AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 114–237

THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

FEBRUARY 11, 2015

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

99–818 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
RON JOHNSON, Wisconsin
DEAN HELLER, Nevada
CORY GARDNER, Colorado
STEVE DAINES, Montana

BILL NELSON, Florida, *Ranking*
MARIA CANTWELL, Washington
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
CORY BOOKER, New Jersey
TOM UDALL, New Mexico
JOE MANCHIN III, West Virginia
GARY PETERS, Michigan

DAVID SCHWIETERT, *Staff Director*
NICK ROSSI, *Deputy Staff Director*
REBECCA SEIDEL, *General Counsel*
JASON VAN BEEK, *Deputy General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
CLINT ODOM, *Democratic General Counsel and Policy Director*

CONTENTS

	Page
Hearing held on February 11, 2015	1
Statement of Senator Thune	1
Statement of Senator Nelson	2
Prepared statement	3
Statement of Senator Ayotte	128
Statement of Senator Peters	130
Report dated November 12, 2014 entitled "Consumer Privacy Protection Principles—Privacy Principles for Vehicle Technologies and Services" by the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc.	131
Statement of Senator Schatz	138
Statement of Senator Daines	140
Statement of Senator Heller	142
Statement of Senator Booker	144
Statement of Senator Fischer	146
Statement of Senator Gardner	149
Statement of Senator Moran	151
Statement of Senator Klobuchar	152
Statement of Senator Manchin	154
Statement of Senator Markey	156
Report dated February 2015 entitled "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk" by the staff of Senator Edward J. Markey	157
Statement of Senator Cantwell	171
Statement of Senator Blumenthal	173
Letter dated February 10, 2015 to Chairman John Thune and Ranking Member Bill Nelson from Gary Shaprio, President and CEO, Consumer Electronics Association	175
Letter dated February 11, 2015 to Hon. John Thune and Hon. Bill Nelson from Scott Belcher, President, Telecommunications Industry Association	176

WITNESSES

Michael Abbott, General Partner, Kleiner Perkins Caufield & Byers	5
Prepared statement	7
Douglas Davis, Vice President and General Manager, Internet of Things Group, Intel	9
Prepared statement	11
Lance Donny, Founder and Chief Executive Officer, OnFarm	21
Prepared statement	22
Article dated January 2, 2015 entitled "Towards Smart Farming—Agriculture Embracing the IoT Vision" by the Beecham Research Ltd.	25
Article entitled "Agricultural Water Conservation in the Lower Flint River Basin of Georgia" by the Flint River Basin Partnership	31
Report dated January 26, 2015 "NEAA Technical Advisory Group Report—NW Agriculture Irrigation Energy Efficiency Initiative" by the Northwest Energy Efficiency Alliance	32
Article dated December 4, 2014 entitled "10 Policy Principles for Unlocking the Potential of the Internet of Things" by Daniel Castro and Joshua New, Center for Data Innovation	50
Report dated April 2014 entitled "AgTech: Challenges and Opportunities for Sustainable Growth" by Suren G. Dutia, Ewing Marion Kauffman Foundation	57

Page

Lance Donny, Founder and Chief Executive Officer, OnFarm—Continued
Report dated May 2014 entitled "Agriculture Gets Smart: The Rise of Data and Robotics by Amanda Faulkner, Research Manager, Cleantech Group and Kerry Cebul, Principal, Cleantech Group 83
Adam D. Thierer, Senior Research Fellow, Mercatus Center at George Mason University 89
Prepared statement 91
Justin Brookman, Director, Consumer Privacy Project, Center for Democracy & Technology 116
Prepared statement 117

APPENDIX

Letter dated February 9, 2015 to Hon. Fred Upton, Hon. Frank Pallone, Hon. John Thune and Hon. Bill Nelson from Thomas E. Kern, Interim President and CEO, Intelligent Transportation Society of America (ITS America); Mitch Bainwol, President and CEO, Alliance of Automobile Manufacturers; Michael P. Melaniphy, President and Chief Executive Officer, American Public Transportation Association; Frederick "Bud" Wright, Executive Director, American Association of State Hihgway and Transportation Officials (AASHTO); John Bozzella, President and CEO, Association of Global Automakers, Inc.; Greg Cohen, President & CEO, American Highway Users Alliance; Jill Ingrassia, Managing Director, Government Relations and Traffic Safety Advocacy, AAA; Roger A. Wentz, CAE, President and CEO, American Traffic Safety Service Association; Brian Pallasch, Managing Director of Government Relations and Infrastructure Initiatives, American Society of Civil Engineers 191
Response to written questions submitted by Hon. John Thune to:
Michael Abbott 192
Douglas Davis 193
Response to written questions submitted to Lance Donny by:
Hon. John Thune 194
Hon. Roy Blunt 195
Response to written questions submitted by Hon. John Thune to:
Adam D. Thierer 196

THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS

WEDNESDAY, FEBRUARY 11, 2015

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 9:47 a.m. in room SR–253, Russell Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Blunt, Ayotte, Heller, Fischer, Moran, Gardner, Daines, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Booker, Manchin, and Peters.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. This hearing of the Commerce, Science, and Transportation hearing will come to order.

This morning we convene to examine what may be the most important trend in technology today: the Internet of Things.

I want to thank Senators Fischer, Ayotte, Booker, and Schatz for their leadership on this issue and for encouraging this committee to examine the IoT.

By now, all of us are very used to having at least one or two electronic items near us that are connected to the Internet, such as computers, phones, and TVs. Increasingly, however, we are seeing common everyday objects being connected online, a literal Internet of Things that will soon be ubiquitous.

These things unobtrusively gather data and communicate with users and with other devices to solve a variety of consumer and business needs.

Some have argued the Internet of Things is the third wave of the Internet following the fixed Internet of the 1990s and the mobile Internet of the 2000s.

The economic impact of IoT promises to be significant and will drive growth in every sector of our economy.

According to McKinsey & Company, the Internet of Things has the potential to create a global economic impact of up to $6.2 trillion annually by 2025, with 50 billion Internet-connected devices by 2020.

There are some truly fascinating examples of the Internet of Things: a bed with smart fabric and sensors that tracks your sleep habits and uses the data to make sure your sleeping environment stays comfortable throughout the night; mobile apps that use roadside sensors to inform drivers of empty parking spots; an auto-

mated sprinkler system that saves money by using real-time weather data to make automatic, water-saving adjustments; a Web-enabled toothbrush that tracks the user's brushing habits to improve oral hygiene. One of my staffers, interestingly enough, actually uses one of these and swears by it.

As exciting as those applications sound, we are only at the beginning of this technology trend, and there is no telling how far it will go. The number of connected things will continue to explode and they will increasingly interact with each other dynamically, seamlessly, and automatically without human intervention.

