significantly more than those in non-IP intensive industries.

So those are important numbers. And as policymakers we want to make sure that they keep going in the right direction.

As always, that means maintaining a healthy balance between the need for adequate IP rights and the freedom of innovators to do what they do with as few obstacles as possible.

So, a couple of things we're doing here at the USPTO to help empower the Internet of Things and the larger information economy is making more and more of our data available.

We currently make our public patent and trademark data available in bulk form which can be loaded into databases and other analytical tools

for research and analysis.

But we're looking to improve that, both the discovery, accessibility and usability of this data through application programming interfaces, or APIs.

APIs as you know power a majority of the mobile applications, many of our IT programs and also create a market for the private sector to develop as well.

We recently launched a developer's hub on our website, uspto.gov, which enables the sharability and social interaction to showcase unique ways that our data is being used, including combining it with other data sets such as economic and geographic data.

Through this forum users can leverage our data and empower the crowd to answer questions in both trends and innovation.

So the Internet of Things touches us and we're trying to touch the Internet of Things.

So in closing, first I want to thank you

for coming to this important workshop.

A shameless plug. I also want to point out while you're on our campus right above us is our Inventor's Hall of Fame. And I welcome you to visit that if you've got time today, or come back again and visit it.

We recently renovated it and it highlights inductees and their great technological achievements.

For example, in 2016 we inducted Victor Lawrence who stimulated the growth of internet through his work in high-speed transmission work at Bell Labs at AT&T.

In addition to that you're also going to see a very unique car that Ford Motor Company donated to us where they combined a 1965 Mustang and a 2016 Mustang, split them down the middle and combined them so you can kind of see how technology has advanced over the last 50 years. It's one of my favorite exhibits.

So again, please enjoy our campus while

you're here. Thank you again for attending and I look forward to a productive workshop. Thank you.

(Applause.)

MR. HALL: Thank you so much, Deputy Undersecretary Slifer.

And I would like to invite to the stage Bridget Karlin who is the managing director of the Internet of Things Strategy and Integrated Products Division at Intel Corporation.

She's responsible for Intel's IoT platform and product portfolio marketing developing strategic business objectives, go to market strategies, success metrics and for managing the commercialization of IoT partner and branded offerings leveraging silicon software and services that engage Intel's ecosystem of partners to accelerate market adoption.

What I think that really boils down to is she does it all. So I'd like to welcome her to the stage and I'll go ahead and get your PowerPoint set up.

MS. KARLIN: Good morning. It's a pleasure to be here. I'm Bridget Karlin, the managing director for Intel for the Internet of Things group. And a very nice introduction, but I do not do it all.

Intel is filled with very talented, brilliant people who make some of these amazing IoT transformations possible.

It's a pleasure to be part of the workshop and I applaud the Department of Commerce and the NTIA to pull this together.

I think this is a very exciting time for all of us in the industry. And frankly, public, private, academia, we are all coming together as part of this IoT phenomenon. So I appreciate being here today.

What I thought I would do is spend a few minutes this morning and talk about how IoT is reinventing our world, and how it's truly transforming every experience in our lives.

This is really something as important

as really when we first became aware of the written word and what a moment that was in time where things really started to culturally transform our world.

This is how significant IoT is, and we are in the era of IoT.

First, let's look a little bit into the future. I love the idea that was brought up earlier about the dog bowl and knowing when to get the next treat. Being able to be in Washington, D.C. and being able to keep an eye on your home if it's in Boise, Idaho, or if it's in Los Angeles, wherever it may be.

Those are some of the implementations of IoT today. But let's think about the other possibilities.

Imagine entire fleets of vehicles rolling down our streets and our freeways with no driver in the driver's seat, or maybe not even in the vehicle at all.

Imagine your car, your Ford Mustang, your BMW being able to drive you to work, drop you

off, go park and come back and pick you up when it's time to go home.

Imagine your elderly parent who no longer has to worry if they took the prescribed medicine at the right time or in the right amount because the ingestible pill will automatically send a confirmation to him or her as well as to his doctor confirming that he's taken that medication and what amount and at what time.

Think about the parent who no longer has to worry that the child is safely fastened into the car seat, or that they're accidentally left behind in the car when they dash into the store.

Think about our shoes and our clothes being able to give us quantifiable fitness information so we can track our progress with our health, or be able to use gestures to make a phone call or bring up our email, or play a musical instrument.

And think about our industry giving us products and services that are tailor-made to

exactly what we like, and they're accessible or delivered to us whenever we want them and wherever we may be.

And then we talked about smart cities, but envision cleaner air, sufficient energy, sufficient water to power a smart infrastructure that is supporting the growth of our cities.

This is basically what IoT is bringing forward to us and how we are going to start to see our experiences and our world transform.

So what I wanted to do is to talk to you today about three basic things. First, why is IoT important and why now. Secondly, what are the challenges with IoT and a little bit about what Intel is doing to enable IoT transformation. And then finally, look at some examples of IoT in action today.

So first let's start with the definition of IoT. One was mentioned earlier, but just to sort of synchronize. This is a broad term, but essentially IoT basically means taking

everyday objects like our phones, our televisions, our cars, our appliances, machinery, connecting them to the internet where data can be shared, analyzed, and then translated and converted into meaningful insights or actions. That's basically what IoT means.

Now, we're excited about that because it has offered up an incredible number of possibilities. And I'll give you a couple of examples.

You mentioned the thermostat. Did we know we needed to connect our thermostat to the internet? Not really. But now that we can it's kind of nice that we can adjust the temperature in our home before we leave the office so the house is cooled off by the time we get there.

Another example is taking the traditional, probably one of the oldest industrial safety pieces of equipment there is, the hard hat, and by adding sensors, and processors, and augmented reality we now turn that hard hat into

a smart helmet so the worker can see through augmented reality schematics of the apparatus he's working on, get realtime instructions for what he should be working with, get environmental conditions and essentially make that worker more productive, make him more aware of the conditions around that he's working in, and ultimately make him safer.

These are two examples, one sort of consumer, one industrial. And together they represent the scope of the IoT. This is essentially a consumer and industrial opportunity, and it represents the analysts are telling us anywhere from a four to a seven trillion dollar global economic opportunity by 2025. So the opportunity is significant.

So, why is it important? IoT is going to be delivering unprecedented benefits for governments, for businesses, for consumers that will essentially change our experiences and our communities.

We have heard from the analysts that it's estimated that 55 billion devices will connect by 2020, 212 billion sensors. So the world is sensing up as well. And together they will be generating over 44 zettabytes of data. And if you don't know what a zettabyte is, it's a lot of data.

And essentially it's an explosion of data that is essentially offering these new meaningful insights and actions that we can take.

When we think about the economic opportunity that that presents this is where it gets exciting and where we start to look at what does that really mean.

Let's ask a little bit more and look a little bit more into where do we see the IoT growth opportunity.

And I wanted to spend a minute and break it down for you from an industry perspective.

Healthcare. That's expected to be a $450 billion market by 2020.

Industrial, manufacturing, energy is

expected to be about a $175 billion industry by 2020.

Transportation, $144 billion industry. And we know from the in-vehicle services that will be delivered that alone represents about a $40 billion services industry.

So these are big numbers, big opportunities and they're cutting across all types of vertical industries.

So while the estimates are impressive, and they are, and they're very exciting, are we living up to the hype?

You know, we sit here today and we have some experiences with IoT in our own world, maybe at work, maybe with our businesses. Maybe we're here to talk about some of the implications of it.

But where are we today? So, analysts are telling us that today in 2016 we are connecting 5.5 billion devices to the internet daily. We're spending $2.5 million on IoT hardware every minute, and we have to date 4.5 million developers working

on IoT applications.

So we have some evidence that IoT is absolutely underway and innovation is taking place.

In addition to having a great economic opportunity for the industries IoT has also become a global catalyst. It has caused the industry to transition.

There are a couple of global initiatives that we should be aware of. Industry 4.0 in Germany is underway as well as across the European Union.

We know that China has stated publicly that they intend to have an entire autonomous intelligent manufacturing ecosystem by 2025.

So these are initiatives that countries all around us are investing in and are pursuing this aggressively.

We also know that over the last year in 2015 $21 billion was invested in mergers and acquisitions for IoT. That's a lot of investment.

And funding for IoT startups has essentially doubled in the last five years for IoT.

So we have consolidation, we have investment and we have countries around the globe committing and implementing IoT for transformation.

So I think one of the things that's interesting here when we talk about the transformation is I'll talk a little bit about what Intel is doing.

Intel is a $55.9 billion industry leading manufacturer of computing, networking and communications products.

We're based in California and we employ 107,000 employees globally.

We're the company basically that powers the cloud and all of these billions of smart and connected devices.

Our vision for IoT for Intel is to essentially lead the industry and drive the experiences of IoT, making it simpler to create

these. That's basically our goal.

But one of the things that we're very respectful of is that this doesn't happen overnight. IoT is very -- you've heard this before, but IoT is very much a journey that we're on here. We're in this new era of technology and it's not going to happen overnight, partly because there are some significant challenges. And I think in the workshop today we'll be covering some of those.

Some of the challenges, I mean we can't have a conversation about IoT without talking about security and data privacy. That is a fundamental concern and a challenge that we face when we think about scalability for IoT.

Secondly, interoperability. With all these billions of devices they weren't engineered to all talk together and share data. So that will be a challenge.

Communications and connectivity. All these devices have different protocols. They

weren't all expected and designed to seamlessly communicate with each other. So that's another challenge.

We have a challenge with the explosion of data. Data is not our problem. We have a ton of data coming at us. How do we harness that and turn it into analytics and into those meaningful insights and actions?

The other thing that we're struggling with is that there are no standards. This is a challenge for our industry for sure in that when we think about scalability and everybody going back and innovating, we don't have a lot of standards to write to. And so that will slow things down.

So, what is Intel doing to help address some of these problems?

First of all, interoperability. This is an important area of getting all this stuff to talk to each other.

One of the things that Intel has done has been founding members of a few standards bodies

that are looking at this problem, both for creating test beds as well as to define specifications.

We have the IIC which is the Industrial Internet Consortium that was founded and now has membership up over 250 members.

The OCF, the Open Connectivity Foundation which is essentially writing and defining device-to-device specifications.

And then most recently OpenFog. We found that we need new architectures. With all this data coming at us, and all these smart and connected devices the traditional architectures of pushing everything to the cloud isn't going to work and isn't going to be efficient.

We may want to analyze some of that stuff right at the device, right at the point of origin. So we needed to have a new architecture and OpenFog is a standards body that will help define that.

Another thing we're doing is that we have defined the Intel IoT platform which has two

things. It has open scalable architectures or blueprints that will help simplify how to build these end-to-end IoT solutions. And we put forth a portfolio of technology building blocks that we put in the hands of the ecosystem to go build these technologies.

Another thing we're doing is that we're investing and developing in 5G. 5G communications is basically high-speed low-latency connectivity in an intelligent communications platform that will be required for things like autonomous driving, vehicle-to-vehicle safety.

So these are the kinds of things that are extremely important and some of the actions that we're taking.

What I thought I'd do is now let's talk a little bit about, let's see some IoT in action.

We've been, in addition to working with the industry we've been collaborating with our partners and our customers to implement IoT.

Let me give you an example of smart

retail. Levi's, and we all know Levi's and their jeans, was looking to address an industry-wide trillion dollar annual problem of out of stocks or overstocks.

So we used IoT in their stores so they could get realtime inventory and know exactly where that specific pair of jeans size 32 in blue, is it in the dressing room, is it on the shelf, is it in the back.

They implemented that. They've now rolled it out to several stores and they are experiencing an uplift in sales that has more than helped pay for the technology. So they're starting to see the benefits of that.

I'll give you an example of trucking. We have a customer, Saia Trucking, they're based in Georgia. They operate a fleet of 3,000 vehicles.

And by implementing sensors in the cab, driver information and connecting it to the internet they have been able to improve

efficiencies with their fleets.

They have now measured that they have saved something like 6 percent on fuel costs which translates to about $15 million for them annually. And it has helped reduce emissions.

So these are the kinds of things that from just a transportation standpoint illustrate to the rest of the industry the benefits of implementing IoT.

Another example is a partnership we have with Honeywell for first responders by using wearable technology, biometric data. Being able to detect if a man was down.

Being able to detect if there's hazardous gas in the area and give the first responder alerts to let them know what the conditions are. Or to send a note to the supervisor that man is down, may need some help.

These are the kinds of things on a realtime basis make all the difference between life and death.

Another example when we talk about safety, and I'd like to use this one is child safety.

I don't know if you're aware, but in the U.S. a child goes missing every minute and a half which is a parent's worst nightmare.

We have a partner called Child-Angel and they've developed a tiny wearable bracelet for the child that can detect where the child is. They an program safety zones so if the child steps out of that zone the parent immediately gets an alert.

Or for example, the car seat. We've got a little picture of the car seat up there.

An example of a smart baby clip with a partner called NABI. They call it the NABI sitter. It's a little Bluetooth-enabled clip that fits onto the car seat.

And so the parent will know first of all if the child is fastened into the car seat, or if they get out of range that they may have left the child in the car and needs to go back and get the

child.

This is the kind of thing -- and it's one of the things when we think about safety is so critical, and yet these are maybe not the most exciting implementations of IoT, but they're so important. And they make a difference when we talk about safety.

In fact, to date this year 27 deaths have happened from children being left in the car. So, something as simple as the smart baby clip makes a huge, huge impact.

And then finally I wanted to give you an example of healthcare.

We have partnered with the Michael J. Fox Foundation to help understand that invisible disease that is addressing some of us around the planet.

We're able to use wearable technology, connect it to the cloud and be able to essentially take vital statistics of patients without really disturbing them.

We are clocking something like 300 data readings per second. We're getting things like blood pressure, sleeping patterns, things like that, so we can get a richer data set that we can use, that the physicians can use to help understand both how the treatment is going as well as other complications of the disease.

So that in kind of a nutshell gives you a sense of some of the things that we're using today for IoT.

But let me step back and talk a little bit about what we're here today to really address, and that is the importance of collaboration across public and private and academic sectors.

First of all, one of the things that we believe in is being able to have consistent federal, state and local policies for IoT to thrive. That will be hugely important.

Also, we feel it's very important to support open and standards-based performance rules rather than technology mandates.

It's very important that we focus on outcomes rather than specifying the type of technology that we want to use so that we ensure we keep pace with innovation.

We want to also consider that this information now with IoT is global. So the rules we make here at home we need to take that into account and make sure that we don't put the U.S. at a disadvantage.

We also want to applaud and encourage continued funding and education, and collaboration with industry as well as academia around IoT with the government agencies.

I think the federal government has shown tremendous interest and is absolutely spot on with holding workshops like this, and engaging all of us together so we can bring the best minds to some of these problems.

And finally, when we look forward and we say what is this world going to look like in 2020 and beyond with all these billions of devices

connected we're basically going to become a smart and connected world.

We're going to be finding things or acting autonomously based on machine learning. And we're going to be able to make better decisions whether we're at home or at work.

We'll enjoy safer environmental conditions whether we're a passenger in a driverless vehicle, or we're out on a construction site.

We'll be able to have more personalized medical therapies so that we can optimize our health.

And we'll have more access to personalized products that are tailor-made to what we want, and we can access them whenever we need them.

Ultimately we want to make sure though that we have positioned the United States to be a global leader and to harness this economic opportunity.

So, with that I want to thank you again. I think we want to get ready for this smart and connected world, and essentially what I call the Golden Age of IoT where every experience will become better. Thank you very much.

(Applause.)

MR. HALL: Excellent. Thank you so much. And I'd like to invite Larry Strickling and Dean from ITI to the armchair for an armchair discussion.

So, Larry Strickling is Assistant Secretary of Commerce, and Administrator for the National Telecommunications and Information Administration, and my boss.

A technology policy expert with more than two decades of experience in public and private sectors.

Larry's focus at NTIA has included leading initiatives to expand broadband internet access and adoption in America, and to ensure that the internet remains an engine for continued

innovation and economic growth.

And Dean Garfield is the president and CEO of ITI, the global voice for the tech sector.

Under Dean's leadership ITI has defined the tech agenda for global policymakers, expanded its membership and influence, and launched a foundation that serves as the preeminent thought leader on innovation.

I'd like to hand it over to both of you. Thank you.

MR. STRICKLING: Thank you, Travis. Welcome, Dean.

MR. GARFIELD: Thank you.

MR. STRICKLING: Thanks for joining us. This is our armchair discussion although in my case I might have preferred not the arms, to maybe just a chair discussion, but we'll get our way through this.

First off I happened to notice that your organization is celebrating its 100th anniversary this year. How can that be?

MR. GARFIELD: I was there at the start. No.

Let me begin by thanking you for hosting this discussion as well as celebrating the folks at NTIA. My wife worked at NTIA some twenty-something years ago, and so I'll say yes to anything that you ask.

So, the top policy issues when we were founded 100 years ago is actually one that's quite relevant today, and relevant to where we are which is patents. It was important then and it's important now.

We grew out of the industrial revolution and so were founded in 1916. It was the commercialization of electricity. And so there were all of these gadgets being developed, and who owned the rights to those gadgets, and how you protected the intellectual property was a key issue and continues to be one even today.

MR. STRICKLING: Well, great. And I think that sets the stage for the leadership you

and your organization are demonstrating in this new discussion on Internet of Things.

To that point what is it that really excites you about IoT? What's new about it? Why is ITI putting so much effort and resources into analyzing and understanding this phenomenon?

MR. GARFIELD: In a word, everything. I think Bridget started it off well, and Alan, and the folks who spoke earlier.

I think IoT will be completely transformative, and is. It's often talked about as something that is futuristic, so 2020 and 2025 and beyond.

But the reality is that IoT is working for our benefit today.

So, Bridget talked about fleets of cars. And the reality is that 90 percent of car accidents are caused by human error.

I was driving back on Saturday at an hour that I shouldn't have been driving back. It made no sense that I was driving after being up all

hours the day before. It would have been easy for my car to be in a fleet and traveling more safely than I was at the hour that I was driving.

Some sixty-plus percent of injuries to people over 75 occur in their homes largely because of poor lighting or other circumstances that lead them to trip and fall and get injured.

With smart lighting and smart homes you'll be able to dramatically impact that.

Through climate optimization in our home by 2025 the expectation is that we can cut 9 gigaton of CO2 out of the atmosphere which is reducing CO2 emissions by 19 percent.

And so in every aspect of our lives, whether it's simply saving people's lives, making our lives more enriched, and as well the economic impact, the estimates are that by 2025 IoT will contribute over $11 trillion per year to the economy.

We tend to underestimate value today and so billions doesn't even seem significant

anymore, but $11 trillion is huge. And so I think the impact that it will have in saving people's lives and otherwise transforming the world that we live in will be truly dramatic.

MR. STRICKLING: So, in this environment ITI has stepped forward to convene what you're calling a national dialogue on IoT.

Tell us about what that is, what's the status of that and where you see that going.

MR. GARFIELD: The idea is really to complement the great work that the Commerce Department and others are doing to ensure that IoT's success is accelerated, in simplest terms.

And so, given the transformative potential we shouldn't leave the deployment and success of IoT to chance. We should ensure that the collaboration and connectivity between the public and private sector is well developed and well thought through.

In the same way that the National Broadband Plan at the beginning of this

administration really accelerated the deployment and thinking about broadband, our hope is that through this work we can help to ensure the same around IoT.

MR. STRICKLING: So, what do you see as the work effort and the ultimate work product of the dialogue?

MR. GARFIELD: The ultimate work product -- well, I'll answer in order.

So, the work effort is really talking to the smartest people in the world about IoT. As it turns out many of them are resident in companies that are members of ITI, and getting the benefit of their thinking as well as those participating in the ecosystem more broadly.

The work product will hopefully be truly a roadmap. And so it will be a document that provides insight on how we accelerate the success in deployment of IoT.

And hopefully will build on the great work that the team at Commerce is doing through your

green paper.

MR. STRICKLING: And I know you've also been a proponent for the development of a national strategy on IoT.

Tell me your sense in terms of what we could accomplish with a strategy, and what you would see as the component parts of it.

MR. GARFIELD: The idea behind a strategy, like the idea behind an odometer in a car is really having the critical information and setting a paradigm if you will, a framework for achieving our shared interests around IoT.

And so, about a year ago ITI with our members came up and developed principles for advancing IoT.

They focused on deployment of broadband. They focused on standards. They focused on integrating privacy and cybersecurity, the kinds of principles that are critical and that Bridget and others have alluded to.

And so part of the plan and the idea for

a roadmap is putting more meat on the bones of that skeletal of those principles into something that is actually more detailed in how we drive and accelerate the success of IoT.

MR. STRICKLING: So, how detailed can we get at this point with the strategy?

I mean, I've looked at some of the work efforts of some other nations in this regard and they do an extremely good job of talking about, hey, this is big, this is important, we need to be involved, but the specifics tend to be lacking.

So how do we move past, wow, this is neat to and here's some very specific things that we need to have people focus on?

MR. GARFIELD: Great, great question. All of your questions have been great.

I think Bridget alluded to this as well in her presentation which is -- and the point I made at the beginning that IoT is not simply theoretical, it is real and meaningful and is happening today.

And there's a lot of learning going on that we can move from the 30,000 foot level of this is a whiz-bang great thing to how do we move forward in deploying it.

For example, when we talk about the need for more investment in infrastructure, specifically spectrum, we can move from simply the principle of the need for more investment in spectrum to some of the steps that are necessary to ensure that it, in fact, occurs.

The NTIA through the Broadband Opportunity Council that you helped to put together got recommendations from the public on ways to do that.

We can now move to the next step of, well, which of those recommendations have been implemented, what are we learning from them and how do we advance that.