With significant economic and societal impacts, the Internet of Things also brings complex policy questions. By their nature, IoT devices require Internet connectivity and we will need to be bold in thinking of clever ways to unleash licensed and unlicensed spectrum for the private sector.

IoT devices can collect sensitive consumer and business data. Therefore, privacy considerations should be at the forefront as we consider this great technological wave.

Security will also be a critical concern of the Internet of Things due to the scope and sensitivity of the data collected due to the interconnection of devices and networks.

These issues are real, but I encourage policymakers to resist the urge to jump head first into regulating this dynamic marketplace. Let us tread carefully and thoughtfully before we consider stepping in with a "government knows best" mentality that could halt innovation and growth. Let us treat the Internet of Things with the same light touch that has caused the Internet to be such a great American success story.

We should let consumers and entrepreneurs decide where IoT goes rather than setting it on a Washington, D.C.-directed path. If evidence shows that there are discrete problems, we should examine ways to solve those problems. But let us have the humility to recognize that the best solutions are often not government solutions, and let us not stifle the Internet of Things before we and consumers have a chance to understand its real promise and its implications.

We have a fantastic panel with us today with diverse experience in the IoT marketplace, and I am looking forward to hearing from each of you in a moment.

Right now, I would like to turn to my distinguished Ranking Member, the Senator from Florida, Senator Nelson, for his opening statement.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you to the distinguished Chairman.

And we are going to have a bed that will help us improve our sleep.

The CHAIRMAN. Sounds good.

Senator NELSON. That does sound good.

But as we get into this subject of the Internet of Things, no one is talking about over-regulating. The promise of the Internet of Things must be balanced with real concerns over privacy. If you saw "60 Minutes" last Sunday, the Internet of Everything could

allow everything to be the portals of the Internet and consequently the threat of cybersecurity. Hackers, as shown on "60 Minutes," can access your car and take over the basic functions of driving your car. It was demonstrated there with Lesley Stahl trying to drive the car under controlled conditions, and suddenly the car braked or suddenly the car turned or suddenly the car accelerated.

The Internet of Things can hack into insulin pumps and cause an overdose to occur or take over a pacemaker and cause a heart attack. And it is not the stuff of TV drama. It is the real threats to our Nation's cybersecurity, but also to our physical safety.

Now, I am looking at this through the lens of being the Ranking Member of the Cybersecurity Subcommittee on the Armed Services Committee, where we are getting into this in detail.

We opened over the weekend a cybersecurity center at the University of South Florida in Tampa. And I was shown a device that is called a "Pineapple," which costs about 100 bucks. You can buy it in commercial stores. And what happens is if I walk into a place where I suddenly tap into the WiFi such as a Starbucks, someone with this device can suddenly have me on their wireless instead of the wireless in the particular store or in my apartment. And all of a sudden, I am in their system.

And so interconnected devices collect, amass, transmit personal information. Consumers' personal privacy is obviously at risk; and it is an aspect of the extraordinary things where we can improve our sleep, but we are going to have to watch out for whether or not we have any privacy.

Now, the FTC just settled a case with a company that manufactured household security cameras that, because of their faulty software, allowed anyone online to peep into hundreds of households.

And some companies may transmit the information they collect to third parties without consumer consent. It is one thing for my refrigerator to inform me that I need more milk. It is another for my refrigerator to tell the local grocery store the same thing for marketing purposes.

And more recently we learned that Samsung's privacy policy for its voice-activated Smart TV informed consumers that their indoor conversations can be recorded by the television and sent to third parties.

Did you ever read "Animal Farm" and learn about Big Brother?

Mr. Chairman, I will insert the rest of my opening statement for the record so that we can get on to the witnesses.

But we are at a time of extraordinary challenge. It is a time of great opportunity with what we have, but at the same time, where is our privacy?

Thank you.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Thank you, Chairman Thune, for holding this hearing today.

In just the past couple of weeks, we have been hearing a lot about the proliferation of Internet connected devices.

And the news is not all good.

We have smartphones with web trackers that you can't delete called supercookies.

We have connected devices in cars out there that are potentially collecting all sorts of information about us—without express consent.

And now, we have news reports about televisions that send household recordings in our homes to third parties.

Make no mistake, the advent of the Internet of Things could result in a sea change in the way we interact with our world, how we go about our lives in our homes, and economic growth and jobs.

Home automation and integration could mean limitless conveniences and save consumers thousands of dollars each year.

Wearables and connected healthcare devices could drive down costs and pave the way for a better life for all of us.

Smart electric grids, traffic monitoring systems, and new industrial processes could revolutionize our country and the economy.

No one is debating the promise of the Internet of Things, and no one is talking about "overregulating." This is a red herring. But the promise of the Internet of Things must be balanced with real concerns over privacy and the security of our networks.

As we saw on Sunday night's episode of *60 Minutes,* the Internet of Everything could allow "everything" to be portals to the Internet and, consequently, threats to our cybersecurity.

Hackers can access your car and take over basic functions, such as acceleration and braking control.

They can also hack into insulin pumps and cause an overdose or take over a pacemaker and cause a heart attack.

This is not the stuff of TV drama—these are real threats not only to our Nation's cybersecurity but also to our physical safety.

In fact, this technology is nothing new. For years, the so-called "Pineapple Mark IV" has been able to hack into Wi-Fi networks and wreak havoc on your laptops and smartphones.

Furthermore, as these interconnected devices collect, amass, and transmit personal information, consumers' personal privacy is increasingly at risk.

The FTC just recently settled a case with a company that manufactured household security cameras that, because of faulty software, allowed anyone online to peep into hundreds of households.

Furthermore, some companies may transmit the information they collect to third parties without consumer consent.

It's one thing for my refrigerator to inform me that I need more milk; it's another for my refrigerator to tell that to the local grocery store for marketing purposes.

And, more recently, we learned that Samsung's privacy policy for its voice-activated "Smart TV" informed consumers that their indoor conversations can be recorded by the television and sent to a third party.

So, Big Brother may really be listening to us.

The FTC just released a report on this very topic, making some wise recommendations—for best practices—for companies as they design, sell, and service their connected devices.

I hope it's the start of real conversation and cooperation between the FTC and industry to make sure the promises of the Internet of Things don't fall victim to a lack of foresight and protections for consumers.

Finally, another important aspect in looking toward the future of the Internet of Things is the platform on which the majority of these new devices connect—wireless spectrum.

Spectrum is the lifeblood of these devices, as well as for so much other innovation in the U.S. economy. We must engage in a careful consideration to balance competing needs for this finite, yet critical public resource.

I want to thank the witnesses for appearing before the Committee, and I look forward to hearing your testimony.

The CHAIRMAN. Thank you, Senator Nelson.

And we are going to turn to our distinguished panel to answer all the questions that you have just raised. Hopefully, they will help us figure out how we get all the up-side benefit, opportunity and potential that comes with this great technology but also the risks which very clearly exist and to which you alluded.