The United States has taken some significant steps in identifying the particular bands of spectrum around 5G.

How do we advance that and move that forward through the auction process or otherwise.

We talk about the need for public-private partnerships. You could talk about that at the theoretical level, but the Department of Transportation in partnership with Vulcan have come up with a $50 million grant to look at smart cities.

What do we learn from the idea of creating a test bed rather than spreading that $50 million across 10 cities, but going deep on one? Is that the proper approach, or at least an efficient approach as far as driving test beds?

And so, our hope is we can take the next step to what's working and how do we accelerate and go deeper on what's proven to be successful today.

MR. STRICKLING: Have you identified any policy issues or questions for the community that are just really unique to IoT that we haven't really had to address in prior contexts?

I mean, you've already mentioned

spectrum, broadband. Those issues have been with us for years in terms of the need to find more spectrum, and to expand broadband access.

Is there something unique about IoT that's presenting questions we've never dealt with before?

MR. GARFIELD: I think that there are questions that are new in this context, and let me explain that.

So, the medical community for a long while has had to deal with ethical issues around approval of drugs.

In technology we've not had to deal with some of those ethical issues in how we develop and drive innovation.

IoT will force us to think through some of those ethical issues.

NPR did a program the other day on autonomous vehicles, it was one of the illustrations in the presentation, where a car, or a machine may have to decide between driving left

or driving right, which may have difference implications for people's lives.

How do you go through making those decisions?

Also relevant in the medical world has been peer review. Is that appropriate in this context as well?

We have been talking about the issues of inclusivity and their role in more productive workplaces.

There is a study that was released recently on how much more profitable companies are that have women leadership. Not token leadership, but real women leadership integrated in the companies. Dramatically more profitable for publicly traded companies.

How do you ensure that the design within IoT are truly inclusive so you're taking advantage of the benefits of all aspects of our society?

So, these are not necessarily new issues, but some of them are new in this context.

And so we're having to think anew about how do we make sense of them and apply principles that we may have learned in other contexts to these circumstances.

MR. STRICKLING: I'm interested also in your thoughts about how IoT will affect personal responsibility and personal accountability.

There was a story in the Washington Post a couple of weeks ago of a family I think in Maryland that had refused to allow the installation of a smart meter for the utility company because of the fear that that was going to be an invasion of privacy. And they were now facing hundreds of dollars of fees from the utility company for having turned that down.

We look at these sensor-based networks and think about all the benefits they bring to us, but at some point when does it now become our responsibility to adopt these measures simply because of the long-term effects of reducing energy usage, or protecting our children, or that sort of

thing?

How do you see that playing out, and at what point does it become more than just nudging and encouraging people to where it might actually become a national mandate that people have to engage with these sensors because of the benefits they bring to the society at large?

MR. GARFIELD: I think it will be -- those will be societal decisions, but they're important to tee up and begin having today.

I think one of the things that we've been mindful of in our work at ITI and with our companies is being brave enough and humble enough to acknowledge we don't know how this is going to play out.

And so there are things where we know that these issues are coming. How do we begin framing them and teasing out the issues such that we can think them through thoroughly without pretending that we need to define the answers today.

In the same way though that when I grew up -- I laugh because I have memories of driving in my aunt's Mustang with no seatbelts. And today we all get in the car and we think nothing of putting on a seatbelt.

When seatbelts were first introduced they were pretty controversial and most people just didn't want to wear them.

And so I think the same will be true around IoT. There will be certain things that will become requirements that will be incredibly controversial, but in the end society will support them because they'll see it and it will save lives, and other things we just never expect.

MR. STRICKLING: All of the lawyers in the audience remember the motorcycle helmet cases.

MR. GARFIELD: Exactly, exactly.

MR. STRICKLING: As you look at a national strategy and the development of a national strategy we've talked about some of the things that you think should be elements of it.

Are there areas you think really ought to be off limits in terms of developing a strategy at this point? I mean, are there areas of this where you really just want to let the field develop on its own? Or should everything be catalogued and captured in a strategy?

MR. GARFIELD: I think that there will certainly be things that I and others are not smart enough to really develop in depth today.

I think it's important though to create a distinction between thinking about issues, strategizing about them, and proposing regulation.

And there will be a full range of issues because this is so nascent where the underlying principle of do no harm, let's see how these things develop is operative.

That is not to suggest that there aren't areas where government intervention isn't apr.

We've talked about broadband where the United States or the FCC or government has a unique role, and so is perfectly appropriate.

As well there have been conversations already today about standards where Commerce is playing a unique role, whether it's in the Cybersecurity Framework that was developed, or the standards that are being developed today around security around physical things.

And so I think there is a role for government, but there will certainly be areas where it's important to allow investment and innovation and development before there is regulation.

MR. STRICKLING: Yes. Well, I think standards is a perfect example of this in the sense that we've seen some nations who have felt that setting standards now is really important to the ultimate development of IoT.

I think the prevailing view from our comments is that no, let's take this slowly.

So again, you could have a strategy that concludes that it's too soon to be setting standards because of the risk that they'll thwart innovation.

MR. GARFIELD: And I think how you set those standards. And so, the approach that NIST has taken on advancing standards in the context of cybersecurity, or cyber physical structures is largely driven by -- not largely, is driven by voluntary consensus-based global standards.

I came back from China two weeks ago and their approach is quite different. It is less consensus-based, less private sector driven.

And so while standards are critical and should be advanced, I think the approach that's taken here of making sure that they're consensus-based, driven by the private sector, and driven by global practices rather than a unique island approach driven by particular nations is critical.

MR. STRICKLING: Yes. And I understand you've spent a lot of time traveling around the world looking at what they're doing.

What other lessons or key examples have you picked up from your travels to see how other

nations are approaching this issue?

MR. GARFIELD: I think the thing that is clear is that most countries if not all, and I think I was cataloguing. I've been to almost 20 countries this year. It's crazy when I say the number. It's insane. My wife reminds me every day that I'm traveling too much.

But see the value of IoT and its potential for their economy. So, there's a consistency there.

I think there are distinct approaches around standards where the U.S. can play a particular leadership role.

I think there are distinct approaches around spectrum where the U.S. is playing a leadership role around 5G.

I think that in some markets, particularly in Asia, Japan with the potential for the Olympics in 2020 has decided to invest a lot in test beds. I think there's a lot that the U.S. can learn from that.

Korea, the same with the Winter Olympics, also investing a lot around test beds. I think there's a lot that can be learned from them as well.

And so we're hopeful that even though our focus is here that we can share with the United States and the world some of the lessons that we're assimilating from our travels and what our companies are seeing as they operate on a global basis.

MR. STRICKLING: So, as we look at the role of governments you've indicated that there's clearly an important role to be an enabler, or a facilitator, or a funder. Maybe less important today for government to be thinking of itself as a regulator.

The enabling and facilitation role probably requires money. How do you see building the national consensus to actually get a commitment from the next Congress and the next administration to actually put some dollars behind this?

MR. GARFIELD: Two elements to that. I think convenings like this are critically important. And so making sure that people understand the potential and that investing in IoT is truly an investment.

And so the idea of an $11 trillion return to the economy is real and meaningful, it's not speculative, and we can speak to that pretty specifically based on what's happening today so it's not some mystical concept, it's truly real.

I think then cascading this conversation so that the public has a deeper understanding of IoT and isn't intimidated by it is important.

I think the last element I'll add is that the U.S. government has a critical role in all the ways that you just spoke to, but also as a leader in purchasing and using these technologies.

MR. STRICKLING: Good point.

MR. GARFIELD: And so there is the opportunity for the United States government to be

a leader in the deployment of these technologies and just using them and integrating them in their own fleet.

MR. STRICKLING: Excellent point. Very important point.

Let's wrap up with just -- I'll give you a chance to look ahead, say, five years. Let's look to 2020.

MR. GARFIELD: It's no longer five years. It seems so far away.

MR. STRICKLING: How would you define success in four or five years into this?

MR. GARFIELD: I think success will be achieved if we can tangibly show the impact in the ways that we've been talking about.

So, lives saved, whether through the deployment of autonomous vehicles or otherwise. More particularized medicines.

So, improving people's everyday lives. I think people will get it and see it and want to invest in it.

I think if we can show the return to the economy in the ways that we've talked about that people will get it and want to invest in it more.

And if we result in new and exciting innovations that we can't contemplate today but that result in the cure for cancer, for example, will be a way that I would define success.

So, it is really around the impact that it has on people's lives.

MR. STRICKLING: Okay. You're putting down a pretty high barrier, but let's hope it comes to fruition.

MR. GARFIELD: Having worked with these companies for seven years the one thing I know is that the timing may be a little bit off, but they always exceed expectations. And so, I feel comfortable that it will be achieved. Maybe 10 years instead of 5, but it will happen.

MR. STRICKLING: Well, thank you so much.

MR. GARFIELD: You're welcome. Thank

you.

MR. STRICKLING: Please join me in thanking Dean for his observations.

(Applause.)

MR. HALL: Great. And if I could welcome the technology panel to the stage.

MR. JILLAVENKATESA: Good morning and welcome to the technology panel.

So, this is I would say certainly perhaps the most exciting panel for a start clearly between our panelists and certainly these early remarks which set the stage I think just for a range of different issues that we can explore as part of the panel.

And to me what's particularly striking are some of the common themes that we heard between Bridget's talk and between Dean's observations.

And what we saw were themes of issues like spectrum, standards, interoperability, mobility, 5G.

So, these will be some of the things

that we'd really like to understand, particularly if we assume that the Internet of Things is a system of systems type framework.

We're not talking about one technology, we're not talking about one application, but a range of applications.

And the opening speakers really laid down the challenge for us which is we can think about this as what the private sector does.

We can also ask some questions about what's the government's role. How does the government work with the private sector?

And so these will be some of the themes that we'll try to explore as part of the panel.

And if we can come away from this discussion with some key takeaways about what are the important technology-related opportunities, challenges.

What's coming down the pike? How can we construct certain government approaches? How can we validate existing approaches and what can

be learned from previous experiences?

That really sets the stage both for us at the Department of Commerce and certainly for the federal government at large to kind of see what is it that we need to do in order to really foster both the development and the deployment of the Internet of Things.

So we have a really distinguished panel over here. And what we'll do is have each of our panelists provide about three minutes of opening remarks to set the stage for some questions where we'll explore these issues in a little bit more depth.

And then we'll open up the floor for questions from you all. So, we have about an hour or so for the panelists.

I'll start out with the introduction of our four speakers, and then I'll invite them based on alphabetical order to come and provide their remarks.

Our first panelist to my immediate left

is Hilary Cain. Hilary is the director for technology and innovation policy at Toyota, and she handles policy issues relating to connected and autonomous vehicles including data privacy, cybersecurity and spectrum.

And previously she was on the staff of the U.S. House of Representatives Committee on Science, Space and Technology where she served as the staff director of the Subcommittee on Technology and Innovation.

And Hilary had a key role in developing the technology projects in the America Competes reauthorization.

Our second speaker is John Godfrey. John is the senior vice president for public policy for Samsung Elements America.

Based here in Washington, D.C. he leads Samsung's public policy formulation and engagement with government and industry, and has a particular focus on communications policy, digital television, wireless spectrum, healthcare,

environment, broadband accessibility and other areas.

Sterling Rooke is the president of X8 and he's also the founder of X8, a technology company that's focused on industrial sensors in cybersecurity.

On a part-time basis he also serves as the director of training within a cyber operations squadron in the United States Air Force.

And prior to this he was an engineer at the Johns Hopkins University's Applied Physics Lab where he specialized in systems engineering of national security information systems.

Ken Tobin is the director of the Electrical and Electronic Systems Research Division within the Energy and Environmental Sciences Directorate at Oak Ridge National Lab.

Ken leads an organization of about 150 staff who are involved in R&D in electronics, sensors, communications and controls for energy efficiency, resilience and security.

And he has authored over 170 publications and holds 14 U.S. patents.

So, we have a diverse and expert set of speakers here who can really help us explore the complexities around technology aspects of the Internet of Things.

Hilary, if you'd like to get the conversation started.

MS. CAIN: Sure. Thank you so much for having us all this morning.

I get very excited when we come together and have these conversations about how we can work together to advance the Internet of Things and provide clarity around the government's role.

The problem is I'm not sure that clarity is possible, and here's what I mean by that.

I think the Internet of Things means a lot of different things to a lot of different people. And it's not because we're unwilling to come together and sort of have a kumbaya moment where we figure out exactly what it is, and where

we're headed as a society.

It's because it actually is a lot of different things. So it's very hard to sort of put it in a box and wrap a pretty bow around it and declare victory.

And for me in the car space which is the perspective that I'm bringing to this I think it's quite pronounced in the fact that it means a lot of different things.

So, what is the Internet of Things when it comes to the car?

Some people would argue -- not me, but some people would argue that now that you can access the internet while you're in a vehicle, you can access your Facebook page, or make a dinner reservation, or listen to Pandora that that is the Internet of Things. Because it's the internet and it's in a thing so therefore it's the Internet of Things.

You could look at Internet of Things as being the ability to access services that are

enabled by connectivity.

So, automatic collision notification. You're in an accident. Your airbag deploys. Emergency responders can be dispatched to the scene of the accident.

Or the ability of manufacturers to monitor vehicle performance and operation, to do a better job of identifying potential safety defects and pinpointing remedies to those defects. That could be the Internet of Things.

You could be talking about the ability of you to interact with your vehicle from your smartphone.

So, preheat or precool your car from the kitchen before you head out in the morning, or check to see how much gas you have left as you're leaving the office at the end of the day from your smartphone. That could be the Internet of Things.

It could be the ability of vehicles to communicate to other vehicles, or with roadside infrastructure primarily focused on collision

avoidance and reducing the number of crashes that we have. That could be Internet of Things.

Finally, you could be talking about your car interacting with your home. Your lights flip on as you turn the corner onto your street at the end of the day, or your door locks as you're pulling out of the driveway in the morning.

These are all legitimately Internet of Things when you're talking about the car, but they each have very different policy implications.

The spectrum needs are different. The infrastructure needs are different. The interoperability requirements are different. The privacy and security tradeoffs are probably different depending on what you're talking about.

So as we have this conversation today I think it's important to just recognize that we're talking about different things all under this umbrella of Internet of Things, and that there's no one size fits all policy strategy that's going to address all of them at the same time.

MR. GODFREY: Thanks. I agree with Hilary that the Internet of Things is not just one thing.

I think it's useful to think of the Internet of Things as really a new phase of evolution in the internet.

It's what will bridge the digital world and the physical world together into one very complex and diverse system.

So, what can government do to help foster this transition and make sure that our society and our economy get the maximum benefit from it?

There are many, many roles for government to play. We've already heard about some of them today.

I would focus on three S's - spectrum, standards and smart government. You probably thought Samsung was going to be one of the S's, but that would be cheating.

But spectrum. We need the government

to make sure there is enough spectrum at low and high frequencies for fixed and mobile use, both unlicensed and licensed, low data rate, high data rate. All of those things are going to be necessary for the IoT.

I'm not saying that the government should designate a band and call it the IoT band. I think that's the wrong approach.

I think the Federal Communications Commission and NTIA have done wonderful things for the U.S. economy and for world leadership by bringing spectrum into commercial use without hamstringing it to a particular use, but rather making it open for innovation.

Second, standards. I don't think we need the IoT standard. There's not one standard that's needed.

Instead, what we need -- and this is a role NIST is extremely good at -- is to foster information exchange, clearinghouses of information, common taxonomies, ways of talking

about technology, but letting the private sector take the lead in developing the standards.

I know we'll come back to more detail about standards.

And finally, smart government. I think there's great potential for the government to lead as a user of IoT in meeting government mission needs, and in doing so not only making government more effective, but also setting grand challenges for the private sector and the academic community to innovate and develop new ways of using IoT and that will bring things forward. Thanks.

MR. ROOKE: Okay, so my name is Sterling Rooke and it was previously said, I'm with a technology company called X8. And we're focused on industrial sensors and also cybersecurity.

And first I wanted to also say that I own a Toyota and have a Samsung Note 5. And then I'm going to have a small challenge for the two previous panelists on my last slide, so it's going to be interesting. It's topics.

Okay, so this is just one view of the Internet of Things. And I've only got three minutes so I'm going to move quickly here.

So, we can look at innovation. Innovation is really important. It's something that's been alluded to already at this workshop.

And the government can really help drive innovation. And frameworks have been discussed previously. So I think that's a role that government can come into play and also innovation can be driven by the government using IoT and purchasing it which has also been mentioned.

And we do face an unsettled IoT environment right now. So anything that can be done here would help with innovation.

One common theme that's already been mentioned, but it's really interoperability and spectrum sharing. That's another place the government can come into.

And also, as was previously stated,

there's going to be billions and billions of points, measurement points in many, many devices out there.

So, some kind of intelligent spectrum management, whether it's cognitive radio or what have you is going to have to be implemented and recommended.

So, and then also too I've got on the slide active versus passive IoT. That could be a concept of where Internet of Things devices are dormant, or not active. And maybe when they're queried or energized and interrogated maybe they come alive at that point. That could help with spectrum sharing as well.

So, cost and applications. This is where I get into something that's a little controversial which will end with the last puzzle piece.

But I really think that the driver of cost will not really be the hardware. It's kind of a Debbie Downer to Intel maybe and stuff, but

I really do think that -- I think that cost will start to go down as more and more products are made, and processes are cheaper.

I think some of the cost is going to revolve around innovation and software. But I think a lot of the hardware cost will go down further and further.

And so, the real example to bring that into play is whenever you buy a smartphone, do you pay extra because it has a camera in it? Maybe back in the day you did. When you bought a phone you had to pay more to have a smartphone with a camera, or back when there were not smartphones.

But now I would really say if you wanted to buy a phone with no camera you'd probably pay more.

So the point I'm trying to make there is that I think all these features like embedded Internet of Things will be freebies. I really think that.

So, the real cost as I see it partially

because X8 focuses on cyber, and industrial controls, and sensors is I really think the cyber cost. That's something that we have not mentioned yet today.

But I think that the more connected these devices get, and the more we depend upon them if the government does not try to have some kind of recommendation, or some kind of standard, or something to try to include cyber all these basically attack points, the surface area, the attack surface area is going to by definition go up. And I think that's a major weakness.

If society is dependent upon this cyber could actually cause some kind of an issue.

Okay. So, these are things to think about I've thrown up here. Maybe this could spur some discussion.

If you look here modern environments could allow for human identities to shape IoT devices as you come near them.

And I've got down here a chip embedded

in hands. Now, at DEF CON they were doing this, by the way, putting chips in people's hands, like RFID chips.

But in all seriousness, maybe IoT could actually adapt as people come by, and the devices in a building or what have you could actually understand who the person is and adapt to that person.

So, I really see it as a societal thing. And I think it's the society of things rather than the Internet of Things, to jump ahead a next generation.

I really think the devices will form a society, and communicate with each other, and communicate with the people. And it's all-inclusive.

And the challenge here, the discussion to Samsung and Toyota. I think it's really important. It's probably stuff they've already thought about, but how will the Internet of Things interact with mobile devices?

And then in the future it's kind of known that cars will be self-driving. Maybe in large cities people won't even own cars and they will just hop into a car that pulls up, and then that car should become that person's car if you will, already know where they're going to work and what have you.

So I think it's a combined thing between the Samsung device and Toyota. So it's right in their wheelhouse.

And that's it. That's my three minutes.

MR. TOBIN: Thank you. So I'm Ken Tobin. I'm with the Oak Ridge National Laboratory which is the Department of Energy's largest science and energy laboratory.

We're about a $1.4 billion annual program that does quite a bit of research in energy efficiency areas, energy resiliency, energy security.

And so for my three minutes I thought

I'd focus on a couple of things.

This is just, I'm a pictorial person. This is another view of the Internet of Things. Everybody has probably seen some version of this. And whether it's healthcare, or manufacturing, or energy there's the similar layers of complexity in terms of the sensing modalities that are becoming available today, and developing devices which are more energy efficient, and do a better job of computing down at the low level so we don't have to expend energy through the RF communications that are there.

Sharing spectrum. Developing capabilities and technologies for the cloud aspect of understanding where our data goes, who has access to it, what the security levels are, what the veracity of that data is, all for the purpose of being able to aggregate that together and make high-level control decisions for our comfort, for our economy, for all those different benefits that come from it.

So, I think when we're talking about the energy IoT I think it's wonderful that we can check what our thermostat is set as from our office and see what our home is doing.

But the real benefit and power of the Internet of Things when it comes to energy in particular but in other areas as well is really going to be, and this is in my opinion nascent today, is in the machine-to-machine piece. So, devices talking to devices.

And this is just beginning to happen. But eventually really what you want is your thermostat to talk to your electric utility so that it can buy power when it's cheap, and turn itself up or down when it's not.

And so your utility can actually transact with your homes, your buildings, and eventually when we have more electric vehicles let's say transact with those battery storage capabilities across what could potentially be millions of vehicles in the nation to help control

power distribution and resiliency, and things like this, optimization on our electricity grid.

We aren't there yet, but that's really where the power is going to come from in the IoT age as we go forward.

So, I think one of the roles that the federal government really needs to take in working with the nation is in these government, industry, utility, academia partnerships.

At the laboratory at Oak Ridge we're part of something right now which is called the Grid Modernization Lab Consortium which is actually quite a few national laboratories, six that are taking lead roles around the nation working in developing technologies for creating an advanced grid infrastructure.

And so the ability to do work with our local regional partners like the Electrical Power Board in Chattanooga, or Kellogg's, or United Parcel Service to help develop, for example, new capabilities for micro-grid technologies which

will give them advantage in cost savings, in reducing their carbon footprint, things like this.