We will start with Mr. Michael Abbott. Mr. Abbott is a General Partner at Kleiner Perkins Caufield & Byers.

Mr. Douglas Davis. Mr. Davis is the Vice President and General Manager for the Internet of Things Group for the Intel Corporation.

Mr. Lance Donny. Mr. Donny is the Chief Executive Officer for OnFarm Systems.

Mr. Adam Thierer. Mr. Thierer is the Senior Research Fellow for the Mercatus Institute at George Mason University.

And Mr. Justin Brookman. Mr. Brookman is the Director for the Consumer Privacy Project at the Center for Democracy & Technology.

So we are delighted that you have all made time to be with us today and look forward to hearing from you.

We will start at my left and your right Mr. Abbott, and if you could confine your remarks as close to 5 minutes as possible, we would certainly appreciate that. Mr. Abbott?

STATEMENT OF MICHAEL ABBOTT, GENERAL PARTNER, KLEINER PERKINS CAUFIELD & BYERS

Mr. ABBOTT. Chairman Thune, Ranking Member Nelson, and distinguished members of the Senate Commerce Committee, I appreciate the opportunity to testify before you today on the exciting and important topic of our connected world and the dynamic role of the Internet of Things.

I would also like to thank Senators Fischer, Booker, Ayotte, and Schatz for your interest in this topic and for requesting this hearing.

I am here today in my capacity as a General Partner at the Silicon Valley-based venture capital firm, Kleiner Perkins Caufield & Byers. Our firm, Kleiner Perkins, has more than 40 years of experience helping entrepreneurs deliver world-changing ideas to market. Through our consumer digital and enterprise digital initiatives alone, we have invested in and are mentoring more than 30 entrepreneurial companies with over $300 million in investments in the IoT space today. I am by background an engineer, an entrepreneur, an investor, and a serial optimist about the power of technology and innovation to help improve our lives.

Today I will focus my testimony on three key areas.

One, the Internet of Things is a robust and vibrant ecosystem in both the consumer and enterprise space, with new platforms and applications coming online every day and strong venture capital investments to help grow it.

Two, the rapid growth in both data and devices leads to a next wave of innovation focused on efficiencies and smart systems using the cornerstones of successful IoT smart hardware, software, and cloud integration.

Third, IoT, or the Third Wave of the Internet as analysts like to call it, is nascent but very competitive. Consumer confidence is paramount, but we must not over-regulate and stifle innovation.

As we look back on investments in the verticals we called "bits," "bytes," "bugs," and "drugs," we now see the rise of the Internet of Things, a connected world that allows us to jump from old platforms of the last decade into a new world in which we can manage every aspect of our lives, from our health to our finances, to our home, all with the swipe of a finger on a smart phone. And the

market is responding. Overall venture investments, $48 billion, in 2014 reached their highest levels since 2000, and the 2014 IPO market was strong both domestically and globally. Overall, IoT investment is harder to immediately qualify since it crosses over so many sectors.

So what do we mean by the IoT?

IoT enables the collection of an unprecedented quantity and quality of data through sensors and devices. According to an often-cited Cisco report, there will be more than 50 billion connected devices by 2020, approximately 2x growth every 5 years. And as the recent EMC Digital Universe and market research company IDC report noted, data is doubling in size every 2 years and expected to reach 44 zettabytes by 2020. That is 44 trillion gigabytes. To put that in perspective, we were at 4.4 zettabytes, just over a tenth of that, in 2013.

So how will we deal with our data obesity problem? What are the smart solutions for managing all of this data in a way that improves, rather than complicates our lives? With many platforms to spur technological advances from the home, to the body, to the car, to the factory, to the farm, we must innovate our way into a smarter connected future. At Kleiner Perkins, we are looking across platforms and enterprises at disrupters and at incumbents, and at the entire IoT ecosystem to use connectivity to transform how we work, play, and care for our families and ourselves.

If great hardware and software are the cornerstones of a robust IoT ecosystem, it is the third element, hardware, software, and cloud services, that will show major advances and create smarter systems. With all these new devices, the stream of data will continue to accelerate. Successful systems must provide data-driven intelligence at both the endpoint devices and through machine learning in the cloud. In order for IoT to grow in meaningful ways to keep both the consumer and the enterprise users engaged, we must have a more intelligent way to manage and rank-order data with real-time usage feedback on what needs a fix or an upgrade. Recent advances in deep learning, the use of algorithms in machine learning for modeling abstractions in data, combined with these streams of real-time sensor data, will present enormous opportunities for innovation on which we are focused.

My testimony today is based primarily on my experience as an engineer and investor. I am not an expert in public policy. There is so much promise in this space, but we are in the early days. Consumer confidence is paramount to growth and innovation in the IoT space and reasonable security and best practices should help bolster that confidence.

The FTC has thoughtfully presented ideas, benefits, and risks in its Internet of Things Privacy & Security in a Connected World report. Congress, as evidenced by today's hearing, is also looking at the intersection of technology and public policy.

However, I would ask that regulators and legislators proceed with caution when considering over-regulation in this space to prevent stifling innovation. As is common in nascent markets, interoperability in IoT is now a challenge, and over time, standards will emerge from the winners in the market. We are at a critical comment in this industry in which innovators and entrepreneurs are

competing with some of the biggest and most historically successful enterprises in the country. And that is healthy. This competition is creating consumer choice in the marketplace, delivering to consumers much better products and services at a lower cost.

An insightful colleague of mine once said that we will all know we have succeeded when we no longer use the term "Internet of Things," just as we no longer say that we downloaded MP3's. As we have found with our music and phones, innovators are turning the scientific and technical breakthroughs of our time into products that benefit everyone, changing the way we live and giving us new opportunities to connect with and relate to one another and achieve our goals. Soon, my bet is that these technologies will likewise become unobtrusive, another chapter in how entrepreneurs and their innovations can help improve the quality of life for new generations in this country and around the world.

I would like to thank the Committee for the opportunity to testify today, and I look forward to answering any questions.

[The prepared statement of Mr. Abbott follows:]

PREPARED STATEMENT OF MICHAEL ABBOTT, GENERAL PARTNER, KLEINER PERKINS CAUFIELD & BYERS

Chairman Thune, Ranking Member Nelson, and distinguished members of the Senate Commerce Committee, I appreciate the opportunity to testify before you today on the exciting and important topic of our connected world and the dynamic role of the Internet of Things ("IoT"). I would also like to thank Senators Fischer, Booker, Ayotte and Schatz for your interest in this topic and for requesting this hearing.

I am here today in my capacity as a general partner at the Silicon Valley-based venture capital firm, Kleiner Perkins Caufield & Byers. Our firm, Kleiner Perkins has more than 40 years of experience helping entrepreneurs deliver world-changing ideas to market. Through our Consumer Digital and Enterprise Digital initiatives alone, we have invested in and are mentoring more than 30 entrepreneurial companies with over $300 million in investments in the IoT space. I am by background an engineer, an entrepreneur, an investor, and a serial optimist about the power of technology and innovation to help improve our lives.

Today I will focus my testimony on 3 key areas:

1. The Internet of Things is a robust and vibrant ecosystem—in both the consumer and enterprise space—with new platforms and applications coming online every day and strong venture capital investments to help grow it.
2. The rapid growth in both data and devices leads to a next wave of innovation focused on efficiencies and smart systems using the cornerstones of successful IoT: smart hardware, software and cloud integration.
3. IoT—or "the Third Wave of the Internet" as analysts like to call it, is nascent but very competitive. Consumer confidence is paramount, but we must not over-regulate and stifle innovation.

As we look back on investments in the verticals we called "Bits, Bytes, Bugs, and Drugs," we now see the rise of the Internet of Things: a connected world that allows us to jump from old platforms of the last decade into a new world in which we can manage every aspect of our lives, from our health to our finances to our home, all with the swipe of a finger on a smartphone. And the market is responding. Overall venture investments ($48 billion) in 2014 reached their highest levels since 2000[1] and the 2014 IPO market was strong, both domestically and globally. Overall IoT investment is harder to immediately qualify since it crosses over so many sectors. So what do we mean by the IoT?

It is my understanding that the primary focus of this hearing is the consumer side of the IoT. But it's worth mentioning that there are many other applications for IoT

[1] NVCA, "MoneyTree™ Report by PricewaterhouseCoopers LLP (PwC) and the National Venture Capital Association (NVCA), based on data from Thomson Reuters," January 16th, 2015. *http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report/*

including business-to-business and machine-to-machine—applications that will only expand. As such, I tend to categorize IoT in two ways:

- First is the consumer market, what I call "The Internet of Me," because it enables people to use connectivity to enrich their lives and the lives of their family and friends.
- Second is "The Internet of IT," consisting of large data generation for enterprises to make smarter systems for everything from precision agriculture to efficiencies in large-scale manufacturing.

IoT enables the collection of an unprecedented quantity and quality of data through sensors and devices. According to an often-cited Cisco report, there will be more than 50 billion connected devices by 2020[2]—approximately 2x growth every 5 years. And as the recent EMC Digital Universe and market research company IDC report noted, data is doubling in size every two years and expected to reach 44 zettabytes by 2020[3]—that's 44 trillion gigabytes. To put that in perspective, we were at 4.4 zettabytes, just over a tenth of that, in 2013.

So how will we deal with our data obesity problem? What are the smart solutions for managing all of this data in a way that improves, rather than complicates, our lives? With many platforms to spur technological advances from the home to the body to the car to the factory to the farm, we must innovate our way into a smarter, connected future. At Kleiner Perkins, we are looking across platforms and enterprises, at disrupters and at incumbents, and at the entire IoT ecosystem to use connectivity to transform how we work, play, and care for our families and ourselves.

We have two critical issues on this front. The first is power management of the devices themselves, and the second is data management, including machine learning. With a growing number of power hungry devices, our firm is looking at innovators working in the Low Power Everywhere space—devices getting lighter, smaller and more efficient. We're also looking at low power processors and energy scavengers that search for energy sources without batteries. There are promising advancements in this space such as the work being done by Ambiq Micro in subthreshold circuits to improve efficiency in sensors and devices.

As investors, we do extensive analysis before investing in a company. But when you are at the disruptive edge of a new technological revolution, it's hard to fully predict how consumers will react. In order for a technological revolution to take root, you must invest early and work with the company to produce some wins.

A great example of this is our investment in Nest. When we started, we couldn't know for sure that Nest would be an attractive device to consumers. But now, with great technology and smart marketing, it's influencing the development of the smart home. This is because the Nest team got two of the most critical IoT elements right: intuitively designed and aesthetically pleasing hardware, and smart software. Together, these produce a seamless and enjoyable user experience, enabling the customer to easily, and remotely as needed, adjust the temperature in one's home and save on heating and cooling costs.

It's the possibility of more stories like Nest that led Kleiner Perkins to partner with Google Ventures to start the Thoughtful Things Fund. The Thoughtful Things Fund is an initiative to back the ideas and companies that can expand what the conscious home™ can do. Consumers see immediate benefits from a connected home, whereas the cycle for enterprise systems may take a longer period of time. But the seeds of change for both consumers and enterprises are there, and we've already had thousands of submissions from all over the world.

If great hardware and software are the cornerstones of a robust IoT ecosystem, it is the third element—hardware + software + cloud services that will show major advances and create smarter systems. With all of these new devices, the stream of data will continue to accelerate. Successful systems must provide data-driven intelligence at both the endpoint devices and through machine learning in the cloud. In order for IoT to grow in meaningful ways to keep both consumer and enterprise users engaged, we must have a more intelligent way to manage and rank order data, with real-time usage feedback on what needs a fix or an upgrade. Recent advances in "deep learning"—the use of algorithms in machine learning for modeling

---

[2] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), April 2011. *http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf*

[3] EMC Digital Universe & IDC, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," April 2014. *http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm*

abstractions in data—combined with these streams of real-time sensor data, will present enormous opportunities for innovation on which we are focused.

My testimony today is based primarily on my experience as an engineer and investor. I am not an expert in public policy. There is so much promise in this space, but we are in the early days. Consumer confidence is paramount to growth and innovation in the IoT space and reasonable security and best practices should help bolster that confidence.

The FTC has thoughtfully presented ideas, benefits and risks in its Internet of Things: Privacy & Security in a Connected World report. Congress, as evidenced by today's hearing, is also looking at the intersection of technology and public policy. However, I would ask that regulators and legislators proceed with caution when considering over-regulation in this space to prevent stifling innovation. As is common in nascent markets, interoperability in IoT is now a challenge and, over time, standards will emerge from the winners in the market. We are at a critical moment in this industry, in which innovators and entrepreneurs are competing with some of the biggest and most historically successful enterprises in the country—and that is healthy. This competition is creating consumer choice in the marketplace, delivering to consumers much better products and services at a lower cost.

An insightful colleague of mine once said that we'll know that we've succeeded when we no longer use the term the "Internet of Things"—just as we no longer say that we "download MP3s." As we've found with our music and phones, innovators are turning the scientific and technical breakthroughs of our time into products that benefit everyone, changing the way we live and giving us new opportunities to connect with and relate to one another and achieve our goals. Soon, my bet is that these technologies will likewise become unobtrusive, another chapter in how entrepreneurs and their innovations can help improve the quality of life for new generations, in this country and around the world.