It's very relevant to the kinds of relationships that need to exist in order to move IoT capabilities forward.

And so let me close just by showing a wonderful example of industry, laboratory, academia partnerships.

This is -- think of this as a nanogrid. This is an additively manufactured printed home and vehicle that Oak Ridge was able to produce using a very large-scale polymer printer. We actually just entered the Guinness Book of World Records for printing the largest polymer element for a relationship that we have with Boeing. So, kind of interesting.

But the beauty of this is that this is a stand-alone nanogrid if you would. There's photovoltaics in the roofing. There's a bidirectional wireless power transfer between the vehicle and the home.

There is a connection to the grid and it's all automated. So, how that energy flows, how that energy is used is sensed and transacted and managed between those two elements, three if you consider the grid, in a way that demonstrates technologies and capabilities in a very useful way.

And the work is done in partnership with everybody from architectural firms like SOM to Clayton Homes, to EPB Power, to all those kinds of relationships are what make these things work well.

And with that I'll conclude.

MR. JILLAVENKATESA: Thank you. So, these are great comments to set the stage to perhaps start exploring some of these issues a little bit more in detail.

My first question for the panelists, and you can choose to answer it in any order that you folks feel, we certainly focused a little bit on the challenges in terms of the technological issues - lack of standards, issues of interoperability.

But if you flip that and instead focus on opportunities from where you sit within your industries what do you see as the most exciting technological developments that are coming down the pike that will really help develop and push the deployment of the Internet of Things and its applications? If you had to pick one or two. And please, feel free.

MR. TOBIN: Well, I guess personally I would have to emphasize once again the machine-to-machine communications piece.

That's, as I mentioned it's very kind of rudimentary in what we're doing today.

And there are a lot of issues around how that's going to move forward that don't just have to do with the way we can control the interactions between our devices, but the physical and cyber physical security that has to exist so that those devices and elements can be protected and perform as they're supposed to.

MR. ROOKE: Yes, so that was most -- a

lot of what I was going to say. I mean, that's part of my society of things if you will type complement is really that's the next thing.

Because right now a lot of devices if you will communicate with the cloud and to a database, and algorithms are run in the cloud like Lambda with Amazon, and things are done in the cloud.

But I think that will be augmented by devices directly communicating with each other at shorter distances wirelessly. So I think that's part of the future.

And to dovetail on that I think privacy is going to be a concern. I mean, that's going off on a tangent a bit, but the public always has an issue with privacy so that's something we're going to have to figure out as we proceed in that direction.

MR. GODFREY: Ajit, I'll give you a specific answer and then maybe a more philosophical one.

The specific answer I think very exciting is the development of 5G mobile networking. And that's a big, complicated topic.

The networks will be lower in latency, more reliable, more energy efficient, provide more evenly distributed quality of service.

But maybe the most kind of gee-whiz exciting part is the incredibly high data rates that are going to be possible with 5G.

And a lot of that is thanks to the FCC's action this summer making available a record amount of spectrum, almost a gigahertz for commercial mobile use in the high-frequency bands at 28 GHz and 37 to 40 GHz as well as unlicensed use above 64 GHz.

And that's an area that Samsung has been very active in. We're involved in trials with Verizon here in the U.S., a test bed initiative with the National Science Foundation, and in Korea leading up to the Pyeongchang Winter Olympics in 2018.

So there's a lot going on in 5G and the United States is in a position to be a world leader thanks to having set aside that spectrum.

And by the way, IoT will include very high data rate applications. It's not only sensors with very low data-intensive applications like turn me on, turn me off.

There's definitely going to be video involved, and cloud computing, and large amounts of data in IoT.

The more philosophical answer is briefer. I'll just say that I think it's very exciting to imagine what intelligence will emerge that we can't predict today from analyzing data that's collected across different domains.

So, as long as the standards allow for -- standards and laws and regulations allow for interconnection and aggregation of data from vehicles, from healthcare, from retail, from the transportation grid, from your home.

As long as that data can be brought

together new services, and new insights, and really whole new industries are going to appear around that that we can't even imagine today as long as government doesn't stand in the way of allowing that to happen.

MS. CAIN: So, 35,000 Americans die in traffic accidents, traffic crashes each year in the United States. So, to put that into perspective that's roughly two jumbo jets full of Americans falling out of the sky every week.

Now, if two jumbo jets full of Americans were falling out of the sky every week we'd all have hell to pay, right? There would be a call for a national solution to this problem.

We have a solution to this problem and it's connected and automated vehicles. So I think we see as the biggest opportunity the ability to bring that number dramatically down.

And just to note, the number is actually going up, disappointingly. I mean, it's been going down for decades. We've made really

significant advances in reducing the number of people who die in traffic accidents.

And it's actually on an uptick now. And so all the more reason to do this as quickly as we can.

MR. JILLAVENKATESA: These comments really set the stage for exploring another issue and that's the societal acceptance. And what are the factors that really impact societal acceptance.

At the end of the day any technology's success really depends upon how willing are people to use that technology, how responsively we address those concerns.

I think what you folks have made amply clear is two of the issues are cybersecurity and privacy.

From a technological perspective how do we start addressing the challenges around cybersecurity, around privacy?

How do we build in the roots of trust,

whether it's in the hardware aspects, whether it's in the software aspects of these.

And do we have the right foundation right now, or do we need to actually focus on addressing some of those foundational issues? So, welcome any of your thoughts.

MR. ROOKE: So, a quick thought I have on that since that's kind of in my wheelhouse so to speak is I think what hits on both of those is really identity management. That's one place we can start to peel this onion apart.

It's identity management of the devices themselves and the persona, the cyber persona or the person itself.

So I think that's a good place to start digging, and I guess we can start pulling it apart there. But maybe that's a good place to start.

I think getting that defined is very, very important. And having encryption that enables that between devices is something that really has to be done. Work needs to be done there.

MR. GODFREY: I would say there's probably not -- one thing to keep in mind is it's not that IoT security is an entirely new topic. Internet security is something we've been grappling with for decades. So we have a foundation in place.

And NIST has played a really valuable role in fostering the cybersecurity framework which has helped provide guidance and set best practices that has greatly moved industry forward.

Also, other agencies like the Federal Trade Commission have issued really valuable, plain language guidance to consumers about protecting themselves and to small businesses.

Now, Sterling, you did mention something that is a somewhat unique new element of the IoT security problem which is device identity management and authentication.

Because in the IoT space the devices may not be physically in the possession of their owner all the time.

And so the identity of who owns this device may be a little less clear. So that's an area that maybe needs some more exploration.

I'm not 100 percent sure, but I think NIST's work on cyber physical systems should be exploring that if it's not already.

MR. TOBIN: I do think that on let's say the cyber physical aspect we really have only just begun to do the work of building that cyber protection piece into the devices themselves.

So, if you think about devices that are used in systems for energy delivery, or control systems for manufacturing, having a device recognize if it's running out of spec if you would, meaning that you need at low cost a more powerful embedded computing locally so it can understand something about its operating parameters, and what's reasonable, and what's not.

I think those are the kinds of directions that we need to be able to go into.

Anyway, cyber is a huge piece of that

and we're just now beginning to implement some of that architecture or structure that can start looking at it from different perspectives.

I think encryption is wonderful, but if you have two devices A and B that are encrypted between them and A has been compromised it doesn't matter if you're sending protected information. The information you're sending it is potentially damaging. So, there's a lot of work to be done.

MS. CAIN: So, I think in the car space we face sort of an interesting conundrum here, maybe more so than some other industries. Maybe I'd put medical devices in the same category.

Cars are unique in that there is -- people view their cars as sort of like an extension of their homes. There's sort of this maybe unreasonable expectation of privacy when you get into your vehicle for a lot of people.

At the same time if there were to be a cyber attack on a car you're talking about potentially somebody losing their lives.

So even though we've talked about this tension between privacy and security in lots of other contexts I think it really comes to a head in the vehicle space.

Because on one side we've got a group of folks yelling at us about fear about monitoring them and tracking them.

And at the same time we're being yelled at by another group of people about how we're not doing enough to monitor and track what's going on in our vehicles in case there's a cyber attack.

And it's really hard to reconcile those two pieces and get to a place where everyone is satisfied.

I think we're going to struggle with that tension very profoundly as we move forward in the Internet of Things.

MR. JILLAVENKATESA: Continuing on this track about the challenges around cybersecurity and privacy I think there's another interesting element.

We all recognize the importance of building in the right capability within the devices within the sensors.

But there's also this very interesting dynamic in many of the sensors, there's this race to miniaturize, make them smaller, make them consume less power, make them faster, more responsive.

So, how do you strike this balance between ubiquity of sensors, of devices which means they have to get smaller, they have to consumer less power, we don't want to be charging these.

But at the same time building in this hardware, whether it's for encryption, whether it's for identity management. Whether they have radios in them where they need to communicate and this information is not being stored on the device itself.

Any thoughts about, you know, what's the framework in which we approach this?

And I think one of the other interesting

layers over here is we know that encryption is constantly under stress. We come up with a new encryption scheme. People are out there trying to figure out how to break it. So, clearly we need to move into more robust encryption methods.

So, any thoughts on how do we take on this challenge?

MR. GODFREY: I'll take up that one, Ajit, because my company makes those devices. We make sensors and processors for IoT. And so we're very aware of that issue.

I think the answer is Moore's Law. I think that the advances in semiconductor manufacturing continue to bring down the cost.

And the cost going down is fine because it means the volume goes up.

So, just to share some information about Samsung's product line, we have an IoT chip family called ARTIK, A-R-T-I-K, which is optimized for IoT.

Small size. Low energy use. But

maybe most important, security built in at the hardware level. So there's a secure embedded element which is in the hardware, will be tamper evident if somebody tries to compromise that.

And from that, secure boot to make sure that any software that runs on top of the chip is either authenticated or it's going to be rejected.

And the more of that kind of hardware rooted security is throughout the IoT architecture the better for security.

Now, maybe not every single node in the connected web of IoT has to have the same level of security, but the more authentication -- it's not only encryption, it's also authentication and integrity management that's out there, the more secure the system will be.

MR. ROOKE: I don't have a whole lot more to add because a lot of it was taken already. The thunder was stolen.

But definitely doing hardware encryption is the way to go for less power

consumption. And it's definitely way more secure.

And if you have the process, assuming you don't have a supply problem which can always be a problem. You never who's doing what to your hardware because things are made around the world.

But assuming you don't have that, if you do hardware encryption it's very, very difficult for an adversary to really know what's going on.

MR. TOBIN: I would also add to that that there's a spectrum of sensors that will be available out there.

And at some level you'll have devices which have a fair level of complexity, and local computing, and encryption issues, and cyber physical kinds of things that will be very important.

But it's also important to note that we're now also starting to see a whole category of sensors which are things like these RF-SAW devices.

You can look that up later if you want to, but these are passive devices that are turned

on by shining RF on them. And they can be functionalized to give you one simple measurement, a temperature, or a humidity, or something along those lines.

And so the device itself doesn't really have to be secure. What has to happen is the reader, the place where you aggregate maybe multiple tens or hundreds of those little, cheap -- and by cheap I mean sensors that can cost as little as a dime in consumable materials, but where you bring those together you need to have that kind of configuration to protect and make sure the data coming back is correct.

But there's a whole spectrum of kinds of devices out there that you really have to look at. There's not a simple answer I guess is my point.

MS. CAIN: Well, I'll just add in terms of the car context we definitely need the cost of the sensors to come down.

I'm sure you all have seen those

self-driving prototypes driving around. The sensors on those things are multiple times the cost of the car itself.

So, we're at a place right now where the car is probably going to be out of reach for most of us in this room, let alone most of your average consumers. So, sensor cost is a big technological challenge for us going forward to be able to sell these things in the mass market.

MR. JILLAVENKATESA: So, we can switch tracks a little bit. I think I have a set of issues over here which I want to explore it in the context of the framework of public-private sector partnerships. I think that was something that was alluded to by various speakers this morning.

And as we look at issues of interoperability, standards which is truly a public-private sector partnership based undertaking in the United States, exploring issues of spectrum, availability of IP addresses, if we can explore that a little bit.

But before we get into that particular set of issues what I'd like to do is invite our audience who may have any questions to -- we have a couple of microphones in the room. If folks who have questions would like to either raise their hands so I have a sense for approximately how many questions, or if you'd like to line up near the microphones or sit near the microphones we'll then transition after we explore some of these issues.

Great. We have a couple of questions in the room.

So, the role of public-private sector partnerships. There were references made to, for example, the NIST coordinated cybersecurity framework which was done in a truly public-private sector partnership.

Standards development, particularly consensus standards development happen almost exclusively in private sector-led standards developing organizations.

These have been some of the bedrocks

which have really defined the U.S. approach to many of these technological issues.

So, I would really like to explore some of these issues. If you folks could share perhaps a couple of things.

Whether it's spectrum, whether it's interoperability, whether it's standards what are some lessons learned from successful examples of public-private sector partnerships, the role of the government as a convener to bring together often folks who have very different interests, but are all working in a similar set of issues, and how can we strengthen particularly our approach to public-private sector partnerships?

So, some thoughts to get from you folks.

MR. TOBIN: I'm not so much the standards person as looking at sort of the new technologies, but I do understand standards from the point of view of the old adage that the wonderful thing about standards is that there's so many of them.

And I think that we're seeing that in the IoT area in particular. And everybody who's kind of working a particular standard in a certain area thinks that their particular standard is the way to go, and that's okay.

In a marketplace economy we do that. And you always have your Betamaxes and your VHS's at the end of the day, but it takes time to get there.

But I do think that sort of the government-industry interaction kind of helps to meter that, to allow people to look at some of the -- and of course I'll go back to where we're focusing a lot of our energies which are things like grid modernization.

In order to do that you can't have 100 standards from 50 different groups in order to make progress there. You've got to get people to work together.

And over time those kinds of partnerships, those kinds of big demonstration

projects will lead to new products, new markets, new integrations into these large infrastructure facilities and such. And that's a very good thing as we go forward.

I think on the transportation side it's absolutely an analogous situation.

MS. CAIN: Yes, and I can jump in on that.

You remember I talked about the different types of Internet of Things and the car. One of the things I talked about was vehicle to vehicle, and vehicle to infrastructure communication. And I'll just focus in on vehicle to vehicle for a second.

The interoperability piece is essential. You have to have all cars speaking the same language or else it's not going to be a very effective vehicle communication network.

So, if Toyota cars can't talk to Ford cars we've got a problem. If Toyota cars today can't talk to Toyota cars that come on the road 10

years from now we've got a problem.

And so a lot of work has gone into public-private collaboration and the development of communications standards, interoperability standards to support that network.

I can tell you it's a source of great frustration to me because I think the development of these standards has been a poster child for how public-private collaboration and partnership should work.

And then now that we're at the one-yard line there's some Monday morning quarterbacks who are second-guessing sort of what we did and how we got to it which is complicating things.

But how we got to where we are today is a model for how public-private partnerships work between the auto industry and the Department of Transportation.

MR. GODFREY: It would be a mistake for the government to speed up the interoperability process by stepping in with law or regulation and

picking a standard.

That very likely will lead to rigidity, getting in the way of innovation, not reaching the right final answer.

It's worth taking the time to allow the public and private sector collaboration to find the right interoperability standards, whether it's for IoT or any of the vertical applications within the IoT space or the internet.

The economies of scale and scope from interoperability are so great, the opportunities are so real and so large that they exert this strong gravitational pull in favor of open systems and open interoperability.

So, it's really worth relying on the market forces to get you to that point.

And one of the forums that Bridget mentioned where that's already happening is the Open Connectivity Foundation. Samsung and Intel are cofounders of that. Really trying to develop a framework for interoperability across the

different parts of the IoT.

And that's something that government is welcome to participate in. Government is a very important user community.

It's not something that needs government to step in and mandate through regulatory choice.

MS. CAIN: So, can I pose just -- I'm interested to hear folks' perspective on this. Because I struggle with this quite a bit in the car context.

So, a car is the second most expensive thing you're probably ever going to buy in your life besides your home. And you're going to have it for about 12 years, 11-12 years on average.

So, this the market will work and we'll figure this all out isn't really a great proposition for a company like Toyota who wants to sell a vehicle that you're going to be really ticked off if that thing only works with half of the Internet of Things and not the other half, or that

doesn't work two years down the line.

It's not your phone. It's not something you replace every year or two.

MR. GODFREY: I think what I mean is there is a role for bridges and interfaces and adaptors.

So, you could have a Ford car talking one standard, a Toyota car talking another standard, and some cloud service or some device that simply translates between the two.

It's not that you pick a standard and you're stuck with that for 12 years and can never interoperate with anything else.

MR. ROOKE: Yes. I guess to follow on that directly and then I'll make another comment, but I think -- how many of you have rode in a Tesla before, or have a friend who has one? Yes.

So, they're pretty amazing in the sense that they do live software provisioning and updates.

So long as the hardware is agnostic and

extensible enough if you will you can push updates as required to modernize the vehicle to some extent. So that's one thing.

And then I guess with regard to the public-private partnership and how the government can get involved, and the engineer in me, I'm going to actually step back and take a different turn.

I hate to say it, but I think almost the lawyers and the policy people need to be involved.

Because we've mentioned privacy before. But I think the government can step out and implement Internet of Things and push the edge there and define laws with privacy and how to deal with the public so that companies can come along and with confidence build IoT devices that are compliant with law and the privacy of the public.

So, I think that's one role the government can really play is to just go out and do it so that can be defined.

MR. JILLAVENKATESA: Interesting comments which we can explore if we have time.

But let's perhaps switch tracks and see if we have any questions from our audience. We have a couple of questions. If you could please come up to the microphones in the room.

And if you'd also like to say whether you are asking a particular panelist to address the question, or whether it's for all of the panelists.

MR. SUBRAMANIAN: Thank you. Rangam Subramanian. I work for the NTIA.

Now, on the Internet of Things let's focus on the word "internet."

You know, this IPv4 has been a blessing, but it has also been a chaos right now. If you look at it from a security perspective.

From an IoT sense where do we go from here? Is there something that we should really invent and apply? And what role that the government should play in terms of getting a new routing a safe, secure routing grid.

MR. ROOKE: I was going to say, safe and secure is only as good as the next hacker. So,

what's the safest system the adage goes is an unplugged system.

So, what we're actually doing is we're doing the opposite of an unplugged system. The Internet of Things is going to be ubiquitously connected and deployed.

So, therefore, yes, you're correct, that's a conundrum is the attack surface. It's always on. Everything is connected.

So I think work definitely needs to be done in this area. I think it's a challenge.

MR. GODFREY: I am not an expert in IPv6 but I think that's the direction things are moving. And we'll get there because you need the extra address space.

MR. SUBRAMANIAN: I have one more question.

We didn't address this. From the international perspective where do you think United States is from an IoT, pushing an international technology?

Is there anything unique that the nation should do ultimately to have leverage from an international technology perspective?

MR. GODFREY: Success stories. If the United States goes to international forums and can show that the U.S. model of public and private sector collaboration works I think that's a powerful example to show to other countries where they may be starting from the idea that the government is going to pick the standard, pick the spectrum, pick the use case and fund it.

And then they say to the U.S., well, why are you behind. You haven't picked the IoT standard yet like we have.

Well, actually, the U.S. is on the right path there. So, success stories.

MR. JILLAVENKATESA: Great. We have a few speakers from the floor. We'll start with the gentleman in the back and then go front, please.

MR. NEW: Hi. Josh New with the Center for Data Innovation.

From an international perspective I know the Department of Energy runs a couple of working groups or forums that specifically focus on international smart grid interoperability in terms of internet standards are cohesive, and they're industry led, and they're not kind of mandating any specific national standards.

Do you think that has been effective? Do you think that model could be applied to other areas like transportation, like consumer smartphones, things like mobile wallets?

And if not, what role do you think the U.S. government should play in kind of coordinating these international efforts beyond just saying we need these to be not mandated by a country. How can we ensure that everyone is on the same page?

MR. TOBIN: Tough question. You would have to look at the outcome of what the DOE is doing in these areas.

But I think the idea of not -- of being able to demonstrate positive results through what

we do in this country versus mandating or specifying directions is the critical piece.

I'm not adding much in my comment here, but I do think that the federal government can't and shouldn't mandate the standard or a set of standards, but should allow those to organically come together.

And what the government needs to do is demonstrate through big platforms how they work together because that will drive where those standards go, and how they're adopted, and how they become part of the marketplace.

MR. SZABO: Thank you. Carl Szabo with NetChoice.

First of all, Hilary, I think you should get Dean one of your self-driving cars as soon as possible. It seems like he needs it.

Question for John and the rest of the panel.

A lot of the comments have called for government mandated disclosures by businesses of

tech specs, access to source code, the ability to kind of tinker with your devices.

Can you talk about how that would detrimentally impact the ability to secure and protect these devices, and the ability to keep hackers out.

MR. GODFREY: I admit I don't think I've read those particular commenters' requests so I don't know what their argument was, but disclosure of our trade secrets or our intellectual property would not go over very well.

And more generally mandating that systems are open, mandating that there be open access points, or open APIs as you sometimes hear people call for I think is generally not necessary for the reason I outlined earlier.

There's such opportunity in open systems and such a market force driving towards open systems that truly closed off systems will fall behind in the marketplace over time.

Not every time, but I think there's a

general advantage to open interconnection, especially in something like IoT where no one company is going to make a car, and a wearable, and a retail point of sale terminal, and a traffic light, and you know, all the components that need to talk to each other. So everything needs to communicate.

MS. CAIN: So, I think where you may see that tension the most is in highly regulated industries who are now coming online because you find yourself in a place where automotive, medical devices again, where your regulator says jump and you have to say how high. And it's just the world that we live in.

And so when the regulator says hey, we're a little worried about cybersecurity, we'd like you to turn over X, Y and Z so we can take a peek.

Or, hey, if we're going to do this automated driving thing we're going to need you to share a whole bunch of your data and information

with us so that we can have confidence that it's safe.

So, I think in the industries that have had the benefit of not being regulated in the past I think there's less of a conversation there in that space.

But I think you are seeing it for example in the automotive space, medical device space, in these traditionally heavily regulated industries.

MR. ROOKE: So, I think from the perspective of showing test results and performance, I think that's really great.

But I have one acronym and it's OPM. Remember the Office of Personnel Management hack? Some of you've gotten letters who were unfortunate.

So, you know, I think that some companies really may look at that and say hey, if we share our source code with the government is it really going to be protected.

If there are secrets there such as --

remember the Apple phone case. And I don't know if you saw the interview with General Michael Hayden where he was talking about it I think on Fareed Zakaria.

And of course he's an authority since he was the CIA and NSA director, but he said absolutely Apple should not be providing any kind of back door to its encryption or what have you because that just opens it up to attack then. And that's something they shouldn't be doing.

So that's kind of a balanced approach there.

MR. JILLAVENKATESA: We will take one last question from the floor and then we will wrap up given our time constraints.

MR. BHATT: Thank you. I'm Hardik Bhatt. I'm with the State of Illinois.

So, I've seen especially for Toyota and Samsung IoT is a big play for the entrepreneurs.

Because what we have seen in terms of the platform's infrastructures the traditional

companies like Cisco's and others as well as the service providers like AT&T and Verizon and others are kind of slow to come to the market, come to basically the party because they are still working with their older technology and trying to kind of repurpose them for IoT.

And we have seen some entrepreneurs like Jasper and others kind of coming very quickly to the market.

What have you seen in your industries, or what do you see -- what's the entrepreneurial play in IoT? We see it as a huge play.

MR. GODFREY: In Samsung's case we have a very large venture capital operation in the United States centered in Silicon Valley and New York City.

And one of the leading entrepreneurs in IoT was a company called SmartThings that started here in Washington, D.C.

And two years ago we bought them and brought them into Samsung. So that's now a part

of Samsung.

And then the other thing I would say is there's a role for companies like Samsung and other component and system makers in developing kind of toolkits that entrepreneurs can then use.

So, maybe a secure IoT chip that is low-cost that an entrepreneur can then build a service or a device on top of that has security built in.

MR. WENGER: Eric Wenger from Cisco. Just for the record not to be outdone by Samsung, Jasper is now a Cisco company.

MR. GODFREY: Thank you, Eric.

MS. CAIN: I was just going to say we are finding -- I mean, the connected and automated car space, I think there's not much of a hotter space right now.

And so we're seeing a tremendous number of smaller companies, and entrepreneurs, and startups, and non-traditional players to be very interested in this space.

I think it's exciting. I think it's pushing all of us sort of legacy companies to think differently and approach things maybe more proactively and aggressively than maybe we have in the past.

And so I think it's a raise all boats kind of thing and it's exciting. It's a very exciting time.

MR. JILLAVENKATESA: When you get a chance you should connect with Sterling. I think if anything he manifests the small entrepreneur who's exploring the IoT opportunity.

We could actually have this panel go on for the rest of the day, but recognizing where we are what I'd like to do is to invite our panelists to kind of pull together any closing remarks or closing observations for the last round.

MR. TOBIN: I'll follow on to that last question just a little bit.

Obviously as a government laboratory people don't consider us entrepreneurial. But all

the Department of Energy laboratories are actually managed by universities, non-profits, LLCs and such for the Department of Energy.

And as such, we actually create a significant amount of intellectual property. And we work very closely with industry as part of that technology transfer mechanism to get technologies out there into the public domain and into the economy.

And so as IoT goes there's plenty of opportunities to work with companies to do things that are -- we can work with proprietary information, we can work with creating new devices and technologies, we can license that technology in a useful way that makes sure it gets out into the community.

So, I'll leave it with that I guess.

MR. ROOKE: So, a lot of things I have already said. As one famous person said, I don't remember who they were, but they said it.

So, one thing is that small companies

can actually be very innovative because there's obviously a lot less impediments. They can take a lot more risk, jump out there in the marketplace if they have proper funding from larger companies as was alluded to.

So, I think that's just part of my closing comments is to look at the small innovative companies and see how they match up with the ecosystem.

MR. GODFREY: For my closing comment I actually want to bring up a slightly new topic.

We've talked about spectrum, and standards, and security, and government use, and collaboration today. I think we'll hear about that some more today in the later sessions.

But it would be a mistake since we're here in this beautiful Patent and Trademark Office not to also mention the role of patents and intellectual property.

Congress is now grappling with updating the nation's patent laws to rebalance a little bit

the incentives for innovation versus the threat of patent holdup, or patent holdout when new technologies are perhaps related to an essential patent that someone holds and they decide to aggressively assert that patent in a way that holds everyone back.

And to get really interesting Samsung is particularly interested in the issue of design patents. I just want to flag that for you.

You may not be aware of it, but unlike utility patents, under patent law design patents which have to do with the decorative design on a carpet or wallpaper or something, a 100-year-old law. With design patents the patent holder can claim 100 percent of the profit from a product that is found to infringe.

And in a technology product like an IoT product if there's one design patent but there are thousands of functions in that device it just seems like an absurd result that the design patent holder would get all of the profit.

What if there are two design patent holders? Then do both of them get all the profit? So it's an issue that's hot right now. Thanks.

MS. CAIN: So, I think as we're talking about the government's role in all this one thing that we need to -- that the government needs to keep in mind is this Internet of Things ecosystem is an extremely competitive space.

Everyone wants a piece of this. There are -- everyone wants a piece of it and there's a lot of folks who want bigger and bigger pieces of it.

And I think that as we go forward it's important for government to sort of recognize that and make sure that they're not, you know, we could turn the picking winners and losers dialogue on its head here.

And just need to be concerned about presupposing the outcome. I guess I'll put it that way.

MR. JILLAVENKATESA: Lots of food for

thought. With this I'd like to thank all of our panelists for getting our conversation started. And my thanks to NTIA also.

We strongly encourage folks to continue the conversations over the rest of the day.

So with this I turn it back to Travis. Thank you.

(Applause.)

MR. HALL: Okay, so with this we're going to go on break. We're running a little bit behind but that's okay because we added in some time with lunch. So we're going to come back at 12:30 -- I'm sorry, 11:30. So, coming back at 11:30.

Really quick, we do have a table over here with the agenda, with hard copies of bios of the speakers.

Also there's a sign-in sheet. Sign-in is not required. It's just simply if you're not on the listserv it's just a little emailing list for this work stream. Go ahead and sign in.

There's also name tags. They're

sticky. They're going to fall off at some point in time. But it might be helpful.

So anyway, thank you so much and I'll see you at 11:30.

(Whereupon, the above-entitled matter went off the record at 11:14 a.m. and resumed at 11:30 a.m.)

MR. MORRIS: All right, well let's get started. Folks who are still loitering in the hall will miss the kickoff.

So, welcome back. I'm John Morris with NTIA. I'm happy to start off the next panel focused on IoT policy challenges and opportunities.

So, I'm not really going to do introductions other than just to kind of just the name the folks.

We've got Harley Geiger from Rapid 7. Michelle De Mooy from Center for Democracy and Technology. This is a little bit of a CDT alumni panel here.

We've got Craig Spiezle from the Online Trust Alliance. And Dan Caprio who's right now -- well, he's spent a whole career in technology issues, but now heads the Providence Group.

And then finally and not least John Kuzin who's VP and regulatory counsel at Qualcomm.

So, we're going to just try to jump right in and get started with some questions. I'm going to kind of go down the line and ask a kind of intro question for each one.

And so Harley, let me start with you. Obviously just on the last panel security already was a topic. Rapid 7 has worked a lot on a whole lot of different issues related to smart devices.

And just wanted to kind of get your sense of what the key issues are that you see in the security realm.

MR. GEIGER: Thanks. So, for those of you who don't know Rapid 7 is a cybersecurity company and we aim to help organizations including IoT manufacturers and operators reduce their risk

of cyber attack and of data breach.

And we also conduct extensive independent research into IoT device security.

And from our perspective IoT security is critical to maintaining consumer trust, global industry growth, privacy. And because IoT interacts with physical objects also safety.

But the proliferation of highly diversified IoT devices will dramatically expand the attack surface for malicious actors. So we think that this conversation is very timely.

And from a policy perspective the top four things that Rapid 7 believes the government and the industry should focus on, and to a large extent already are focusing on are the following.

First, field upgradability and security patching for vulnerabilities.

Today, a commonly accepted way of rolling out patches for security vulnerabilities in IoT devices just does not exist once the device leaves the manufacturer.

And there are several reasons for this, some of them better than others. But the fact is without an upgrade capability it is difficult to protect devices from known or discovered vulnerabilities, especially at large scale.

And second, supply chain coordination and transparency.

IoT supply chains can be quite complex in part because IoT is highly diversified and because there is a lot of use of third party subcomponents which can make ownership of security responsibility very difficult.

It can also make replacements and rapid repair of parts pretty challenging. And so we support greater standardization and tracking of IoT subcomponents as well as better coordination between manufacturers and vendors on security.

Number three, we think that industry should adopt processes to receive and handle vulnerabilities from external sources such as independent security researchers.

There's been a lot of great groundwork laid on this by NTIA and through the ISOs already, but what we want to see now is greater industry adoption of that groundwork so that when an IoT vulnerability is disclosed to a company by a well meaning independent security researcher that disclosure is not met with legal threats, or with avoidance, but rather is taken seriously and prompts a patch that ultimately keeps people safe.

And then finally, we urge the industry and the government to leverage independent security researchers who are acting in good faith.

There are just too many IoT devices and too many vulnerabilities for companies to rely solely on their own security teams to catch everything.

From our perspective independent security researchers protect cybersecurity by calling attention to vulnerabilities that manufacturers may have missed or may have ignored.

And ideally this prompts appropriate

fixes that help keep people safe.

But there are several existing laws, most notably Section 1201 of the DMCA as well as the Computer Fraud and Abuse Act that chills valuable research without distinguishing that research from malicious action.

And we also see new laws, the interrelation to IoT that are being proposed that would also chill cybersecurity research.

So we urge industry and Commerce to make use of independent security researchers and support reforms that protect rather than stifle their work so that the IoT ecosystem as a whole can evolve more securely. Thanks.

MR. MORRIS: Great. Thanks, Harley. I'm just going down the line.

Michelle, obviously also we've already heard on the first panel kind of suggestions that privacy and data is a concern. So I'm interested in CDT's take and your take on this.

And also are the privacy issues raised

here new and different? How do you approach these?

MS. DE MOOY: Thanks, everybody, for being here and for inviting me, for having the unofficial CDT alumni reunion.

I wholeheartedly second not surprisingly everything that Harley said.

And so I'm going to shift a little bit because I think he covered a lot of the security issues that are interrelated with privacy to a certain extent and say that what we're trying to do at CDT is think a little bit differently about privacy.

Of course there are sort of similar privacy questions that concern transparency, disclosures. As Harley went through, questions of access to the information.

But the questions of ownership, and the questions of how IoT devices interact with our lives have made us feel that there needs to be a more forward-thinking approach.

And a lot of that centers around the

idea of data ownership.

And so for example, because there are really ethical questions when you start talking about sensors that are not just in your home, but in your body.

And so it goes beyond the idea of privacy in the traditional sense and more to the idea of what is ownership and what is the ethical framework to place around that.

Some of the ideas that we've looked at that we think are sort of different are the ideas of data stewardship, that companies are no longer just sort of data silos or holding data for us, but they are stewarding it for us.

And that comes with it a lot of sort of ethical responsibilities and rights for people.

I think one of the biggest differences in the IoT questions are how do we approach this now.

The internet sort of had a central group of people who were developing it and standards were

very important, interoperability was very important in the beginning.

Privacy and security - kind of a mess, kind of still a mess in some ways.

And so what I think is truly different beyond the conceptual ideas that we have in thinking about how we should approach privacy are how do we approach this ecosystem in a way that's really beneficial to people.

And because there's an ethical framework, how do we that responsibly?

So, what does that mean as far as if we create sort of a data commons?

So, I do a lot of work in health. And there's a lot of data commons in health. Genomic data commons.

These things aren't going to necessarily fit exactly into the IoT framework, but the idea, if you say to yourself that there's an ethical responsibility to give people some access to this information because it's of them, of their

lives, of their bodies, then perhaps one approach to governance is to look at commons, is to look at sort of interoperability from a place where the person is the hub.

The information can go to lots of different players and can be used in lots of different ways, but that the individual is ultimately the hub for the information.

And so those are quite different from a lot of the privacy approaches that we've taken in the past. But I can go into them in a little more detail in a bit.

MR. MORRIS: That's great, thanks. Thanks, Michelle.

Craig. Obviously your organization OTA has been grappling with a lot of these issues for a long time. And I think you've been developing a code of conduct.

So let me ask you, we've heard about some concerns, but let me ask you to address both sides.

What are some of the good developments you've seen in industry to address some of these issues, and what are the major concerns you see?

MR. SPIEZLE: Thank you. And I want to thank NTIA for hosting us today and really having this meaningful dialogue.

There are a lot of good progress. I mean, I think a lot of us focus on the missteps all too often, whether the security flaws, vulnerabilities, or the data usage and privacy issues.

But I think one of the things is the previous panel mentioned, one speaker said about security is complex and it's hard to get everything right.

But I think that's -- we have to recognize that, that getting the basics is really important.

And some of the challenges we're seeing in IoT are not new. They're the same problems we had in mobile, some of the same problems that we've

had in websites today. So I think that's -- getting the fundamentals right is one of the main issues.

And the framework, and I want to actually thank the teams at CDT, actually Rapid 7 and Dan as well who contribute a lot to the thinking of our framework to address some of these key things.

But I think one of the things that makes it really hard, it's not just the device.

Hillary talked about it means a lot of different things, but it's multidimensional. It's a physical device, it's quite often a mobile or web app, and it's also a cloud service.

So, not only do you need to look at the security and privacy of all three, you need to look at the flow of the data between all three. Who has access, is it encrypted, how is it stored. So I think that's one of the challenges that we had.

And again, to Harley's comment one of the things that we're very focused on is

sustainability. It's one of our key pillars. And so life cycle issues.

Hilary also talked about the cars where they're going to be upgraded in the future.

So we're concerned about all these devices that are out there, and are they going to be orphaned. Are they going to be left on their own. And what's going to be the challenges of that.

And so one of the risks and one of the concerns that we have is they become an attack vector. They become weaponized. They become really an area where they're diverting first responders.

So, those are things that we really need to think about.

And the biggest concern I have is companies aren't thinking about it. They aren't investing in those areas. And it's beyond the warranty.

And I think we have to put it also in

scope of what's reasonable for a $5 sensor versus a $5,000 device. So, the upgradability and such is different there.

I think the last thing I want to mention, and again was also mentioned about vulnerabilities.

I do think it's a collective area. And one of our key principles is companies need to have a conduit for responsive disclosures from the research community.

So companies need to have that sort of welcome mat to -- whether it's from academia researchers or users, and how to respond to those areas.

And I think the last thing is that we also think about, and Michelle, you mentioned about data and privacy. And that's really key.

But it's a whole new dimension when you think about the smart home. You have these devices that are connected to the wall.

What happens when someone moves? Who

owns that data? So, you have data portability issues, or do you have data right to be forgotten, or both of those?

So, I think when we look at that we need to address that. And so it's a whole new world, but it's a whole new world of opportunities at the same time. Thank you.

MR. MORRIS: Great, thanks. So, Dan, certainly your work at the Department of Commerce and your work since then, a lot of it has been focused on innovation issues.

And so what's your take on the relationship between some of these policy issues and innovation in the IoT space?

MR. CAPRIO: Well, thanks, John, and thanks to Larry and Alan and the team at NTIA and Commerce for putting on this workshop. It's very relevant and very timely, and I appreciate being included.

So, a couple of things sort of related to innovation. Sort of three comments.

The way that I think about this, and having thought about the internet things for over a decade now, we really need to figure out or think about how to protect privacy and security and enable innovation. And those things aren't mutually exclusive.

So, first thought is the Internet of Things, and we've heard speakers discuss some of this this morning on the initial panel.

But the Internet of Things broadens our horizon for innovation and economic growth. I mean, some things that we could never even imagine. So if you think this is going to be big, it's probably going to be bigger than we can even imagine.

But there's a challenge with that. And the Internet of Things multiplies risk so we must think strategically and proactively about cybersecurity and securing the Internet of Things.

The way that I think about privacy is that you can't have privacy without security. And

when it comes to securing the Internet of Things this is not a check the box compliance exercise.

We need to approach cybersecurity using the NIST cybersecurity framework as a strategic risk for CEOs and boards.

IoT cybersecurity and risk is actually different from all other risk because it touches all types of risk. So that's operational risk, reputational risk, legal risk, regulatory risk, et cetera.

And it's because the IoT risk is such a complex and multifaceted risk that it needs to be addressed through an enterprise risk management approach.

And moreover, IoT cyber risk is extremely dynamic and as a result requires boards and senior executives to frame the risk appropriately and understand steps that might be taken to mitigate and respond to those risks.

Second, how to protect privacy and security and enable innovation to build on some

comments from earlier today.

We do need a national strategy for the Internet of Things. And I think there's a model that exists that's almost 20 years old, but it was the 1997 Clinton administration Framework for Global Electronic Commerce and it had five key elements which I think are still applicable today.

One, the private sector should lead. The internet should develop as a market-driven arena, not a regulated industry.

Number two, government should avoid undue restrictions on electronic commerce.

Number three, where government involvement is needed its aim should be to support and enforce a predictable, minimalist, consistent and simply legal environment for commerce.

The fourth element of the '97 framework, governments should recognize the unique qualities of the internet.

And five, electronic commerce and internet should be facilitated on a global basis.

So, I mean that really does touch all the elements.

The third point I wanted to make is the importance of international engagement. I've been involved and done a lot of work over the years with the European Commission, with their expert group on the Internet of Things and the importance of trans-Atlantic.

But also have been involved in some more global work through the Internet Governance Forum.

And IGF has created a framework, a voluntary framework to build global trust in the Internet of Things.

We have an IGF dynamic coalition on the Internet of Things that brings together stakeholders from all over the world to engage in a dialogue on best practices in IoT with the intent to find a realistic and ethical way forward, to pick up on some of the good work that Michelle is doing at CDT.

The core of this framework which is --

we've been working on this for six or seven years but it's on the agenda for the IGF meeting in Mexico City in December is that Internet of Things best practices aims at developing IoT products, ecosystems and services, taking ethical considerations into account from the outset both in the development, deployment and use phases of the life cycle.

Thus defined an ethical, sustainable way ahead using the IoT to create a free, secure and enabling rights-based environment that really does three things - embraces IoT to address societal challenges, creates an IoT environment that encourages investment, and then third is the emergency of a trusted IoT environment which includes on the privacy side meaningful transparency, clear accountability and real choice.

So, with that I will yield back the balance of my time.

MR. MORRIS: Great. Thanks, Dan.

John, obviously we've already heard a lot about privacy and security issues. And I know Qualcomm's done a fair bit of activity on those issues.

Are there other issues that you want to kind of put onto the table?

MR. KUZIN: Sure, sure. Well, first of all, I want to thank NTIA for putting on this forum, for inviting Qualcomm to speak here. It's a very important subject.

And as you might know, as the largest wireless chip set provider in the world Qualcomm is in the middle of the IoT.

And another thing as you all know is a key reason why the IoT is getting so much buzz now is because of the expansive growth of wireless technology over the past decade, and the continued expected exponential growth over this entire upcoming century.

And 5G is being billed as the IoT interface, but we need to recognize that IoT is here

today, and it's using 4G interfaces, 3G, Bluetooth, Wi-Fi, et cetera.

Just earlier today Verizon and AT&T separately announced initiatives where they're going to be deploying technologies using LTE Cat-M which is an interface that supports M2M applications.

So, one of the messages is that the IoT is here today. It's been here for awhile. It's very successful.

But the specific topic, issue, policy that I want to focus on in these opening remarks is the importance and the success of technology neutrality.

What technology neutrality has done with regard to wireless policies is that it has enabled wireless companies to introduce new technologies and air interfaces without having to ask the government for permission.

So in this regard the path that the FCC took and NTIA took -- I want to give a shout out

to Paige Atkins, Peter Tenhula, Derek Khlopin and all the others in the spectrum group, Ed Drocella, have done to help open up these bands that have been mentioned.

The high-millimeter wave bands, both unlicensed and licensed.

The rules that the FCC put in place in these bands are technology neutral. They set power levels. They set bandwidth restrictions, out of band emissions, and they said go ahead and deploy.

And today 4G technologies could be deployed in these bands because of those rules. And that's a very good thing.

Obviously the new 5G interfaces are being tested, et cetera. There are experimental licenses that the FCC has granted to further testing. But the fact that a particular technology is not mandated is very important.

So, opening more spectrum obviously as we've heard is very important to supporting IoT

growth, but that's not the only part.

Several years ago Qualcomm announced an initiative which we called the 1000x Challenge which is to support a 1,000 times increase in wireless data demands over the next 10 years.

Technology-neutral rules are critically important to meeting this challenge.

So, Qualcomm and others in the wireless industry are busily developing 5G interfaces, and at the same time we're continue to expand 4G.

One example I'll give you is as we were designing what would be nice to have in a 5G world, many of the technologies that were discussed our engineer said you know what? We can do that with 4G, and we are doing that with 4G.