I would like to thank the Committee for the opportunity to testify today. I look forward to answering any questions.

The CHAIRMAN. Thank you, Mr. Abbott.

Mr. Davis?

STATEMENT OF DOUGLAS DAVIS, VICE PRESIDENT AND GENERAL MANAGER, INTERNET OF THINGS GROUP, INTEL

Mr. DAVIS. Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. Thank you for the opportunity to provide testimony on the importance of the United States establishing a global leadership role in the Internet of Things.

As head of Intel's IoT Group, I own the company's overall strategy in this space. Intel's 30 years of investment, innovation, and standards leadership in the evolution of computing provide the foundational elements of that strategy. Intel believes the Internet of Things represents a transformational opportunity for the U.S. and the world. It will enable innovation, increase productivity, and deliver efficiencies across both public and private sectors.

Now, while some think the Internet of Things is smart thermostats and wearables, these consumer devices are just a few of the many applications. The primary economic driver will be non-consumer areas such as industrial and commercial applications.

I will address three topics that are important to consider as you chart your policy.

One, why is the IoT important?

Two, what are the potential barriers to successful IoT ecosystems?

And how can policymakers accelerate deployments to ensure U.S. leadership?

So first, why is the Internet of Things important? It will drive unprecedented benefits for the Government, businesses, consumers, and communities. As Mr. Abbott pointed out, the growth in the

number of devices and the amount of data that they are generating will increase at dramatic levels by the end of the decade. The IoT presents the opportunity to connect these devices, efficiently analyze the data, and use the information to improve decisionmaking. And in doing so, the IoT is expected to have a multi-trillion dollar global impact, as we have noted.

What should most excite U.S. policymakers is that America and other developed economies are expected to capture 70 percent of this impact if we lead.

Let us consider one IoT application. SAIA Trucking, located in Georgia, has a nationwide fleet of about 3,000 trucks. They recently deployed an Intel-based IoT solution which alters routes and guides driver performance real-time. SAIA increased fuel efficiency by 6 percent, translating into $15 million in annual savings.

The U.S. trucking industry consumes 54 billion gallons of fuel per year. Extrapolating SAIA's success, our Nation could save over 3 billion gallons of fuel yearly while reducing CO_2 emissions.

Second, what are the potential barriers to a successful IoT ecosystem? One barrier could be security if not implemented at the outset. For this reason, Intel prioritizes security as the foundation of our IoT solutions. We will integrate security at the outset, building cryptography into our chips to enable strong identity and data protection. In addition to the compute device itself, our solutions will employ advanced software security to prevent harmful applications from being activated on the device or taking down the network. Integrating multiple layers of security at the outset enables trusted data transmission necessary for successful IoT implementations.

Other potential barriers include connecting to legacy infrastructure, interoperability amongst devices, and developing global standards. To address these barriers, Intel collaborated with industry leaders to define five tenets for successful IoT solutions. They are security, ease of connectivity, interoperability, data analytics, and ease of deploying new applications and services. Based on these tenets, we recently launched the Intel IoT Platform.

Finally, how can policymakers accelerate IoT deployments to ensure U.S. leadership? Well, candidly, the U.S. is behind. Other countries are aggressively investing in and deploying IoT implementations to transform their economies, address societal problems, and spur innovation. China, Brazil, the United Arab Emirates have all adopted national IoT plans with time-bound goals and are investing heavily in IoT R&D and infrastructure. The U.S. must leverage our vast resources and capabilities. Promoting industry alignment around these large-scale IoT deployments based on secure, open, and interoperable solutions will showcase U.S. leadership.

Congress can advance our Nation's IoT momentum by collaborating with industry to establish a national IoT strategy, encouraging public-private partnerships, and investing in IoT research.

Intel is confident that the U.S. can lead the IoT transformation with a continued open dialogue, as you are doing here today, and by implementing these recommendations.

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

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF INTEL CORPORATION

Intel Corporation ("Intel") respectfully submits this statement for the record in conjunction with the Senate Commerce, Science & Transportation Committee's hearing on "The Connected World: Examining the Internet of Things." Our statement focuses on the opportunity to unleash the vast potential of the Internet of Things (IoT) through public-private partnerships and to create a leadership opportunity for the U.S. in this multi-industry transformation.

Witness: Doug Davis is the vice president and general manager of Intel's worldwide IoT Group (IOTG). Doug has been an Intel employee for 31 years, and began his career as a product engineer in the company's Military and Special Products Division. Over the last decade, Doug has run Intel's worldwide Embedded and Communications Group, managed wafer factory operations, and now leads the IoT Group. This organization is responsible for the company's IoT strategy and solutions—consisting of hardware, software, security and services across a wide range of market segments, including transportation, manufacturing, healthcare, retail, smart home, smart buildings and smart cities. For the past 30 years, Intel has made significant investments, driven exciting innovations, led standards activities, and supported what has evolved to become the Internet of Things. At Intel, we like to say IoT is an overnight transformation thirty years in the making.

Intel and the Internet of Things

Intel's Role

The evolution of IoT goes back more than 30 years with Intel as a leader from the start. In 1972, Intel introduced the Intel 4004, the world's first commercially available microprocessor—an invention foundational to the "computer revolution." In the late 1970s, came the Intel 8048, the world's first commercially available microcontroller, which integrated memory, peripherals and the microcontroller on a single chip. These microcontrollers fueled new business opportunities in a variety of markets. In 1981, IBM launched the IBM 5150, igniting the rapid-paced growth of the "personal" computer (PC) market segment. This first IBM PC ran on an Intel 8088 microprocessor and used Microsoft's MS–DOS operating system.

Initially, microprocessors were used for personal computing, leaving microcontrollers for 'use specific or 'embedded' applications like factory controls. A critical shift occurred in the mid-1990s as customers began using Intel microprocessors in embedded market segments, bringing the power of computing to what had traditionally been based on microcontrollers. Intel began a concerted effort to support the unique attributes of embedded market segments including manufacturing life-cycle support for 7–10 years, extended operating temperatures, and utilization of real-time operating systems.