I'll just mention a few. Carrier aggregation is a technology where you combine multiple bands and provide a bigger pipe to the user.

Another one is the device to device connectivity. If your device is within earshot of

mine there's no need to bounce signals off an access point, or a small cell, or a base station. They can communicate directly.

A third technology which is useful for public alerts and also in a stadium setting when you want to send the same information to a lot of users is LTE broadcast technology.

So, technology-neutral rules not only made the ready deployment of each of these technologies possible, technology neutrality actually encourages them.

I just want to also say a few words about -- I've been talking about LTE licensed spectrum. Unlicensed spectrum is also critically important.

So, FCC rules in the unlicensed run very similarly. Set power levels, out of band emissions, bandwidth requirements.

And these general technical parameters have allowed Bluetooth, ZigBee, the various stages of Wi-Fi from 802.11A and B to G to N to AD, AC, and pretty soon AX.

All of these advances mean better performance, better throughput to the users. The FCC's unlicensed rules have enabled that.

They've also enabled the deployment as you may have been reading in the news for a technology called LTE unlicensed spectrum.

All of these are going to provide a better mobile experience.

So, the last point I would raise is that 5G obviously is going to use all spectrum bands, licensed, unlicensed and shared, high band, low band and mid band.

So, as the earlier folks have mentioned, I think both John Godfrey and the Intel talk from earlier today, it's critically important to continue to implement performance-based rules that define a goal and let the industry innovate that are not prescriptive. They don't say you must deploy technology X. That is going to make that happen.

Thanks a lot. I look forward to the

discussion.

MR. MORRIS: Great. Thanks very much. So let me toss out a few questions and anyone please jump in and weigh in.

One of the questions that we had our RFC on, our request for comment on this workshop is just to kind of figure out what is new, what is not new, do we need new policy solutions.

And I think just on this panel we've already heard I think, you know, Michelle is kind of starting to look at privacy from a different lens.

And Dan is simultaneously engaged in the IGF kind of a new policy forum, but referring back to a 1997 Clinton policy.

So, let me just kind of go back and ask you guys in the areas that you're working on how much do we really have to do to kind of create a new policy model because of IoT?

So, I don't know, Craig, do you want to jump in first?

MR. SPIEZLE: I think one of the biggest areas is data. Data is king, and we've heard that for years. It's driving our economy and a lot of new, innovative services.

But what's concerning is that the data that's being collected redefines what PII is in a sense. It's ultra-sensitive, it's dynamic, it's about what you're doing, your lifestyle issues, or even your work style issues.

And so what concerns me is the number of VCs that even reach out to me and talk about the company's business model is data. It's not the device.

So what are we thinking about on the data collection?

And one of the concerns is, well, we're caught in the old paradigm of well, it's a disclosure statement and we're covered. It's a terms of use. And as long as they click on that when they download it we're fine.

Michelle used the term "stewardship"

and I talk about that a great deal. So that's a big area of concern in what's different.

And it's uniquely different if you think about buying that 16-inch TV at Costco or Best Buy. You bring it home. You install it on the wall and you try to get to use it.

And IoT use the key features that you thought you were buying you have to give your data. And that's not the time of adequate disclosure.

So we have to rethink what that is, and that's I think the big area there.

And the other area that I mentioned what's new is the weaponization issue here. These are now connected to all these devices.

And this may sound alarmist, but we look at the hacks that are happening today in the areas here.

And so it doesn't take a whole lot of creativity if you want to paralyze a city or a country by exploiting an installed base of 100,000 garage door openers, or 100,000 devices.

So those are things that I think that's new and that does require a fresh set of views on the issues.

MS. DE MOOY: I would just add to my sort of mushy discussion of ethics, I think of it as mushy although more and more when I put it in the context of IoT it's not. But the idea of equality of access.

So typically we talk about broadband, we talk about digital divide and of course those issues still remain.

I think in the Internet of Things there's a term that's out there that's called data feudalism which is such a creative use of that, but also really speaks directly to some of the concerns.

If we have these devices, these sensors that are ubiquitous in our lives and they're creating more and more data, it gives a lot more power to companies that their fuel is data. And it takes a lot less power away from the people who

are providing it.

This is sort of what I was trying to get at a little bit in my concept of the person being at the center of this universe.

So, I think that's an important part. I know it's a tricky part for the government to get involved in, but the idea that digital inclusion is much more than just broadband, that it's about understanding that more data means more automated decision-making that may impact -- may harm different underserved communities, or different communities.

I think that's a really crucial policy question that has really not been addressed. And partly it's because it's really complicated and complex.

But I think there needs to be a structure created by the government to look into those questions and to come up with some policy solutions.

MR. MORRIS: Okay. Dan?

MR. CAPRIO: Thanks, John. I think of this as an evolution, not a revolution.

The Internet of Things, it's an important transformational trend, but it's not fundamentally new and different writ large.

I mean, some of the issues, some of the privacy issues especially around notice, choice, access and disclosure, those are still important principles, but we're evolving from those in terms of -- I mean, the ethical discussion, transparency, accountability.

I think we've got to be careful and strike the right balance between regulation and innovation as we strive to protect privacy and security and enable innovation.

It's also important to note that, and you heard Dean Garfield talk about this earlier in Intel, but we face a large number -- there's an increasing number of societal benefits that the Internet of Things provides, but also some challenges.

But I think it's important to stipulate that the Internet of Things is still in its infancy, and is still evolving rapidly.

So we're really -- even though we're going back to the future with the '97 framework from the Clinton administration things were evolving very rapidly, but those broad, durable principles I think still serve us well.

MS. DE MOOY: The idea that the way the internet evolved, it was very sort of separate from us. And I experience this a lot when I work with my Millennial colleagues who don't understand the internet a lot of times as separate from them because the way that they grew up is it's just this integral part of them.

For me it's this separate beast. I think the Internet of Things is going to be a similar kind of beast.

And the idea that you go onto it to accomplish certain commercial ends or whatever kinds of ends is going to be completely different.

This is something that's integrated into how you make decisions about your life, about your body, about your health, how the government deploys resources and makes decisions about those really crucial things.

So I think that paradigm and that sort of approach as the Internet of Things as separate is no longer valid.

And I think that's part of why concepts of data stewardship, and social good, and individual dignity have to be at the heart of the policy framework. Just a comment to piggyback.

MR. KUZIN: Yes, I just wanted to highlight, repeat what Dan said, that it is critically important to recognize at this stage that it's still very, very early in the deployment of IoT which is the reason why any regulation should be really thought of carefully before implementing a heavy-handed regulation.

Now is the time to let a billion flowers bloom.

And picking on another one of Dan's points about the Clinton framework. Two other frameworks that we believe work well and are good models.

And it's important to look to the existing models, the existing policy frameworks at a minimum as a good starting point to the extent they need to evolve.

And two that I'll throw out are the FCC's existing privacy framework that includes the core principles of transparency, consumer choice, privacy by design and security.

And the other one is the NIST cybersecurity framework that was developed via a collaborative process that included academia, industry members as well as government stakeholders.

So, both of those, if you're looking for models those are very good starting points. We think they work well.

And again, it's time to just tread very

carefully. And that's all, thanks.

MR. MORRIS: Last word.

MR. GEIGER: So on the question of whether or not there's a lot that's new with regard to IoT and whether we need a new policy framework, we tend to agree with Dan that this is more of an evolution rather than a revolution.

IoT typically runs general purpose computers. They're running software. And although they're embedded in physical devices we're familiar with a lot of security issues related to general purpose computers and with software.

Really what's happening is that it's exacerbating a lot of existing issues that many of us in the room are familiar with.

I think really it's an issue of scale. There's going to be a lot more devices, a lot greater diversity of those devices.

We'll have new entrants, many of whom are not necessarily experienced with security.

And so kind of have to be brought into a conversation that folks who are experienced with security have been having for quite some time.

One issue that I think is going to be exacerbated in particular, and Michelle has touched on this a bit already, and that is device ownership.

You know, you buy a toaster and part of your toaster breaks down, you can repair your toaster. You can turn your toaster into a train set, or I don't know what you can do with toasters.

But you buy a connected toaster and suddenly you don't own all of that toaster. The software in there, you only license it.

And if there is a broken part of the software then you as an independent person are not necessarily able to repair that toaster, or to even hire somebody who's an expert in the field to repair that toaster without the manufacturer's consent which can sometimes be more trouble than it's worth, leading to less patched vulnerabilities,

leading to potentially larger cybersecurity issues as IoT connects to broader networks, which connect to broader networks, and so forth.

So, an evolution, not a revolution, but it brings to prominence issues that we've already been dealing with and need to pay attention to now.

MS. DE MOOY: And what happens if the company that made the toaster goes out of business, or decides not to do it anymore? And so your toaster doesn't work. Even though it's not broken, it's just not being serviced anymore. And who's responsible for that.

MR. GEIGER: Agreed, a great point. And especially for cheaper IoT devices. Light bulbs, for example, where the economics just aren't there for continued security updates well past the life cycle of the device.

But light bulbs can last for quite a long time and consumers try to make as much use out of their items as they can.

So, what if the company were to turn

over security to third parties or to independent researchers? Would current laws really allow that sort of service, or would it chill them?

And I think that that's a conversation that we need to have.

My personal opinion is that no, currently laws need to be reformed in order to allow that sort of service to be empowered.

MR. MORRIS: Okay, quickly, Craig.

MR. SPIEZLE: A quick comment. We're talking about regulations or guidance and such there.

One thing I do want to say is that developers need advice now. They're trying to go out there.

So it is the Wild West. A lot of innovation. That's one of the reasons that the IoT Trust Working Group got created over a year and a half ago.

And so you asked earlier what's the positive news. And we're actually seeing a lot of

adoption. We're seeing international testing organizations, National Association of Realtors.

So, our framework is a baseline criteria. And I think it's also a good example where the public sector and the private sector can work together and provide that prescriptive advice that's very dynamic.

So, I think there's progress today. But again, to separate those type of frameworks and best practices and code of conduct from a government activity I think are very important to consider.

MR. MORRIS: Thanks, that's helpful. Let me actually kind of pose another what I view as kind of a big picture question.

We've heard already this morning IoT applications ranging from things that are very, very consumer focused to things that are industrial focused.

And so from a policy perspective, whether it's privacy, or security, or any other

issues, do you think that we -- should we be trying for the same policy covering all of the sectors, all of the applications?

Or do you think it's going to be a better, more productive approach to kind of look in sectors? Anyone want to jump in? John?

MR. KUZIN: I think you more or less answered the question.

Where there are technologies and applications that touch a consumer I think it's very different when you then look at industrial applications where it's inside of a factory, or inside of a contained environment and there is no consumer data being involved.

One definitely impacts privacy and the other probably doesn't in many cases.

They both need to be secure, but I do think that there is a difference between industrial applications versus consumer applications.

MR. MORRIS: Anyone else?

MR. CAPRIO: I think of this at two

levels. One, at the horizontal level and part of the reason why we're having this workshop.

But again, kind of the need for a national strategy, at least aspirationally to kind of coordinate government policy to avoid regulatory collision.

But to John's point there are very specific verticals. We heard some on the prior panel. Smart homes, smart cars, smart meters. Those are going to develop separately.

And a lot of the economic efficiency that we're talking about will be in what we're calling the industrial Internet of Things.

And so in the work that NIST is doing on cyber physical systems is important.

But yet in the industrial Internet of Things there are many of those areas that really don't implicate privacy the way the consumer-facing side, what Michelle's talking about.

So, I think you've got to think of it

horizontally and vertically. But the challenge for the public-private partnership working with industry and government is how do we strike the right balance as we go forward.

MS. DE MOOY: I think I would say for privacy and security from a sort of broad policy perspective it would make sense -- I still believe that there is a use for a broad data protection law in the United States.

We have exactly two, HIPAA and the FCRA, and those are flawed to say the least. But they do some things very well also.

So, I think there would be a place for that.

I think the United States is really lax in not having this. Whether that's a political reality is a different question.

I also think when you take privacy and security that reforming the Digital Millennium Copyright Act would be a huge, huge positive impact here in the United States, abroad, or just not

enforcing it, I don't know.

But something that would kind of tie privacy and security together sort of in a constant way would be a really important government act.

I think also from a kind of smaller potatoes aspect when you talk about things like digital divide or data feudalism, the government should plow money into things like job skills, like training skills.

Have people be able to make these products. Not just the hardware, but the software. Give them the tools that they need to participate in this ecosystem.

Also, plow money into security. Give the companies a platform and a mechanism for coming together to create standards, to create security standards, things that I think the government is actually really good at doing.

MR. SPIEZLE: So John, you know, Hilary mentioned about not one industry. So we think of automotive, industry controls, medical devices,

consumer devices. So we have that.

What's concerning is I talk to companies in industrial controls and they don't think there's a privacy issue. Because they're thinking of it's just HVAC, and it's a company, and they don't think consumer laws apply to them.

So, the challenge is as you look at -- it's a blur. You have consumer devices being brought into the workforce, whether they're BYO type devices or they're a smart TV that's now in the conference room of the board. So you have that occurring.

And you have conversely people working at home. So I think we do need to look at a baseline framework of data collection principles, privacy principles, whether it's in industrial control or a consumer item.

And I think again the other part is that it's not really clear what data attributes all these devices are collecting.

And so I think that's -- whether again

it's a commercial device or a consumer device that disclosure needs to go a lot deeper and help understand.

And then the normal principles, how is it used, who is it shared with, how long is it retained and all those are pretty much absent in any of the industrial controls. And I think any business should be asking their business for that today.

MR. MORRIS: Okay. Harley. Last word?

MR. GEIGER: So, from a regulatory perspective it's probably the most practical to work within our existing regulatory frameworks which are for better or worse already divided. They're already sectoral.

And for connected medical devices, for vehicles and so forth. And I think that's unavoidable.

However, the policies and the approaches that each of those different sectors can

take can be coordinated.

And we think that it really makes the most sense to coordinate based on a spectrum of risk. It's a risk assessment that includes the likelihood of damage and the severity of damage.

And on that risk assessment should include things like physical damage to individuals, or to infrastructure, breach of privacy, and so forth.

And there will be some that don't pose much risk, and there will be some that pose an unacceptable level of risk.

And in making that risk assessment I 100 percent agree with what Craig had said which is that it's hard to look at the device in isolation because these devices are connecting to networks, which connect to networks, which connect to networks.

As we all know an HVAC system can connect to the point of sale devices in retail chains and cause massive breaches.

So, we can't look at just one in

isolation. We should be looking what that system is connected to as well.

MR. MORRIS: Great, thanks. In a moment -- I mean, I have probably another couple of hours worth of questions, but let me ask you if you guys have questions in the audience can you start lining up at the microphones?

I'm going to toss out what may be a shorter question just to see if folks have comments.

But to really kind of follow up on something that John Godfrey on a prior panel raised.

We are here in the Patent and Trademark Office. And I don't know if any of you have kind of thoughts and observations on the point that he raised about patent trolls and intellectual property issues.

Is there anyone who wants to jump in on that? Craig?

MR. SPIEZLE: I do think there is a lot

of concern. On one hand there's a lot of standard development. And we talk about the importance of protocols.

And one of my concerns is there's a lot of platforms providers -- I'm not going to say who -- but that they're focusing on their technology.

And my concern is they want to be the center of the universe. So I'm a little concerned about that becoming some of the proprietary standards. And so I think that's really important.

So it's that we have open protocols for compatibility, communication, the standard APIs out there.

I do come across a lot of companies that believe they have proprietary technologies. So I think we're going to see the normal patent troll as much as we don't want to see that. I think there's going to be an assertion.

I also think some of the large companies are amassing very large patent portfolios from a

defensive strategy.

So, I think we're going to see that. As Harley mentioned, as more and more of the devices are working with others or perhaps even bundled we're going to see more of that challenge.

So, I think just recognizing that is going to become the norm unfortunately. So, hopefully I'm wrong on that by the way.

MR. MORRIS: Anyone else want to jump in? Okay. Got a good crowd. Let me start at the back microphone. If you could identify yourself and if you're targeting your question to a specific person say so, or the panel.

MR. FORGETY: I am Trey Forgety with the 911 Association.

In the public safety sector we're just starting to think about all of the ways that the Internet of Things can speed up or improve our ability to respond to emergencies.

But obviously we have very special sensitivities around privacy, security, data

protection, and so forth.

As we start to think about these sorts of things and put them front of mind for our members are there specific policy areas that we should be focusing on?

This is all going to be new territory for a lot of the police, fire, EMS, 911 folks that we deal with.

So, what should we be putting front of mind first? I'll throw that out to the panel.

MR. MORRIS: Great question. Michelle?

MS. DE MOOY: I don't know where to start. I know Debbie Matties is here and she could probably talk more intelligently about this in terms of the database that CTIA is building for e911.

There are working groups, there is a working group that is looking specifically at these questions. So the first thing I would tell you is to join this working group.

Because there are a lot of representatives similar to you that are asking the same kind of questions.

And really, it's tricky because it's contextual. But whenever I'm sort of in that situation I start with the individual's expectations.

It's kind of a longstanding way to approach these types of questions, but it works fairly well.

If you are incapacitated you're probably okay with your location being shared. If you need help that's probably okay. The technical questions aside, just policy questions.

If you are in an abusive type situation, a violent situation, you're probably okay with your location being shared.

So there's sort of maybe a not satisfying range of what people are comfortable with and what they're not comfortable with.

And I know, I think a lot of times when

I speak with EMS or other people who are in the public safety field they want much more black and white answers.

And unfortunately I don't think that's the case. It's sort of like every question in health and wellbeing. There's a range of what's okay and what's not.

The default I think is personal safety. I think most people would agree with that, their family's safety. The default in this case is not privacy, which you don't hear me say very often. But in this case I think that's true.

MR. SPIEZLE: Two quick questions on there that's come up, one from my own city.

As more and more devices get tied to the fact that you call 911 it's creating some challenges for cities how to manage that. So, it's a false positive. And so effectively a lot of them, it's a low end of a response.

The other issue that I'm concerned about on my past work with the CSRIC and as a utility

commissioner in my own city is 911 outages, but specifically the voiceover, the internet provider which up till recently the unnamed cable providers don't provide that data of internet outage.

And so if you're dependent on 911. And so that's a challenge. And while I don't support more regulation, I really highly encourage ISPs and cable providers to freely provide that data to their cities, their franchise agreements and such because that's really needed to understand how 911 is going to work if it's not working with your phone system today.

MS. DE MOOY: I just want to amend my answer to say quickly identifiability is a really good question to ask. Is it necessary to actually identify somebody if really what you need is their location.

So, the questions of how -- the kind of information that you actually need to perform the job, but also what happens to the information afterwards.

You know, so if you have records that are tying somebody to a specific public safety call, a specific diagnosis even or type of care, that's problematic probably from a privacy perspective and isn't something that somebody would necessarily expect to be collected, retained and then perhaps shared with law enforcement.

So, a huge part of that is asking all of those questions and coming up with policies. So, how long do we actually hold onto this? Do we need to tie a person's identity with this information about this call?

What is our policy with law enforcement? A lot of organizations involved in public safety have some mandates, but they're not all mandates.

Some of them are choices about how much information you want to share. How you store the data can matter a great deal in terms of what law enforcement can get.

So, these are the types of other policy

questions.

MR. MORRIS: Great. So, we've got a lot of people at the line. I'm going to try to turn the questions into a little bit of a lightning round if we can keep answers pretty quickly. We'll go to the first microphone.

MS. ROSS: Thanks so much. My name's Michaela Ross. I'm with Bloomberg BNA.

I have a question about, as we were talking about the evolving nature of policies for IoT, and Michelle had mentioned that Millennials in her office look at the internet differently.

We're seeing kind of some changing definitions of what does privacy -- what is a reasonable expectation of privacy, intergenerational differences.

And I'd just like to get a comment on if you see that policies made now might be too defined in several years as these things shift.

MS. DE MOOY: Well, let me clarify. What I meant by Millennials in my office which is

really, you know, they would probably kill me for even calling half of them that.

But what I meant was that the way that I look at the internet and digital services and products is really as very separate from me. In fact, almost philosophically as this separate beast and what is this.

Whereas, when I talk to a lot of people who have grown up with these services and devices it's really not separate. It's a part of how every decision is made, the considerations of how someone lives their life.

And so that kind of ubiquity with the person seems to make a great deal of difference.

And so when I talk about privacy shifting to things like data stewardship to individual dignity that's part of where that comes from.

So, if you are maintaining a customer's dignity, if you are a data steward and you are thinking about not only the customer's dignity but

the social good aspect, how you deploy that means things like recognizing their expectations.

So, a lot of that isn't different, but it's in a different context and it's in a different deployment when you're talking about, like I said, somebody's body or somebody's home.

A lot of the surveys that you actually see show that people care just as much about privacy as ever. In fact, younger people care even more because they understand more perhaps the consequences of surveillance.

They've sort of grown up also with the ubiquity of government surveillance, of sort of commercial tracking and surveillance, things that make people wildly uncomfortable in surveys, but nobody really has great solutions for.

So, I think when I say that what I mean is that they have the chance to look at policy differently. And so a lot of what I'm doing is kind of picking their brains.

I think the Internet of Things policy

framework has to be original and innovative, as original and innovative as the system itself.

MR. SPIEZLE: One point of research to recognize is perceptions and views on these issues change as people go through life stages.

So, a Millennial's view today who's 23, just one or two years out of college is going to be clearly different when they have a home and when they have a kid.

And we've seen that in other research attitudes. So, don't assume that those views are static I guess is just one thing because they do change. And we've seen that before.