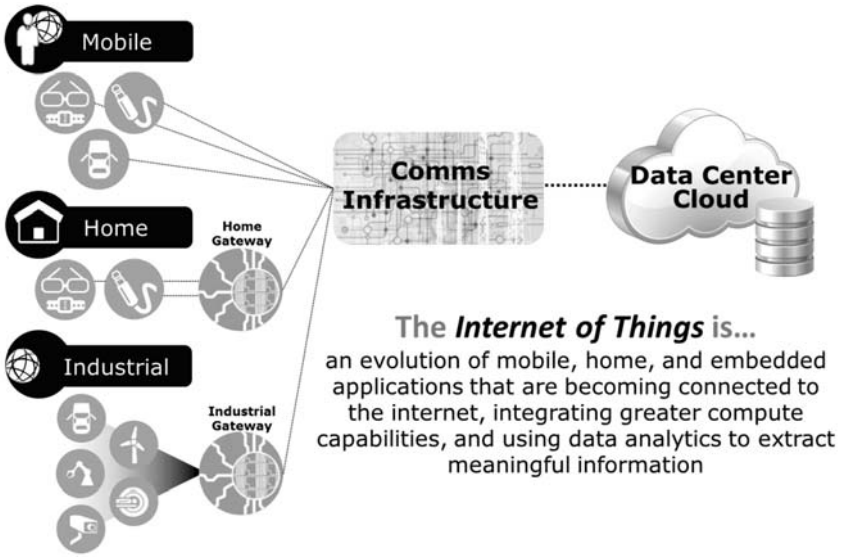
The early 2000s saw an unprecedented uptake in Internet usage, as the PC and mobile markets exploded. This "connectivity" trend wasn't limited to connecting people; embedded systems were simultaneously taking advantage of this powerful capability. Over the course of just a few years, industries worldwide were profiting from the scaling benefits of computing and networking and consumers were enjoying the benefits of connected PCs.

In the late 2000s, "Machine to Machine" (M2M) emerged. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. Before M2M, people had to be physically located at the machine to analyze the data to make decisions for managing each machine. With the introduction of M2M, machines could now be managed remotely. All of these innovations within the datacenter, cloud computing, wireless communications and M2M formed the basis of what is now widely known as the IoT.

Moore's Law, the business model that drives the semiconductor industry, states that the number of transistors in an integrated circuit doubles approximately every two years. In essence, the marketplace experiences a doubling of the computing capability at approximately the same price every other year. The observation is named after Intel co-founder Gordon E. Moore. This explosion of networked devices also began to represent another "law" of scaling called Metcalfe's Law. Metcalfe's Law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). This enables the Network Effect, whereby the value of a product or service is dependent on the number of others using it. Together, Moore's Law and Metcalfe's Law demonstrate how the power of intelligent, connected devices like connected digital signs, cars and homes can unleash innovation, leading to the creation of platforms for new applications and services.

IoT Definition

IoT is defined as endpoint devices such as cars, machinery or household appliances that connect to the Internet and generate data that can be analyzed to extract valuable information. There are three sub-definitions emerging out of the IoT space, however, all three definitions overlap. The "Mobile IoT" comprises devices like cars, wearables, sensors and mobile phones which all connect directly through broadband wireless networks. The "Industrial IoT" connects devices in industrial environments like factory equipment, security cameras, medical devices, and digital signs. These devices are able to connect to the Internet and into the datacenter (cloud) through an industrial "gateway."[1] Finally, the "Home IoT" connects devices like game consoles, smart TVs, home security systems, household appliances and thermostats through at gateway to the internet.



The Five Critical Tenets of IoT

In September 2014, Intel and key global partners collaboratively identified five critical IoT tenets which describe how endpoint devices should connect to the cloud. Here are the five key tenets, as illustrated in the graphic below:

First, *Security as the Foundation:* With billions of internet-connected devices by 2020, it is important that IoT is secure from the sensor to the cloud, including all hardware and software. Second, *Connectivity, Device Discovery, and Provisioning:* Billions of devices cannot be managed manually. Rather, devices need to be able to communicate their "status" to the rest of the system independently. Third, *Data Normalization:* With so many different data types, there must be some level of interoperability between devices such that they are speaking the same language. Fourth, *Actionable Analytics:* The data must be turned into meaningful information through analytics. Fifth, *Monetize Hardware, Software, and Data Management:* The IoT infrastructure must be built to allow developers to manage and monetize innovative applications and services.

[1] A gateway is a node on a network that serves as an entrance to another network.

With these tenets in mind, in December of 2014, Intel launched the Intel® IoT Platform,[2] which unifies security and connectivity to enable scalable IoT deployments. The Platform provides a secure device-to-cloud (end-to-end) open reference model for connecting devices to deliver trusted data to the cloud and value through analytics. The Platform enables tenets 1–3—security, connectivity, and interoperability—by creating a foundation on which to build IoT solutions. This enables tenets 4 and 5—data analytics and monetization of new products and services, many of which we never could have imagined a decade ago and may not even conceive of today.

IoT: A Transformational Opportunity Built on a Foundation of Security

With respect to the critical element of security, Intel values this first and foremost. We believe that security is the foundation of IOT and it is fundamental to Intel's roadmap planning. We have dedicated security products and security features embedded into both our hardware and software products. Our hardware and software are being designed from the beginning to be secure. This is important for trusted data exchange in the IoT, as data generated by devices and existing infrastructure must be able to be shared among the cloud, the network, and intelligent devices for analysis. This enables users to aggregate, filter and share data from the edge of the network all the way to the cloud with robust protection. Moreover, data must be accurate to be beneficial. Intel prioritizes the security, accuracy, privacy and integrity of data in all market sectors, and especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. Intel understands that we must deliver and evoke consumer and industry trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

Intel believes it is critical to integrate security into the hardware *and* the software, from the smallest microcontroller (MCU) at the edge of the network to the most advanced server CPU in the data center (cloud) and all gateways and devices in between. These hardware-and software-level security capabilities will create redundancies which prevent intrusions and enable a robust, secure, trusted IoT end-to-end solution.

Hardware. Intel's hardware will provide transistor-level security *on the actual compute device itself.* By integrating security into the device itself from the outset (rather than layering it on top at a latter point in the design cycle with other, less secure external features), Intel's IoT solutions will enable our customers to know the exact unique identity of every device on their network. This technology also has the capability for encrypting that unique identity to provide anonymity properties in addition to hardware enforced integrity. Because each compute device can have an immutable identification to enable secure provisioning, a non-approved device will not be allowed to access the network. The MCU or CPU itself will provide the "baked

[2] *Intel Unifies and Simplifies Connectivity, Security for IoT,* Intel Corp. (Dec. 2014), *http://newsroom.intel.com/community/intel_newsroom/blog/2014/12/09/intel-unifies-and-simplifies-connectivity-security-for-IoT.*

in" (irremovable, non-changeable) identity of the device, making the level of security significantly more robust.

On top of this immutable device identification, Intel's IoT solutions will employ advanced hardware level security capabilities such as "whitelisting," which prevents harmful applications like viruses, control agents, and malware from ever being activated on the device. What this means is that, if the CPU ever "sees" an application that is not on its known good list ("whitelist") try to run on the device, it will automatically lock out that device and not allow it turn on. At other layers in IoT solutions, Intel also uses another advanced hardware security capability called "blacklisting," which blocks a defined list of known malware from entering the device and the network.