MS. DE MOOY: And I think there's more of an understanding of privacy as a right, as something that should be designed and built into products and services as opposed to sort of an afterthought.

MR. MORRIS: Let me cut it off, go back to the back mike and Eric, there's a line back there. We'll try to get to you.

MR. MINARDOS: George Minardos from .build internet registry.

Great panel. I could skip lunch but I'm really hungry. My watch told me to stand up, so my question is --

(Laughter.)

MR. MINARDOS: A few minutes ago my RingCentral camera pinged me and said that my kids were driving out of the driveway as my wife's taking the kids to school in L.A.

And I remember I signed a paper yesterday. I was intrigued by the release for our 13-year-old to use his iPad which is a requirement at school.

And I had to sign that he would not use encryption technology on the iPad.

And I thought that was kind of interesting. And it went further to say that because the export of such technology is not allowed by government and the school gets federal funding.

So, my question around encryption and policy is what do we need to do for the internet in general, but then also with IoT and encryption.

MR. MORRIS: All right. Very quick answers?

MR. GEIGER: So, with regard to export and encryption, that's very interesting actually that a domestic school is not able to use encryption on a laptop because of exports.

And I'd like to see that fleshed out more, but that sounds like something that could --

MR. MINARDOS: Give me your email and I'll send you the doc.

MR. GEIGER: Well, I'd be interested to see that.

But with regard to encryption more broadly and IoT a lot of what our IoT security research shows is there's a variety of common vulnerabilities, but at the root of several of them is lack of encryption, or the use of encryption that is just too weak.

And so from our perspective we'd like to see greater adoption of stronger encryption, but perhaps most importantly, and this is something that is obviously broader than just IoT, but it absolutely relates to IoT and that is to protect strong encryption from calls both in the United States and abroad to put back doors into encryption, or to have legal regimes that require companies to write software to undermine their own security features.

From our perspective that would result in an even more complex and exploitable environment that would undermine cybersecurity for everybody.

And in the case of Internet of Things when we're talking about the deployment of billions and billions of devices, many of which can even impact safety, it becomes an even more important issue that these devices and the information on them remain secured.

MR. MORRIS: Okay. Rick.

MR. LANE: Rick Lane with 21st Century

Fox.

Since we have limited time I won't get into a DMCA fight with the panel on the impact allowing for legal hacking tools in the marketplace would have on privacy, security and content protection.

But my question is really about the fair information privacy principles.

There was a huge debate during the ICANN meetings about privacy proxies, and the ability of commercial entities to hide who they are through privacy proxies so that consumers would not know who they're dealing with, who is collecting their information.

Yet the fair information privacy principles always allow for and state that you should know who you're dealing with on the other side.

I'd be curious from the panelists what their thoughts are on that. Should commercial entities be able to hide who they are if they're

collecting data?

MR. MORRIS: Other quick answers?

MS. DE MOOY: It's a tricky question, and a really good question.

I'd like to say no with that kind of -- I actually think that the answer is that it would be okay under certain circumstances.

And part of the reason I feel like that is because the disclosures and the notice to consumers are absolutely useless.

Knowing what entity necessarily specifically is taking and sharing your data isn't necessarily what we want to know.

Do I care that it's some company that's incorporated here and maybe in five other places? Not necessarily. Maybe if I'm in a lawsuit I do. And for that reason it would matter.

But from just a consumer understanding standpoint I think what people really want to know is are you meeting my expectations. Are you using my data without telling me in a way that I would

not be okay with.

And if that is the case there is a straightforward exchange of that information.

The company that's behind doing that to me is less important than that.

MR. SPIEZLE: So let me clarify real quick. I say no, but a consumer should have the notice before product acquisition. If that is the policy of the company then let the consumer make the decision.

But how is that disclosed? If it's buried in that convoluted policy on page 54 I would say then it's not adequately disclosed.

MS. DE MOOY: And I would just say one thing. I think that would impact free speech and so that's part of where if I had another hour --

MR. MORRIS: We could have a whole other panel on it.

(Simultaneous speaking.)

MR. CAPRIO: It's interesting that this issue has come up in ICANN. I mean, this has

been a longstanding issue for some time, for as long as I can remember.

It implicates the issue of anonymity and how you go forward on the internet.

But I think to the question about the fair information practice principles - notice, choice, access and security, those are still important, but those were designed in the seventies with centralized databases, one-to-one data.

We don't live in that world anymore. And so the real question rather than talking about how many angels can dance on the head of notice, choice, access and security is how do we get to transparency, how do we get to accountability, and how do we create ethical frameworks.

MR. MORRIS: All right. Very quickly.

MS. GRADY: Just a question about jurisdiction. We talked about the fact that different agencies have different parts of the privacy, the cybersecurity, the HIPAA, whether you have rights to your toaster or whether you licensed

your toaster.

Where do you think the holes are as far as these agencies not having jurisdiction? And do you think there's really the political push yet to fill those gaps?

MR. SPIEZLE: Well, I think that question, actually, I'll go a little further than that. It's also is it U.S. law or is it international law.

And I think companies in IoT have to recognize where is that user residing when they -- not necessarily today, but tomorrow. So, to have provisions.

So, our advice and recommendations that we've outlined in the framework is that you basically aim towards international law in these areas. A higher standard in a sense of that.

So, whether you like it or not, but users will buy these devices and move to the EU and then you're going to be governed by there.

So, that was an indirect answer to your

question, but I think that's a bigger concern that organizations should be thinking about.

Can I just close out by saying I don't want to create the impression, or leave the impression from this panel that there's some significant gap in U.S. law with regard to protection of data.

I think there are challenges that we face with regard to how we make the U.S. system interoperable with other countries.

I think there are challenges with how we evolve FIPS so that we can deal with new evolutions of technology, with technologies that don't necessarily have interfaces that are readily available to convey information, or to take permissions from consumers.

I think it's an important point that Michelle raised about the idea that we want to focus on what's expected and unexpected outcomes from the use of technologies as we try to figure out what FIPS means as the technology grows and evolves.

But if we circumscribe the uses of data too quickly then we won't reach the points of innovation that John referenced in the prior panel with regard to all the things that can be done.

And just as a point of caution Dan and I have been on panels together on a lot of these things for decades now I would say.

And I was on a panel on some issues relating to the use of technology and tracking at the FTC in the late nineties and had some of the views been adopted then that were expressed about what would be acceptable for consumers and what they would put up with we wouldn't have things like Facebook and Google.

So, we should be careful about figuring out what the rules are now before we really understand what the technology does, or what people might expect of it.

MR. MORRIS: Okay, I'm going to take that as a good comment, not a question. I'm going to straight to just a very, very last question.

You each get 30 seconds, no more.

The next panel right after lunch is really kind of asking the role of government question. Can I just ask if there's a specific thing that you want to kind of give advice to that panel or that discussion just as a wrap-up?

So, why don't we start with you, Harley, if that's okay.

MR. GEIGER: So, number one, I agree largely with a lot of what Eric said and think that right now a lot of this needs to be industry led.

And we're not calling for prescriptive regulations on IoT security at this time.

I think NTIA has already got a fair number of multi-stakeholder processes and other processes.

NIST has a lot of really great standards on a variety of topics that we've discussed here today. So, these things are already happening.

I actually think that the biggest issue is industry adoption of these policies and

standards that are coming out of these processes.

MR. MORRIS: Great. Michelle?

MS. DE MOOY: I would say you can't have privacy without secure devices. I think the government needs to put money into security.

I think it needs to convene companies in a sort of cross-company way so that there's a discussion of interoperability and standards that's productive.

I think the government needs to think outside the box in terms of creating data commons similar to the precision medicine initiative where people can participate more actively and use their data in more productive ways.

I think the government needs to consider questions of data feudalism as really social questions.

They aren't just questions of how commercial entities deploy and monetize their services. They're questions of how we interact with each other, and how we participate in our

society. So I think those are crucial policy questions.

I also think that the questions of sort of the potential for how data can be unexpected and how it can be used in harmful ways is a core policy question that groups like NTIA can address.

MR. MORRIS: Okay. Craig, quickly.

MR. SPIEZLE: I think just to echo Eric's comment the vast majority of companies are doing really good things here, so let's not be a downer and be negative. I know we focus on the negative here.

But I do think to Harley's point we need -- I think the big area is driving awareness and adoption.

We have a ratified code of conduct, best practices out there. How do we now drive them out there?

And I think the third point, again, it's not just security, and it's not just privacy, but what we call sustainability. The whole life cycle

issues associated with patching the device, data ownership, transferability. Those are key areas. And what we can do there.

And last is we need to take a global view. The IoT is outside this wall, outside of Washington, D.C., outside the U.S., and we need to take a look at what are those issues.

So, combined I think with funding and grants that would be really key areas for the government to help on.

MR. MORRIS: Great. Dan?

MR. CAPRIO: And thanks for the panel. I'd say three things.

One, I mean on a tactical level adopt a framework for a national strategy led by the Department of Commerce and a whole of government approach.

Two, I'd say be strategic. I said at the beginning you can't have privacy without security.

And we really need to think about this

strategically using the NIST cybersecurity framework for managing enterprise risk and getting CEOs and boards involved at the outset.

And then third, I'd just repeat Craig's point is to be global. The world is moving very quickly. Asia-Pacific especially. Europe is moving very quickly as well.

So, for the United States to continue to be competitive we've got to be able to tell the global story and be very proactive about what we're doing here.

And then the relationship with the rest of the world.

MR. MORRIS: All right. John, last word?

MR. KUZIN: I'll be as quick as I can.

First and foremost stay the course. I think we're at a very good stage, very good early stage to support the future growth of the IoT. Keep the hand on the wheel in the same direction.

And just for what government can do --

I think this was raised in one of the earlier panels -- specifically is as a large user of IoT to basically be at least a consciousness raiser of what good it can bring, and in the best of cases a cheerleader for the IoT and what great things government itself is doing to be more proactive and public about the good things, to kind of spur the IoT even more. Thanks a lot.

MR. MORRIS: Great. Well, join me in thanking what I thought was a really great panel.

So, we're breaking for lunch.

MR. HALL: I've got details.

(Simultaneous speaking.)

MR. HALL: So, what we're going to do is we're just going to have a slightly shorter lunch in order to maintain the pace of the panels moving forward.

We will come back at 1:30. We're going to hear some exciting stuff from the Fashion Innovation Alliance.

Then we'll get onto our final rock star

panel talking about the government role.

A couple of quick things. In terms of lunch options there is a cafeteria here. If you go in this direction out of the building across Duke Street we've had recommendations of Sweet Fire Donna's, Quattro Formaggi and Trade, Drink and Eat.

If you just simply go out the building this direction across the street there's Zikrayet Lebanese, Sumo Hibachi and sushi, and a couple of other restaurants.

So, lots and lots of options. See you back at 1:30. And again, if you haven't had a chance to pick up an agenda or sign in feel free to do so over here at the table. Thank you.

(Whereupon, the above-entitled matter went off the record at 12:37 p.m. and resumed at 1:36 p.m.)

MR. HALL: All right, we still have a few people trickling in from lunch, but let's go ahead and get started.

Thanks again for coming out to

Fostering the Advancement of the Internet of Things Workshop. It looks like our title of that changed in the interim because these things happen, but it is Fostering the Advancement of the Internet of Things. Don't let the slide fool you.

We are really excited to have Kenya Wiley join us from the Fashion Innovation Alliance. As the Fashion Innovation Alliance Founder and CEO she works with fashion technology leaders around issues of public policy, social values and fashion law which is really cool. I would love to hear more about fashion law -- to shape the future of fashion tech.

And she is going to talk a little bit about some of the more exciting, innovative uses of IoT. So, with that, I'm going to pull up your slides and hand it over to Kenya.

MS. WILEY: Can everyone hear me okay? All right, great, because I changed mikes. First of all, I'd like to thank the Commerce Department, especially NTIA, for hosting today's first

Internet of Things Workshop And also for the opportunity to share the future of fashion tech.

I'm Kenya Wiley, with the Fashion Innovation Alliance and we're a new non-profit organization based here in D.C. And we're bringing together the entire fashion tech ecosystem around issues of public policy and social values.

We are fashion tech startups, technologists, academics, creative entrepreneurs and technology companies.

So, what exactly is fashion tech? Today I'm going to give you an overview of fashion tech, and then I'm going highlight a few of the fashion tech products and services that we recently featured at our fashion tech showcase on Capitol Hill.

First is e-commerce and mobile. How many of you have made a purchase online? Hands up? That should be everyone in the room.

How many of you have checked out products online, but you end up making the purchase

in the physical brick-and-mortar store?

Okay, so we see that e-commerce and mobile are changing the way that we do business in general and the way we shop, and especially for fashion.

Another area of fashion tech is retail tech. And this is more behind the scenes for retailers as a way to really engage with their customers and track the customers' behavior.

A couple of examples include let's say that you're in the store and you're picking up a shoe or another display.

The retailer is able to track what you're picking up. They're able to mix and match it with the inventory in the store. So that way they know what the customer is picking up and what they're purchasing.

Another example in retail right now, they have interactive mirrors in stores. And so how that works is that, let's say you can have your own personal identification number -- in some

stores, they use your cell phone number.

You key in your number, you determine what you want to put on in the dressing room. And that way the retailer knows what you're putting on, what you're purchasing, what you're trying on and what you're putting back on the rack, and what you don't like.

Next, we have smart accessories and apparel. And this is what we're going to spend most of our time talking about today. In June at our fashion tech showcase we highlighted a number of fashion tech products and services.

And we really discussed that the heart of fashion tech right now, it's about the strategic partnerships and the collaborations between technology companies, fashion brands and the innovative startups.

So, exactly what does that mean? Smart accessories. How many of you in the room have some sort of fitness tracker, whether it's a band or a smart watch? Okay. How many of you are thinking

about getting one? Okay.

Well, I like to highlight Microsoft. Microsoft is our founding partner and member. And Microsoft has been working with another startup that we're working with, elemoon, and really helping them grow and scale to the next level.

As you can see on the left side of the screen that's elemoon's wearable bracelet. And do you notice something different about the elemoon bracelet that you haven't seen in other wearables? It lights up.

elemoon actually has a color-matching feature so you can change the lighting based on what you're wearing.

Exactly how does that work? Well, of course, there's an app for that and you code it based on what you're wearing.

You can actually put the camera phone up to what you're wearing. It matches that and voila, you can change it to white, red, whatever you're wearing.

elemoon is also different because it has a filter feature where you can filter your calls and text messages. So, let's say today you only want to hear from your supervisor, or your spouse, or your kid's school.

You can set those features on your phone so that when you're wearing your watch, your elemoon bracelet, the only thing that pops up is an icon, or a certain graphic so you know exactly who's trying to get in touch with you.

The elemoon bracelet also serves as an activity tracker like the other fitness bands on the market. But, what's different about the elemoon bracelet is that you can wear it to the gym, but it's also stylish enough where you can wear it to the office, or even the opera.

And, of course, there's a find your smartphone feature on the elemoon bracelet as well, and that's connected to the app.

Another cool thing about the elemoon bracelet is that we're noticing that as the tech

is getting smaller in these products they're becoming more stylish, but there are also more functions available as well.

And elemoon calls their bracelet -- it's the first consumer-ready flexible computer for your arm.

And what makes elemoon so unique as well is that pretty soon you'll be able to make smart payments.

So, not only can you match it with your favorite outfit, but you can pay for your morning coffee with your elemoon bracelet as well.

And, I'd also like to highlight, a lot of the companies that we're working with right now, you can see their commitment to social good.

Elemoon has partnered with the United Nations and other organizations to use fashion as a way to get more young girls interested in technology, and thereby increasing the number of women in STEM, science, technology, engineering and math, or as we like to say at the Fashion

Innovation Alliance STEAM, adding art to the discussion.

So, smart accessories. That's the first wave of wearables.

Now we're getting into the second wave and that is with smart fabrics. Just out of curiosity, how many of you attended the Commerce Department's Smart Fabric Summit in April?

Okay, of course. And, in addition to government we're also seeing how industry is getting more involved in smart fabrics as well.

ASTM, the standards organization, they now have a committee for smart textiles. And they recently formed a task group for data security for smart textiles, and I'm the chair of the task group for data security.

So, on the screen you'll see Maddy Maxey of The Crated. Maddy was one of the presenters at our fashion tech showcase in June. And Maddy and her team have really been at the heart of integrating tech into textiles.

I actually brought a sample along today. You can see it's pretty stretchable and the circuits are integrated into the tech. And the possibilities are endless for this. You can use it for biometric sensing, if you want to determine your breathing rate, or your heart rate. It can be used for EKG. It can be used as a stress detector.

It can also be used for posture sensing. Let's say that you're an employer and you have factory workers, and you want to make sure that they have the correct form when they're working.

It can also be used for athletes as well. And you'll notice on the left it can also be used for heating.

So, on the left we see the Kelvin jacket, and that was designed by Maddy and her team. They're actually based in Brooklyn, New York.

And the tech is integrated into the jacket, and it serves as a heater for you. So, let's say it's the middle of summer, but you're

inside in the air conditioning and you are freezing. All you have to do is put on the Kelvin jacket to keep you warm.

Or, let's say it's the winter. You just want to wear a blazer, but you still want to stay warm. What you can do is put the Kelvin jacket underneath whatever you are wearing.

So, we had smart accessories, smart fabrics. Now we are getting into smart payments. We also had Visa at our fashion tech showcase in June. And, Mark Jamison, one of the heads of new product and design at Visa, you can see Mark is showing off Visa's new wearable payment ring.

Exactly how does this work? It is very simple. All you have to do is put the ring on, and then you hold it up near an NFC, near field communication, payment terminal and voila, you've paid for your morning latte.

And it's also very sleek and small, so you can wear it with just about any outfit. You can wear it to work, you can wear it on the weekends,

or you can wear it to the gym.

So, what's next for fashion tech? We're going to see more collaborations, more in the smart fabrics area, between technology and also fashion brands.

One hot collaboration that's going on right now is Project Jacquard. Have any of you heard about Project Jacquard with Levi's and Google? Show of hands. Oh, okay, we do have a couple of people in the room.

Well, it's a new cycling jacket that will be on the market hopefully spring of 2017, and it's geared for cyclists.

So, the tech is integrated into the jacket. So, you wear it while you're biking to work. How many of you bike to work? Okay, so this is not a big cycling crowd, but we have a few in the room.

All right, so, let's say you're biking to work and you get a call. All you have to do is just swipe your sleeve, touch your sleeve or swipe

it, and that actually activates your phone.

So, you can silence a call, you can adjust the volume on your music app, or let's say you want to know how much longer is it going to take before I get to work. The app will do that for you while you're riding your bike to work, and you don't even have to touch your phone.

And, there's something for the athletes too. We're just getting off of the Olympics. There have been a lot of high-tech fashion products that the athletes use to improve their performance.

One goes back to the tech that's integrated in the fabrics with the biometric sensing. We saw a lot of the shirts that the athletes are wearing underneath their uniforms that could detect their heart rate and their breathing rate.

And it was a way for the coaches and the trainers to really figure out what the athletes were doing, if they were performing at their best.

But let's say you're not an Olympic

athlete, you're just an everyday athlete. There's actually a smart shoe for you. Do we have any runners in the room? We have a few. Do any of you have a smart shoe? Okay, you have to get one.

And, how it works is that there's a chip embedded in the shoe. There's an app for it, of course.

But the beauty about the smart shoe is that you do not have to take your smartphone with you when you're running. It's able to track your runs, it could track the distance, your speed, your duration.

But let's say you aren't an elite athlete, you aren't an everyday athlete, you just want to sit on the sidelines and you just want to be a fan.

There is now a jersey shirt for you. It's actually called the smart shirt that you can wear to the football game.

And how it works is that there are sensors in the shirt. You actually download the

app. You can select your favorite team.

So, if your team just made a touchdown and they're excited you can feel the same vibrations and the feelings as the players on the field. And, yes, this actually does exist.

So, as you can see, the possibilities for fashion tech are endless. They're fun, they're exciting and they're also very stylish.

Well, thank you all for being such a great audience this afternoon, and also for everyone who's watching the webcast.

If you have any questions about the fashion tech community, the future of fashion tech, the products that are on the market, I can be reached at kenya@fashioninnovation.org.

And we also have a lot of cool and exciting products that we highlighted at our recent fashion tech showcase in June. We have a video recap on our site, and you can view that at fashioninnovation.org.

And, of course, we are always available

on social media, and the hashtags are listed on the screen. Thank you.

(Applause.)

MR. HALL: Thank you very much, Kenya. And I'm going to go ahead and turn it over to Linda Kinney to start our final panel of the day on the Government Role in IoT.

MS. KINNEY: Ok, welcome everybody to the afternoon panel. Thanks for coming back after a long lunch. So, you've heard a lot today about the whiz-bang things that are going on with the Internet of Things.

But that got me thinking, so what was the first connected device? And is this really a nascent trend, or have we had these things around for a long time?

So, I did a little research, and it turns out that the very first connected device was in 1982 at Carnegie Mellon.

There were some exercise-challenged grad students who got their offices moved far from

the Coke machine and got tired of walking back and forth to the Coke machine and finding that it was empty, or that the Cokes were warm.

So, they hooked up to the Coke machine some sensors, some technology that they could check from their desk to find out, number one, were there any bottles in there and how long had the bottles been in there because that would determine whether they were cold or not. So, that was pretty awesome in 1982.

So, here we are 34 years later and we're talking about the Internet of Things and it's actually become mainstream. So, it has taken a little while, but there are so many new and interesting things going on.

But we wanted to talk today a little bit about what the government role, if any, should be in this area. To do that we have some very distinguished panelists here with us.

I'd like to introduce to you first Hardik Bhatt. He is the secretary-designate of

the newly-formed Department of Innovation and Technology. And he's also the Illinois State CIO.

He also spent a stint in the private sector at Cisco, so he knows a lot about this on the private side. And, prior to that, he was the CIO for the City of Chicago. So, welcome Hardik.

We also have Julie Brill, a former FTC Commissioner. She's now a partner at Hogan Lovells and the co-director of the Privacy and Cybersecurity Practice Group.

She's often referred to, when she was at the FTC, as widely seen as the Commission's most important voice on internet privacy and data security issues. So, welcome Julie.

We also have Len Cali, the SVP of Global Public Policy at AT&T. And he's responsible for developing AT&T's positions on public policy issues, and leading AT&T's international external affairs activities. So, welcome Len.

And we also have Cam Kerry. He joined Sidley Austin after serving as the General Counsel

and the Acting Secretary of the Department of Commerce. Cam is also the visiting fellow at the Brookings Institute and a visiting scholar with MIT's media lab.

So, thank you all for joining us today. I'm going to sit down here with the panelists, as we kick off our Role of Government panel.

So, I thought that the first thing we would talk about is aside from privacy and cybersecurity one of the things we learn from the commenters to our request for comment is that there's a lot of concern about a developing patchwork of regulations.

And we are hearing from industry and other commenters about the fact that these devices cut across many different sectors, from transportation to the health sector. We're talking about drones and the FAA. And so, folks want a consistent regulatory framework.

So, given our group of panelists today I thought we had some expertise in this area.

And, I'd like to go to Julie first to talk a little bit about whether that's possible or practical. What are your thoughts, having come from the FTC, which is an independent agency, what are your thoughts about trying to have a consistent regulatory framework?

MS. BRILL: Sure. So, thank you so much, Linda. And thank you to the Department of Commerce and NTIA for inviting me here. It's a great and important conversation.

So, not only was I a Commissioner at the FTC for six years, but also prior to that I was very involved with state attorneys general, having led two different consumer protection and competition divisions in two different states.

So, I certainly do understand the federalist system within which we live. And, I've spent many, many years hearing about, and discussing with the business community and other stakeholders concerns around patchwork quilt of regulations.

I think it's important to take a step back though before I directly answer your question to focus on why it might be that you'd see a number of different agencies involved in issues around the Internet of Things.

And, it sounds like you spent much of the day focusing on how fabulous Internet of Things can be for individuals, how important it will be for societal benefits. And I truly believe that and truly embrace that.

But there are also some risks and concerns, and I'm not sure how much of the day was spent on some of those.

So, with respect to, for instance, security issues there are some real concerns when you're talking about networked devices.

The network that is created through connected devices is only going to be as strong as its weakest link. And so we need to be thinking very deeply about how to protect those network devices, particularly when some of them are

designed to be inexpensive, to be throwaways.

And you're going to have companies involved who aren't necessarily traditional tech companies who have been thinking deeply about security issues, and may not necessarily have the business models in place to provide patches and updates to consumers.

There's also some really serious privacy issues. Not only will the Internet of Things be dealing with highly sensitive information, whether it's a wearable or a system to monitor kids in their cribs, or some other system that's dealing with geolocation.

Each bit of information is sensitive, but when this information is put together it can create a real portrait and picture of individuals on a very personal level.

There's also some concerns, and I know the NTIA talked about it in its call for comments here, with respect to disadvantaged communities in particular.

Big data and how big data can be used, and obviously the Internet of Things flows into big data types of analyses.

There can be some real issues around disadvantaged communities if we don't recognize up front that sometimes the data that's flowing into these analyses can actually be biased. The entities that are using or implementing some of the devices may themselves skew to one community or another community.

So, the FTC has talked about how it's very important to be thinking about these issues as Internet of Things moves forward and as this data aggregation that comes from Internet of Things creates portraits of our society. But those portraits can be a little bit skewed.

So, the reason I put all that down as a preface is because these are really serious issues. So, to say to entities like NHTSA or the state attorneys general or local folks who are dealing with traffic issues, departments of

transportation in the states, or frankly DOT as a federal agency.

To say stay away, you have no role here, that's going to be hard because these are some really serious issues. And I think they all do have some kind of a role.

I think the question and the difficulties become when you start talking about how we want to think about data use and privacy and data security, as opposed to say like how are cars interfacing with traffic signs and safety signs, and are they doing it in an appropriate way.

So, one of the things that I think government can really do is, for instance, have the Federal Trade Commission and entities like NIST talking to each other about what are appropriate security standards.

And, clearly that's happening even if it doesn't appear to be happening on the surface, because just yesterday you see that the FTC issued a statement saying NIST has come out with a really

good cybersecurity framework, required by the President, required by executive order, and we're going to look favorably on companies that follow that framework as we are developing and looking at data security issues.

So, I think it's important for the different government agencies to encourage strong security when it comes to Internet of Things, but also to be speaking to each other about the different frameworks that are developing and to try to, as best as possible, harmonize them.

I think another issue is should we be looking at Internet of Things-specific legislation? I mean, the Federal Trade Commission a year and a half ago said no, there should not be Internet of Things-specific legislation.

Because generally speaking the FTC doesn't like to focus on tech-specific requirements. It likes to, and believes very strongly, that we need to have rules that are tech-neutral.

And that's because technology is changing all of the time. And you can sort of think about one silo, and one technological silo that might exist today, and it's going to morph and move dramatically in the future.

So, tech-specific legislation is certainly something that we wouldn't want. But we do want to see, I want to see strong data security legislation and baseline privacy legislation which can address a lot of these different issues in a tech-neutral way.

MS. KINNEY: Okay, so building off that, I'd actually like to address Cam. One of the things that Congress did do is introduce the DIGIT Act. And that's something that's being discussed on the Hill today.

And it talks about -- it is actually called Internet of Things, so I guess you could call that Internet of Things-specific legislation.

And one of the things it talks about is having Commerce be a lead agency in convening some

of the different agencies, and try to get to this place where you would have maybe some sort of consistent regulatory regime.

So, I'd like to talk to Cam and hear maybe some of his views from the administration and his seat as the former general counsel, and how he was able to talk to, or deal with some of the other agencies in his space.

And then maybe also go to Len and find out some of the concerns that AT&T has voiced in this area.

And, ultimately to go Hardik and talk about how we're dealing with that at the state level because he has very similar issues. So, Cam?

MR. KERRY: Well, thanks. And, it's always great to come to the PTO. If you haven't been there, you ought to go up to the museum on the first floor. It is great to view the history of American innovation, and I think very appropriate for the topics that we're talking about today.

So, you asked about the DIGIT Act. I

would like to pick up where Julie left off with the notion of baseline privacy legislation. But I think the DIGIT Act certainly reflects that we've come a long way in the last four years.

I was going up on the Hill to talk about the Consumer Privacy Bill of Rights. I met with a subcommittee chair of one of the subcommittees that was supposed to have subject matter expertise.

And I talked about some of the issues that we're facing becoming Internet of Things. And I got this blank look. What's the Internet of Things?

Certainly, the hearings that we've had at the Senate Commerce were I think very thoughtful and focused on the right set of issues.

I think the DIGIT Act is helpful, but I don't think you need the DIGIT Act to convene. You're doing that today.

Certainly, it's helpful to have the statutory authorities in the National Science and Technology Council subcommittee that I was leading

that produced the Consumer Privacy Bill of Rights.

Having that charter from the White House certainly made a difference in convening the agencies.

But you're moving forward, and I think there is a lot that could be accomplished without the legislation, without charters.

But there's a lot to be done. And I think there is a need for the sort of baseline legislation that is reflected in the Consumer Privacy Bill of Rights.

And, what we're seeing today, whether it's people talking about legislation for Internet of Things, or legislation for drones, or education privacy, it's serious problems coming up.

And as the volume of data expands, as it cuts across different sectors, whether it's fitness bands that in one context may generate HIPAA data if you give it to your doctor, but not if you give it to an insurance company, or to an app. It's got the same sensitivities in either

context.

The pace of data, the pace of innovation, the pace of new technologies is moving faster than trying to regulate this sector by sector can keep up with.

I've likened this to that I Love Lucy episode where Lucy gets a job working on an assembly line in a chocolate factory, and the assembly line keeps speeding up and she's sitting there going until she's all balled up. And she says, I think this is a losing game.

Trying to do this sector by sector, state by state, problem by problem is a losing game. And it's time for baseline legislation. I think the Consumer Privacy Bill of Rights that we developed as a White House policy statement in 2012, that the Commerce Department put out last year as a discussion, draft of legislation provides a starting point for that discussion.

It is broad, it is principled, spaced in a ways that apply the technology-neutral, in

ways that are adapted to today's technologies in the way that the principles are stated.

Control, not consent. Those are different things. Focused collection -- that's something different from pure data minimization. Certainly being intelligent about what is collected, and not simply collecting everything because it's possible to do.

It's important, but focused collection is about making intelligent choices. Context, instead of purpose limitations, recognizes that as technology moves you cannot anticipate all of the purposes.

It's broad, but in the use of multi-stakeholder processes, backed up by FTC enforcement and the prospect of FTC enforcement of the principles, creates an iterative process that is consistent with the way that technology develops today.

It would address the distrust in the marketplace that NTIA has found, that Pew research

has found. It would create symmetry across sectors.

So I think the developments, the comments that we're seeing certainly build the case for picking up that discussion about baseline privacy legislation that will apply regardless of sectors, regardless of geography.

MS. KINNEY: Good. So, Cam is saying that the volume of data, for instance, and the fact that IoT cuts across so many sectors, the rapid pace of innovation, all of these things create a new environment in the sense not that these issues are new, not that we didn't have privacy back in 1982, not that we didn't need security, but that these things about the Internet of Things are different and we need sort of a more consistent regime.

So, Len, do you have some thoughts from an industry perspective? I mean is there a really problem, or are these things that -- do we need any changes?

MR. CALI: Well, I do think we need an

affirmative policy to avoid or at least reduce fragmentation.

I understand the concerns Julie's raising, but you do have -- what makes IoT somewhat different, in some ways it's an extension of the digital revolution, but in other ways it's going to affect every sector of our society.

And there is a real risk of fragmentation. And the question is do you want to -- if we all believe the benefits of IoT are there, and I think we do, how can you foster the deployment end of IoT.

And so a comprehensive, coherent, consistent policy framework seems a way to go. I heard Dan Caprio earlier referencing the Clinton policy from '97 on e-commerce and I couldn't state it better.

Given the pace of technology, the competitive and dynamic nature of the field it should be a multi-stakeholder policy, a private sector-led policy, a light touch regulation.

It's interesting, just last week the chairman of the French regulator ARCEP, Chairman Soriano was interviewed.

And he said you could approach IoT in two different ways. You could look at it as a very organized French garden, or a blooming English garden.

And so the French chairman says I choose the blooming English garden. And he says the reason I do that is we're never going to be 100 percent right trying to predict it.

The market should make the decision. Entrepreneurs should have their day, and the job of regulators here is to create opportunity, not to limit business opportunities.

Very consistent with what you hear from the Clinton policy back 20 years ago. But not everyone agrees, and this is a concern.

So, if you look at the ITU today. So, the ITU formed before the UN, grew up during a period of monopoly telecom providers many of which

were owned by governments. And the ITU does legacy standards work for telecom interconnection.

Well, they're extending that remit into IoT. They just opened some study groups related to IoT and particularly the first one up, I believe, smart cities, the U.S., the UK, Germany all said it's premature to launch this study group. But nonetheless it was launched.

It's more than just premature. It duplicates some of the work being done by expert associations and the private sector, multi-stakeholder bodies in standards development.

And what you do is you do run a real risk of fragmentation in a standards-setting. You run a risk of top-down versus bottoms up which we think will slow innovation.

So, I wanted to highlight we've got issues internationally where not all governments align. Some do.

And I don't want to -- we've seen

governments act very well. So for instance, IoT, one version here is you put a SIM in a device. It's manufactured. We call it a global SIM. It's built into the device. The device is built in the factory, shipped around the world. And then the device may move depending on what it is.

Some governments have looked at that in a very progressive way, Belgium, Germany, BEREC the group of European regulators, CTeL have looked at that and said you know what? Even though that looks like it's inconsistent with the territoriality of numbering codes that really doesn't apply here and we should allow the extraterritorial use of numbers.

So I think in that context you've seen the private sector broadly deal with issues around numbering, deal with issues around connectivity using the old roaming frameworks to help allow connectivity for IoT.

So, the pitch here is the flexibility. Giving the private sector wide berth, this is all

new to us, to find paths forward doesn't mean there's not a role for government. There certainly is.

And I think with a framework our government could be a great convener-collaborator globally as well as domestically, a great advocate of the right framework to foster growth.

Cross-border data flows is another area where we see governments wanting to restrict, but this technology really goes in the other direction and would be fostered by greater flows of data.

So our government could be a real voice in spectrum policy and others.

Some people talk about dedicating spectrum just to IoT. We think that's a mistake.

We think they should be flexible use. Providers who are using the spectrum should be able to optimally allocate it among their uses.

So, domestically as well as internationally it's a coordination function, it's a conversation. It's trying to reach

harmonization.

There will be things like airspace coordination. Well, the FAA is going to take the lead on that.

But fragmentation and the uncertainty it will drive and the friction it will create can really slow the deployment of this technology.

MS. KINNEY: Okay. So, I'm going to bring a little bit of what you were talking about because I think what we heard earlier this morning, it's important to continue to drill down to specifics.

And one of the things like Len was talking about, Dan spoke about in the second panel was this Clinton -- the 1997 Framework for Global Electronic Commerce.

Now, what's very interesting about that framework is I would call it a sort of hands-off approach.

So, if you look at the five principles which very high level, private sector should lead,

get rid of unnecessary regulations, a minimalist legal environment.

And they cite IP, privacy and cyber as do as little as possible.

The internet is unique. It's decentralized. It should be bottoms up, not an active government.

And then lastly, the internet is global. Everyone needs to think about consistent regulation.

But what we're hearing is something a little bit different and I'd like to drill down on that and move to Hardik and talk to him about maybe -- I'm hearing that maybe we need a little more action, which is different.

So, one of the things Len just said is government should be a convener. Well, that's an active role.

Instead of private sector leading it's government convening. So, it's actually taking an action.

And do we need to update this '97 framework with some more active role of government? Or not?

And the other thing he said is a collaborator. That's another active role of government.

And the other thing the panel this morning talked about is maybe government as a user. Again, that is an active role, not a hands off, but actively use technology.

So that's where I think maybe we can learn a little bit from a state perspective. I know that's an area that has been a priority for you, Hardik, in Illinois.

And you've really been at the forefront of trying to be government as a user. So maybe you could tell us a little bit about that experience and why you think it's important and what you've done.

MR. BHATT: Certainly. Thank you, Linda, and thanks, NTIA and Department of Commerce

for inviting the State of Illinois here. It's great.

I think Illinois was one of the only local or state government that responded to the green paper comments.

So, prior to Illinois I have worked with numerous governments globally. I've worked with Barcelona, I've worked with Dubai, Hamburg, how Copenhagen is using their smart lighting technology, Chicago, San Francisco and others.

And what -- that was in my prior role at Cisco.

What we actually are forgetting, or kind of missing the big picture of IoT. We've been talking since morning about which touches the surface, scratches the surface about consumer use of IoT.

There's a profound impact that the Internet of Things is bringing to the mankind around how healthcare changes, how education changes, how agriculture and food changes, how

water distribution, retention and all those.

The key assets in our lives is going to positively get impacted by the Internet of Things of technology and how it gets implemented.

So, in Illinois we look at the government's role from three aspects. It's not just about policy and legislation.

The first and very active role of government is government as a customer. And we need to start getting our act together as government to start being the role model of how the Internet of Things technology can be used.

We all know how government technology is, and it has been like this because we have always worked in silos within the government.

And whether it's breaches that are happening right now is how we started building technology many years ago.

And IoT is going to in fact accelerate those issues, or in fact make them more transparent if the governments continue to work in their silos.

Not just the silos within the government bodies or the boundaries, municipal, state, federal, but also within the government also there are so many silos. Transportation, public safety, public health.

And we act as if we have nothing to do with each other, but we forget that at the end of the day we are serving the exact same taxpayer that's driving on our road, that's going through unfortunately sometimes our public safety or corrections system, that's also using our public safety, and that's also using the food and water that governments enable.

So, one big thing that we are doing at the State of Illinois is we have an Internet of Things center of excellence in which we have brought 11 different agencies that have anything to do with IoT.

Public safety. That includes state police. Corrections, emergency management, National Guard. We also have transportation and

tollway, public health.

Department of Innovation and Technology is the convener for this center of excellence where we all work together.

We have done an internal survey to understand what is our baseline of IoT penetration in the state. And then we are now building a prioritized list of what we need to implement.

We are not doing that in a vacuum. We have an external advisory body that's working with us that is made up of the industry, of the academics, as well as the entrepreneurs that are helping us to see where IoT industry is going in terms of solutions, technology, policy bottlenecks that they should foresee. Financing, how do we finance these things?

So, we're looking at this from a comprehensive point of view from a government as a customer. So that's role one that we're looking at.

The role two is the government as an

enabler or a facilitator. And that's what I think we have heard since the morning is that government should facilitate until it knows what to regulate and how to regulate.

There is a lot that the government can do before it starts regulating. We have an incentive structure that we have to improve our innovation and entrepreneurship.

And Illinois is working hard at making sure that we are actually creating that IoT entrepreneurship in Illinois, whether investing in incubators, whether investing in tech commercialization.

We also have two fantastic national labs, Argonne and Fermi. How do we commercialize the technology that gets developed over there.

And at the same time focusing on talent development because you need analytics. You need mobile. You need sensor technology. You need cybersecurity.

That talent needs to get developed.

And whichever state is ahead in that is going to be a part of that.

And the third role that we are looking at is IoT is really gaining traction in cities, large cities. Chicago, San Francisco, New York.

What happens to Peoria, Illinois? What happens to Sandwich, Illinois with 1,000 residents? How do they get in the game?

And that has been -- I mean, look at the United States. We have maybe 10 big cities, and then everything is mid-size and then small cities. How do we get the rest of everyone in the game?

And that's where the government's role also comes in. For the State of Illinois we have two major levers that we are looking in.

One, we have a tremendous proliferation of state-provided fiber called Illinois Century Network. And that goes across the state. We are looking to improve the usage of that.

And then most of the state governments have -- and then the federal government has GSA.

But most of the state governments have statewide joint procurement authority. If a state can do a joint procurement which is statewide for, say, a smart lighting solution, Peoria and Sandwich can buy off of that, and now suddenly we are giving economy of scale to those smaller cities.

So we are looking at that comprehensively as a practitioner for the IoT.

MS. KINNEY: Excellent. Well, that was very helpful.

Just to involve the audience at this point, I think Hardik has talked about some of the reasons why the government should be a user and what the benefits of those are.

And one question I have is are there other reasons why it's helpful to have the government be a user of this technology.

Because we heard a lot about that in the comments and I'm just curious about why that was such a universal theme.

MR. HOSAIN: Hi, I'm Z Hosain, CTO for

Aeris Communications.

We have been very successful in deploying a cellular M2M IoT service. I'm one of the founders. We've been doing this for 20 years, before the terms IoT and M2M even existed.

Third largest in the country behind our friends at AT&T and Verizon. And globally we're in the top 10.

We find that there are situations where people don't understand the issues associated with deploying these kinds of applications.

And setting generic policies that try to cover the whole gamut of the kinds of applications that you see is a problem.

The fragmentation issues that Len mentioned and Cameron mentioned creep up all the time.

National issues creep up all the time. We have to incorporate data centers in countries because they have data privacy rules that data cannot leave the boundaries of the country, et

cetera, et cetera.

Even our data center in London, the EU isn't monolithic. We're discovering national issues that restrict the capabilities that we have.

If we are not careful about the U.S. and we create situations which cause fragmentation down to the city, state, or even lower, cities within states, or counties such as the taxation policies that go on with cellular phones today we would create a cost burden that would not foster the Internet of Things of applications. That's a comment that I think we need to be careful about for all the policymakers that are out there doing their job today.

MS. KINNEY: Okay. So, just building off that because I really want to get to some specifics here.

We've heard -- we have a lot of high-level notions and I think Len did a good job setting the stage on the international issues that we're all confronting.

So again, this title of this panel is the role of government. And so we're looking at what is the role of government there. I mean, what should we the United States be doing.

One of the things NTIA does, we have -- we do represent the United States government in some of these fora.

So we heard this morning about problems with the ITU. Also Len raised that.

Is there a partnership here? Is there a way that the industry can work with the federal government and try to deal with these issues in the international realm? So, Len?

MR. CALI: To build off what you said earlier. I want to draw a distinction between the policy and the role of government.

So you can have what you would characterize as a hands-off policy and that's the right policy maybe. I think it is the right policy.

It's like privacy. You talk to some

Europeans and they don't think this country has a privacy policy. Well, it clearly does. It's an affirmative choice.

But articulating and advocating that, being the voice at the table.

And I think the U.S. government has done this wonderfully. The U.S. government has stood for internet governance that isn't government dominated.

It's worked hard in international fora to partner with industry in making the case. So I think that is a very concrete role, and I think we need to do that.

The second aspect, going to the points Julie made, there will be questions with IoT that are tougher than questions that came before.

But rather than regulate first what we should be doing is stepping back. I think Hardik made the point.

Understand these things. Figure out the right way to deal with them. I think a

multi-stakeholder process with the people who are inventing the technology and deploying the technology is part of the answer to figuring out where is the problem, what's the best way to resolve it and do we keep the innovation going.

MS. KINNEY: Did you have a comment also?

MR. SZABO: Yes. Carl Szabo from NetChoice.