Software. In addition to the advanced hardware security capabilities in Intel's IoT solutions, Intel Security (formerly McAfee) integrates advanced security capabilities that provide robust software-level protection. This means that the software is continually monitoring the activity of its networked devices-and looking for any abnormalities or possible threats. If the monitoring software identifies a threat, it proactively notifies users and/or automatically quarantines any devices on the network that could be at risk.

By employing this combination of transistor-level security, along with advanced hardware and software level security, from devices on the edge of the network all the way to the data centers in the cloud, Intel will protect IoT assets and information in ways few others can. Intel knows that security is critical to protect the integrity of IoT solutions, so we will design it in from the outset.

IoT Priorities—Enablers of Scale

Security

As discussed above, security is foundational to the IoT ecosystem and a top Intel priority. With billions of connected devices producing enormous amounts of data –EMC/IDC forecasts that devices will generate more than 44 zeta bytes of data by 2020[3]—security of this data will be critical to enable scale of IoT deployments. That is why we emphasize again the importance of having security designed into the IoT systems from the outset. Secure data delivery systems are critical to enabling trusted data exchange and scale, thereby unlocking the full potential of IoT.

Interoperability

The IoT marketplace is currently aligning around industry sectors/verticals that are starting to deploy IoT solutions to meet their specific business requirements: manufacturing, retail, transportation, healthcare, and others. As early adopters deploy technologies to enable IoT solutions, it is important that the various IoT technologies are "interoperable" with each other as well as being able to adapt and grow to accommodate new and changing business requirements. Proprietary technologies that are inherently antithetical to the concept of the Internet of *All* Things will slow down IoT adoption, limit scalability and delay economic benefits.

The Intel IoT Platform's building block components are secure, interoperable, and scalable, enabling "horizontal" end-to-end IoT deployments across industry sectors from transportation to energy to healthcare and beyond. By creating a secure, horizontal, interoperable platform, Intel will enable IoT to scale quickly by creating a repeatable (reusable) foundation that ultimately enables choice and interoperability in the marketplace. For example, Intel offers businesses that use the Intel IoT Platform the choice and flexibility to use some or all of the technology components from Intel, or interchange them with ecosystem partner components. In summary, if the U.S. wants to lead in IoT, we must prioritize interoperability from the start.

Open Standards

How do we drive a secure solution that is interoperable and scales across a global IoT ecosystem? The solution is a voluntary, global, industry-led, open set of standards which enable scale to drive cost-effective solutions. Over the last 10 months, Intel co-founded two industry consortia focused on interoperability and open standards: The Industrial Interconnect Consortium (IIC)[4] and the Open Internet Consortium (OIC).[5]

IIC founding members include major U.S. companies such as AT&T, Cisco, GE, IBM and Intel. The IIC has reached over 135 members since its inception in March

[3] *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things,* EMC/IDC (April 2014), *http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm* .

[4] *http://www.industrialinternetconsortium.org/*

[5] *http://openinterconnect.org/*

2014. IIC goals are to: (i) build confidence around new and innovative approaches to security; (ii) drive innovation through the creation of new industry use cases and test beds for real-world applications; (iii) define and develop the reference architecture and frameworks necessary for interoperability; (iv) influence the global development standards process for Internet and industrial systems; and (v) facilitate open forums to share and exchange real-world ideas, practices, lessons and insights.

The OIC was founded by leading technology companies with the goal of defining the connectivity requirements for devices, and for ensuring interoperability between the millions of devices that will make up the emerging IoT. OIC founding members include Cisco, GE, Intel, MediaTek and Samsung, and membership has reached over 54 members. OIC goals are to: (i) define the specification, certification and branding to deliver reliable interoperability; (ii) ensure this standard will be an open specification that anyone can implement and is easy for developers to use; (iii) include IP protection and branding for certified devices and service-level interoperability; (iv) provide an open source implementation of the standard; and (v) ensure this open source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

Both IIC and OIC recognize that a certain level of standardization and interoperability is necessary to achieve a successful IoT ecosystem. In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Furthermore, open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path. Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, and Intel is taking a leading role.

Market Trends Driving the Emergence of IoT

If we've had broad use of the Internet for over two decades why is the IOT industry emerging now? Intel believes there are three emerging trends are driving the inflection:

Ease of connectivity—Whether it is an unlicensed (WiFi, Bluetooth) or licensed (3G, LTE, 5G) spectrum, connectivity is becoming more pervasive and inexpensive. The opportunity to add value via increased connectivity is extremely large, as 85 percent of devices are not connected today.

Compute economics—Moore's Law is impacting technologies that range from the cloud to the network to storage to sensors. This means that the economics for "compute" have become much more appealing. Specifically, there has been a huge drop in cost for "compute" technologies over the last 10 years; the cost of sensors has decreased 2X, the cost of bandwidth has decreased 40X, and the cost of processing has decreased 60X.

Big Data and Analytics—The emergence of data science (extracting knowledge from data) combined with the reduction in the cost of high performance computing has created an opportunity to turn data into actionable information, thereby enabling new services and new business model innovation.

These three market trends are generating unprecedented opportunities for the U.S. public and private sectors to develop new services, enhance productivity and efficiency, improve real-time decision making, solve critical societal problems, and develop new and innovative user experiences. All of these opportunities are revolutionizing sectors like smart buildings, transportation, healthcare, and manufacturing. Here are just a few examples of quantitative results already enabled by IoT:

Smart Buildings: The integration of Intel IoT technology with sensors and building automation systems, such as heating and air conditioning, allows for the identification of opportunities in real-time to reduce energy costs. In conjunction with Intel and Cisco, Rudin Management, a large, commercial real estate company in New York City, deployed Intel's Smart Building IoT solution, which saved Rudin $1 million in just one building in the first year of deployment. Consider the U.S. potential opportunity: There are over 5 million commercial buildings and industrial facilities in the U.S.,[6] with a combined annual energy cost of more than $202 billion.[7]

[6] *Commercial Buildings Energy Consumption Survey (CBECS),* US Energy Information Administration (5.6 million commercial buildings in U.S. in 2012), *http://www.eia.gov/consumption/commercial/reports/2012/preliminary/index.cfm?src=%E2%80%B9%20Consumption%20%20%20Commercial%20Buildings%20Energy%20Consumption%20Survey%20(CBECS)-b1.*

[7] *http://thesemco.com/about-us/why-energy-efficiency/*

It is estimated that the U.S. could save $20 billion if all commercial buildings and industrial buildings increased their energy efficiency by just 10 percent.[8]

Smart Transportation: The integration of Intel IoT technology with New York-based Vnomics fleet management solutions enabled real-time monitoring and feedback to Georgia-based SAIA Trucking drivers and headquarters. The goal was to reduce maintenance costs and improve driver safety by monitoring braking in real-time. In the first year, SAIA increased fuel efficiency by 6 percent across a fleet of 3,000 trucks, achieving a savings of $15 million. Consider the U.S. potential opportunity: The U.S. trucking industry accounts for about 13 percent of all fuel purchases in the U.S. and trucks consume about 54 billion gallons/year for business purpose.[9] Extrapolating SAIA's success, a 6 percent improvement in fuel efficiency across all trucks in the U.S. would save more than 3 billion gallons of fuel each year, as well as help reduce CO_2 emissions.