Hardik, I'm glad you're here because I think a lot of this will operate on the state and local levels.

And Commissioner Brill, I do agree with you. There is a role for states and state governments.

One of them is getting some antiquated laws off the books that are impeding. So Illinois, for example, your state just commissioned an autonomous vehicle study group.

I think it's a good first step into legalizing autonomous vehicles because that kind

of paves the way, no pun intended, for that technology.

Likewise, we have laws against trucks slipstreaming essentially, reducing drag, increasing fuel efficiency. Get those laws off the books.

Would it be helpful, Hardik, some other laws that could possibly -- that are kind of outdated, need to be updated to facilitate innovation, and/or having the federal government as kind of a convener/champion of some of this updating and innovation of these antiquated laws.

MR. BHATT: Absolutely I think it does.

So, one of the five areas that we are focusing on our IoT generally is policy and regulations.

And how we are approaching that is we already have an internal survey that we have sent out to all our general counsels to look at technology policy and regulations holistically and come back to us as to what are the bottlenecks of.

And then we have compared them -- we have given them the list of things, potential things that might be coming like the autonomous vehicles, or like the providing telehealth, telepsychiatry and other services that we need to provide.

And then come back to us with everything that they think is going to be.

Now, you know, changing legislation, it's not that -- especially in Illinois it's not that easy.

MR. SZABO: You're much faster in the states than we are here in D.C., so there is that.

MR. BHATT: But then the other part of that is just not doing it from inside. We are also looking at input from outside.

So, we are looking at building a virtual policy center within our center of excellence and trying to get input from outside.

And that's where Cisco's and IBM's and Microsoft and AT&T's are playing a key role because

they have a global view of policy and regulations that they come across.

Things that are working in Australia and Barcelona, if we can at least learn about those things we can apply those things.

But you are absolutely right. I think we are trying to implement 21st century technology with the boundaries of 20th century regulations and we need to change that.

MS. KINNEY: So, I'd like to go back to Julie. We are again talking about the role of government here.

So, I know one of the areas that you feel strongly about is multi-stakeholder processes, and the importance of those.

So, why do you think those are important? Do we have enough of them? Do we need a strategy around that?

MS. BRILL: So, I actually think there really is an important conversation that needs to take place in a multi-stakeholder context with

respect to some particular IoT issues.

I just have to comment, we're never going to get the FDA out of the business of regulating the safety of medical devices.

We're never going to get NHTSA out of the business of regulating the safety of cars.

We're never going to get the FAA out of the business of regulating the safety of drones.

I think that's their role. I actually think that it's good to have them participate.

So that just goes to the fragmentation issue.

I do think it makes sense to have someone sort of coordinating or have these agencies converse with each other when there are issues of overlap like data use.

And frankly the FAA even stepped away from thinking about privacy issues with respect to drones because they realized that just isn't their role.

But to your particular question I think

there are two really important conversations that I'm hearing about from both academia and from the business community that they feel these issues haven't really been addressed very well.

One is with respect to the use of health data. There have been a number of groups that have put together principles with respect to health data and how it can be used, and when it can be used, and what kind of permissions we need, and what kind of use-based models we need, et cetera, et cetera.

None of those principles have really taken off. And in the meantime you have researchers who are really struggling to figure out, well, how can I use this data?

There's this incredible rich source of data out there from wearables and whatnot and we're just not able to access them in a way that we feel will be protective of individuals' rights and also give us the benefits that we need.

So, I would say that one area where I think NTIA could play a very useful role would be

to focus on a multi-stakeholder conversation around health data.

The other topic that I think is blossoming now is the connected home. And I will throw into the connected home connected toys.

I just did an event with a number of different organizations around kids and connected toys.

And the concerns are when you have one child playing with a toy that's connected you can have that parent give permissions under the Childrens Online Privacy Protection Act and you can follow all those rules.

But what about that child's playmates? And what about all the information that is connected in an ambient way through connected toys?

You really need to look out and say it's not just about toys. It's really connected homes in general.

You can have the individual who owns the home give all sorts of permissions about whether

or not data should be collected or not and how it should be used.

But then what happens with guests in that home? What happens with other people who come in the home?

So, I think this notion -- so I bucket all of these issues into the connected home because it's information that is being gathered where you have one group of people who are clearly able to give permissions, but you have others who may not even know that their data is being collected and certainly aren't in the permission stream.

So, I think a really good conversation could be had through NTIA's auspices that would be a multi-stakeholder conversation to talk about this ambient data issue with respect to the connected home, and connected toys, and other connected devices.

Because I think you've got folks in industry scratching their heads trying to figure this out. And it would be good to get some

principles circulated so people can really start to think about it in a more cohesive and logical way.

And also to get the learning from others and maybe really develop some consensus around what those principles should look like.

MS. KINNEY: So Cam, what about what Julie says about having the Department of Commerce maybe be a coordinator and bring together some of these other agencies?

So, given your experience at the Department of Commerce is that realistic? Is that a good idea? Do the other agencies listen to us?

MS. BRILL: Of course they do, of course they do. They just might not listen as well as you want them to, but they listen.

MR. KERRY: So, I think there is an important role for the Commerce Department to play here.

I think the multi-stakeholder processes that we've been talking about are really

at the center of that. And it's something that I think bridges a lot of the discussions that we've had today.

It is I think at the core of a regulatory model that we as a country need to present more clearly to the rest of the world.

I think there are opportunities to do that by engaging in some of these multi-stakeholder discussions -- take connected vehicles -- is a clearly a transborder issue to work with other countries.

Most of the other international manufacturers are here, engaged in our discussions. So, this is something that's easily portable. And I think to engage with our European trading partners, in particular in this process, would give them some greater comfort with a process of policy making that they are uncomfortable with.

I mean, Len talked about -- Julie, and we've all been involved in these discussions with the Europeans. Dammit, we have laws -- we care

about privacy. But you have no law, and you leave it all to self-regulation.

I think to engage with them and get them involved in these processes would help in the understanding of that. It would help in articulating to the world a coherent and effective model.

As I've said, I think that would be strengthened by having legislation that fills in gaps. But, regardless of that, I think that we can proceed.

I think that multi-stakeholderism is part of the credibility that you bring to other agencies and honed in the NIST framework that I fought with other agencies that wanted to take a much more prescriptive approach to cybersecurity.

But, look, this space -- that government prescription is a recipe for failure. You need to do this in a public-private partnership. And that's ultimately the model that was adopted in the President's executive order, and

it's now been carried out in the NIST framework.

NIST didn't just go out an develop a bunch of standards. That is a great example of the government as convener, or as facilitator, working with the private sector to develop an approach to issues.

And that's something that can be replicated across other areas. Whether it is health devices -- he may have some issues with HHS there, but there has been a partnership in the past.

And I think the multi-stakeholder role, to bring people who are not HIPAA-covered into the discussion would add important value to that discussion and, perhaps, help to deal with some of the issues that I talked about earlier about health data being the same data, but being subject to different treatment depending on who has the data.

And, so that's a great example of where a multi-stakeholder process can work, where it adds enormous value to the policymaking framework.

MS. KINNEY: So, Cam's going to get all

of the agencies to listen to us, and the Europeans, so that's awesome.

(Laughter.)

MR. BHATT: So, in Illinois' comments to the request for comments we have gone a slightly different route. And that's based on my experience at the state, and also at the city. And I'm hoping that the federal government works that way too. But, I'm sure it's different.

What we suggested is to have, actually, a deputy CTO position at OSTP and White House that is responsible to coordinate all of the work that goes on in IOT, including working with the Department of Commerce.

I think that position provides the neutrality across all of the agencies. So, even though I'm the secretary-designate for the Department of Innovation and Technology of Illinois, I keep holding the position as the State CI and report directly to the Governor.

And that gives me a kind of -- that power

and neutrality to have all of the agencies work with us and we can drive them. Similarly, a Deputy CTO in the OSTP, or the CTO if that person is made responsible for that, can work with the industry, can work with the administration, all of the agencies can work with the academia, can also work through the Department of Commerce with Congress, and also represent the country internationally with these things.

I think there is a possibility of that and I think that would really help convene the multi-stakeholder conversation that needs to happen.

MS. KINNEY: Thank you, Hardik. Does anyone from the audience have something else to add about government role as a convener?

MR. SPIEZLE: Craig Spiezle here, with the Online Trust Alliance, and this is a question for Julie. Not representing the FTC or any Commissioner here, but reasonable disclosures.

So, the challenge today is, you buy a

TV and you bring it home and you mount it on the wall. You're now setting it up and, at that point, to use some of the cool features, that's when you learn that that's how you have to disclose and share some of your information.

So, I would suggest, and actually one of your colleagues had disagreed with this, is that we have to rethink disclosure notices. It's not like an app or a website you visit. Now you're buying a product.

And, so, what is reasonable disclosure on a physical product and how should that occur?

MS. BRILL: It's a great question. I actually had a piece in the New York Times about this about maybe two years ago.

You know, it's not an issue of whether or not the FIPPs apply, it's how you're going to apply them when you don't have any user interface or you've got very, very limited user interface.

And, I do think -- I've seen some really interesting IoT devices that can't be turned on

until you go to the app and you walk through a permissions or disclosures kind of process.

So, one of the things that I've been recommending, and I have recommended in the past and that some of the more innovative thinkers are saying, is we need to be creative, you need to have immersive apps, you need to also think about auditory signals -- think about Amazon's Echo -- it's visual and auditory.

So, you are going to need to have disclosures and you're going to need to have signals and information going to consumers. But, with respect to connected devices when you don't have clear spots where there are user interfaces on the device itself, you're going to have to be much more creative.

And, I think it's going to have to be apps and it's going to have to be these other kinds of visuals and auditory signals. But disclosures have to happen, to your point.

MS. KINNEY: Thank you. Ajit?

MR. JILLAVENKATESA: Great, thank you. Ajit Jilla from NIST. And, if I may, on behalf of NIST, thanks for the shout outs to the NIST cybersecurity framework.

So one of the questions that actually comes from, whether it's the cybersecurity framework or any other government-coordinated framework-type activity, is where does the government's role end?

Does it end when we create the framework? How long do we actually take care or nurture the framework? And what's the handoff to some of the organizations, particularly with the private sector?

And I think this has various dimensions. It's certainly, how long do we maintain, but also do we take it, for example in the case of the cybersecurity framework, through an international standards organization?

So, what's the tradeoff? So, I'd appreciate any thoughts and feedback from the panelists.

Thank you.

MR. KERRY: Sure. I think, as NIST has done, that the framework doesn't stop when it's announced. It needs to be iterative. There is a version 2.0 in the works. And I think the other thing the government can do is to nudge the uptake of the framework, which certainly I've been very pleased and maybe pleasantly surprised at the degree to which it has had uptake in standards by various organizations, even by other governments -- the UK.

And I think there's some things that the government can do to nudge that along, and certainly to use its role as a customer to help promote the uptake of that or of other standards.

It doesn't mean it endures forever, but it certainly has a life beyond the creation of the framework.

MS. KINNEY: Did you have something to say also, from an administration point of view?

MR. CALI: Yes, well my thought is that

it's impossible to know in advance. It's like asking him a question, when is your child ready to leave home, right? Well, it depends on the child. My only point being, you may not know.

And part of it is going to be the uptake, part of it is going to be the iterative process. The hope is you do see a role for government. If you see a role for government, you engage in a multi-stakeholder way.

And then you see how the industry evolves. You've seen it with the internet, how the U.S. Government began with much more engagement and has been continually privatizing, right?

But I don't think it's something you can sit here and project. I think you have to look at each issue in each context and hopefully you reach that point.

MS. KINNEY: Just one last question, because I think we're about out of time here.

MR. NEW: Hi, Josh New here, from the Center for Data Innovation. Something that wasn't

really talked about today, but I think it's really important for the government as convener, particularly coordinating local and state governments' deployments of smart city technology, or just IoT in general, is the next generation of the digital divide.

We call it data poverty. So, people who live in data deserts, or they can't participate in public and private sector data collection efforts and they don't benefit while people in the more affluent communities benefit disproportionately, and those people are left further disadvantaged.

How do you think the federal government should play a role in encouraging this kind of equitable deployment, either from a government perspective -- like what's the best way to engage these local and state governments? Or from a private sector perspective, what do you want to see the government doing to make sure that you can -- I mean, of course you get more customers this

way, that you can ensure that this is not just a tool for the wealthier communities?

MS. KINNEY: I think Hardik and Julie probably have some quick remarks.

MR. BHATT: Sure, I wouldn't say that this is the only way or a perfect way, but going back to the Broadband Technology Opportunities Program, BTOP, there was funding available for infrastructure and funding available for access and awareness and everything else.

There was not enough, but it was geared towards underserved communities. A lot of that funding went to rural parts of the U.S., but that also is very severely underserved.

In Chicago, we had specific focused effort around awareness education and uptake in that area. So that underserved community can start using technology significantly more. There has been progress. I wouldn't say tremendous progress, but there has been progress through the mobile and smart, and every kind of technology that

is changing.

As I said, that's not the only answer. There are multiple other things that has to happen, and continuous focus needs to be there from the federal government, state and municipal, all levels of government.

And I think that is also -- I will say that it isn't a responsibility of the government only. That's also multi-stakeholder game. And everybody has to focus on that too.

MS. BRILL: So, I will just say really briefly that I completely agree with you and I did try to allude to some of those issues around data that could end up disadvantaging groups, because we aren't recognizing sufficiently data deserts.

I completely agree with what Hardik said. You know, you need to have a strategy to really reach out to those communities and to get them the appropriate tools. But, in the meantime, we also need to recognize that those deserts do exist.

And we can't develop national policies, economic policies, tax policies, road maintenance, whatever you want to talk about. We need to recognize that there might be whole pockets of communities that aren't communicating because they just don't have the means to do that.

And there have been lots of studies on that issue, and I think it's an incredibly important one. So, thank you for reiterating it. I know the Federal Trade Commission has been thinking about that quite a bit.

MR. BHATT: I would like to add to that. It is extremely important because, if you think about it that is where most health and human services is going, the data deserts mainly.

That is where also a lot of resources unfortunately around public safety and correctional facilities are being spent. That is where the least resources are going in terms of education and self-sufficiency.

So, we need to turn that whole thing

around. And, that's what I think technology and IoT can play. And that's where I was going in my initial comments, where IoT has much, much larger significant impact on mankind if it is used appropriately for the right reasons in an equitable way. So, thank you very much for bringing it up.

MR. CALI: And can I, just from a business perspective in critically important issues, smart cities technology, if we're right about it, it should pay dividends to communities.

So, it should not be ultimately a cost, but a real value and a real benefit. AT&T itself has announced they'll host pilot cities. Government clearly has pilot cities and challenge grants that are really valuable.

But the key here is this is all new and we need to figure out how to "productize" it and then costs come down. So, right now we have all of these great ideas, and industry is deploying technology, cities are buying technologies, but ultimately we want to get to a place where it's on

the shelf and you go to a city and every city will be customized a little.

But you go to the city and you say here's what I've got and I know these are the types of returns you'll see. And I think that'll help with uptake everywhere.

MS. KINNEY: That's a great place to end, I think. And also a plug for the Smart Cities Week at the end of September. We actually are working on that very issue from a coordinated federal perspective across all of the agencies, and talking a lot about how do we come up with that strategy and that plan for best practices, lessons learned to help the other cities.

So, just to wrap up and go full circle, I want to be respective of everyone's time. Going back to something that Dean Garfield raised this morning, it seems so long ago.

He said, well, maybe one thing you need is, what the FTC did, was this broadband plan. And that was kind of this comprehensive thoughtful way

to look at all of the various different things you could do in this area.

Len, building on that, said look the policy can be the hands-off policy from '97. Those principles may still be valid, but then maybe you also need a role for government, some proactive measures.

And we talked a lot about those today, so just to sum up some of those, the government as the convener, we talked about multi-stakeholder processes, we talked about the government as a customer -- very important, because that drives economies of scale to bring down the cost of deployment.

The government as a facilitator. So, Hardik raised incubators. I want to put a plug in for our ITS lab out in Boulder. We are actually looking at the Internet of Things and looking at density issues, and tried to measure if all of these things flood the market is there going to be an interference problem?

Again, something a government can do perhaps better than an individual industry. I think we heard more money for BTOP, thank you, and the Broadband Opportunities Council.

We also heard government can help with the infrastructure, whether it's more grants for broadband or more spectrum. So, again, a proactive role. Not necessarily a policy or a strategy, but perhaps a role for government that we could take that would be helpful and proactive from a government perspective.

So, thank you very much to our panelists, but I do want to say this is not the last word, unfortunately, or fortunately for the rest of us. The discussion's not over, this is really the beginning of a conversation.

We are looking at putting out a green paper that will be asking and perhaps trying to define some of the issues, issues spot, narrow some of the things. But, also, maybe make some recommendations, ask more questions, get more

input for the next administration, the next Congress.

So, keep thinking, keep talking amongst yourselves, keep talking to us. We really need to hear your input and input of all stakeholders. So, thank our panelists and our audience.

(Applause.)

MR. HALL: Excellent. Thank you so much. And I just want to -- before we go to our last speaker, Angela Simpson, who is our Deputy Assistant Secretary for NTIA who's going to close things out for us, I do want to say one last time thank you so much to NTIA, to USPTO, to NIST, to everybody who has been involved in making today happen.

To all of the panelists. To the moderators. And of course also the team at USPTO who have been really awesome and responsive in terms of making this space available to us.

And so with that I'll hand it over to Angie. Thanks again.

MS. SIMPSON: All right. Home stretch, guys.

So, I wanted to thank you all for being here today, for what was a very productive discussion.

I feel like we could have gone on and on with each topic that we talked about. So I think that that is a sign of a very timely workshop.

So, we convened this event today to listen, and to learn, and to go beyond some of the issues identified in our request for comments.

One thing that's clear is that there are many beneficial ways the Internet of Things can be utilized from things like realtime analysis of inventory in retail stores, to sensors in the cabs of trucks to help measure fuel efficiency, to the use of connected technology that allows you to adjust your thermostat from work so it's cool when you get home.

And I think that one thing that was interesting to me today was the potential

distinctions that we discussed between industrial and consumer IoT. And so that recurring theme was something that we might explore further.

One of the things that we tried to do was to really drill down deeper into some of the potential policy issues by exploring specific recommendations that people had and discussing what types of government engagement might be beneficial.

And I think we really did advance the ball today on these issues so I wanted to thank the speakers, the presenters and also the audience participants for helping us do that.

Way back it seems like a long time ago earlier this morning Assistant Secretary Larry Strickling had a very insightful discussion with Dean Garfield who is the head of the Information Technology Industry Council.

They talked about the enormous societal benefits of the Internet of Things and discussed ITI's concerns about the need for thoughtful

government engagement and investment.

We also heard about technical building blocks that will enable IoT such as the availability of spectrum, the need for voluntary interoperable standards, identity management, technological neutrality and cybersecurity.

So, all of these issues are things that the Department of Commerce is very well positioned to discuss.

For instance, NTIA's work on spectrum and making more spectrum available for wireless broadband, and NTIA's efforts to promote broadband access and adoption. And also NIST's work on cybersecurity.

I think we also heard a really thoughtful discussion today about the potential challenges to IoT. Again, things like cybersecurity and policy rose to the forefront.

And we've been using multi-stakeholder processes to get at some of these challenges. And they will continue to be priority issues for the

Department of Commerce and NTIA as part of our overall mission to ensure that the internet remains an engine of innovation, economic growth and free expression.

I was particularly interested in CDT's framing of data feudalism and Julie Brill's and other folks' discussion of potential IoT inclusion divides as a potential challenge that we should think more about in the future.

But as we discussed during the last panel the government has many potential roles to play in the IoT space, as a consumer that drives IoT -- in my mind NOAA pops up as a big user in its connected technologies to measure weather -- an enabler of IoT and an educator about IoT.

These considerations extend beyond traditional rule-making and enforcement and beyond the federal level to the state level, the local level and even the international level.

And I think we got some really good insights today about the potential roles the

government should play to help foster IoT.

It's becoming more and more clear to me that we need to work across sectors, across agencies to build a coherent model to engage in IoT. And I think we heard some validation of that point here today with our speakers.

So, Commerce's International Trade Administration, NIST, PTO and also NTIA are actively engaged in these spaces -- you know this -- to help promote positive policy choices and to promote American innovation and trade around the globe.

So, just before you leave today I want to outline a bit more of where we're going from here today.

We plan to incorporate the valuable information that we received today in the discussions as we finalize the green paper that Linda mentioned.

And that green paper will hopefully identify some potential next steps for both the

Department of Commerce and the administration in the future.

In addition, we're also actively addressing cybersecurity related to IoT which we discussed here a lot today. And it was also one of the top issues raised in the request for comments.

Earlier this summer we announced at NTIA that we're going to launch a new multi-stakeholder process to support better consumer understanding of IoT projects that support security upgrades.

I wanted to let you know that we're looking at the third week in October to launch that multi-stakeholder process. And it's likely going to be outside the Beltway so please stay tuned for more information on that as we get more details available.

Also, just wanted to let you know that stakeholders involved in the currently ongoing process aimed at developing guidelines related to

disclosure of cybersecurity vulnerabilities are making really good progress and appear to be on track to wrap up their work before the end of the year.

So also be on the lookout for some output products from that group.

So just in conclusion I wanted to really thank you wholeheartedly, I wanted to thank you all again for your participation in the event today.

And we really look forward to remaining engaged with you as we continue talking about this really exciting topic.

So thank you very much today and for hanging in there till the end. Thanks.

(Applause.)

(Whereupon, the above-entitled matter went off the record at 2:59 p.m.)