Smart Healthcare: Intel has partnered with the Michael J. Fox Foundation to research the use of big data analytics to help improve the treatment of Parkinson's disease. Our IoT personal healthcare solution enables 300 observations per second per patient, thereby monitoring patients' symptoms and drug effectiveness in real-time. This real-time data collection and analysis allows for the identification of the first signs of disease progression and enables physicians to instantly address changes. Patients can receive better, personalized care, and physicians can make improved decisions for treatment in the event that the patient does not notice slight changes that could cause a decline in health before their next regularly-scheduled appointment. Consider the U.S. potential opportunity: Imagine what real-time monitoring of Parkinson's patients' vitals, as well as the ability to make drug and treatment adjustments in real-time, in addition to better tracking and predictability of disease progression could do to improve the quality of life of Parkinson's patients not only in the U.S., but the world.

Smart Cities: Intel has partnered with the City of San José, California in a public-private partnership to further the city's 'Green Vision' goals. This Smart Cities Project, announced as part of the Smart America Challenge in 2014,[10] is expected to help drive San José's economic growth, foster 25,000 clean-tech jobs, create environmental sustainability and enhance the quality of life for residents. Together, Intel and San José City Management are deploying a network of sensors to create a "sustainability lens" that uses Intel IoT technology to measure characteristics such as particulates in the air, noise pollution and traffic flow. This real-time city data will produce meaningful insights that enable the City to make better management decisions, and lead to improvements in air quality, transportation efficiency, environmental sustainability, health, and energy efficiency. Consider the U.S. potential opportunity: The ten largest U.S. cities alone have an aggregated population of 25,292,500 people.[11] What if we initially focused on 10 cities, 10 counties, and 10 rural towns from across the Nation and implemented IoT "smart city" solutions into those communities?

IoT: Extraordinary Positive Impact on U.S. GDP

The IoT presents staggering economic opportunities for the U.S. and the world. Market research firm IDC estimates that there will be 50 billion connected devices in the marketplace by 2020,[12] and Morgan Stanley forecasts 75 billion in that same time period.[13] These estimates would equate to 6 to 10 connected devices for every person on earth. Whether the exact number of devices is 50 billion or 75 billion or something more, one thing is for certain: The number of connected devices will explode in the next five years. In just the automotive industry alone, it is projected that 250 million (or one in five) cars worldwide will be connected to the Internet by 2020—via technologies like WiFi, LTE, Bluetooth, satellite, and 5G communica-

---

[8] *Id.*

[9] *http://www.truckinfo.net/trucking/stats.htm*

[10] *Intel Helps San Jose Become America's First Smart City: http://www.psfk.com/2014/06/san-jose-intel-smart-city.html*

[11] United States Census Bureau: U.S. and World Population Clock *http://www.census.gov/popclock/*

[12] *Business Strategy: The Coming of Age of the "Internet of Things" in Government,* IDC (April 2013), *http://www.idc.com/getdoc.jsp?containerId=GIGM01V.*

[13] *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, Business Insider* (Oct.2 2013) *http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020–2013–10.*

tions networks.[14] For perspective, 250 million is roughly the same number of total cars on U.S. roads in 2013.[15]

The reason that policymakers should be excited about this explosion of devices and this technological revolution is the staggering positive impact that the IoT is projected to have on the U.S. and global economy. McKinsey projects that IoT will have an incredible $2.7 trillion to $6.2 trillion global economic impact by 2025.[16] And what should most excite U.S. policymakers is that the U.S. and other developed economies are expected to capture a remarkable 70 percent of this economic impact, if we develop a leadership position.[17] In fact, GE estimates that IoT could boost average incomes in the U.S. by an exceptional 25 to 40 percent over the next twenty years.[18]

Moreover, a recent Accenture survey of CEOs reveals that 87 percent of CEOs expect long-term job growth from IoT.[19] This will positively impact American lives from our Nation's farms and factories to markets and Main Street. Indeed, "as the world struggles to emerge from a phase of weak productivity growth, fragile employment and pockets of inadequate demand, the [IoT] offers a chance to redefine many sectors and accelerate economic and employment growth."[20] The U.S. must lead in this technological revolution.

Recommendations for Policymakers

Given the predicted enormous positive impact on the U.S. economy and society, how can policymakers help accelerate IoT and ensure the U.S. leads this next evolution of computing?

1. *Continue an open dialogue with industry, experts and stakeholders as you are doing today.* This IoT hearing is a promising start and the right first step. Intel believes that an open, multi-stakeholder process can best enable a secure and vibrant IoT ecosystem. Also, legislators may want to consider encouraging the Department of Commerce to create a non-partisan National IoT Advisory Board of policymakers, agency representatives, industry leaders, think tanks, academia, and leaders of IoT-focused consortia like IIC and OIC.
2. *Encourage focus on security and interoperability as critical foundational elements of IoT.* While industry is in the best position to develop and determine security and interoperability solutions, government can encourage industry alignment around large-scale IoT deployments based on secure, open and interoperable IoT solutions. This will enable deployments to scale quickly and provide both short-term and long-term economic and social benefits to consumers, government, and businesses.
3. *Encourage open standards and open architectures* to maintain the long term viability of IoT, based on an approach that is scalable, interoperable and reusable across a variety of use case deployments, vendors and sectors. While industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, government should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards. Specifically, government should encourage the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

---

[14] *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities,* Gartner Inc. (Jan. 26, 2015), *http://www.gartner.com/newsroom/id/2970017.*

[15] *Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive,* IHS (June 2014) (253M cars on U.S. roads in 2013), *http://press.ihs.com/press-release/automotive/average-age-vehicles-road-remains-steady-114-years-according-ihs-automotive.*

[16] *Disruptive Technologies: Advances that will transform life, business, and the global economy,* McKinsey Global Institute (May 2013), *http://www.mckinsey.com/insights/business_technology/disruptive_technologies.*

[17] *Id.*

[18] *New "Industrial Internet" Report From GE Finds That Combination of Networks and Machines Could Add $10 to $15 Trillion to Global GDP,* GE (Nov. 2012), *http://www.gereports.com/post/76430585563/new-industrial-internet-report-from-ge-finds-that.*

[19] *CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to drive future business strategies,* Accenture, at 7 (2015), *http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-CEO-Briefing-Report-2015.PDF.*

[20] *Winning the Industrial Internet of Things,* Accenture, at 2 (Jan. 2015), *http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDF.*

4. C*ollaborate with the industry to develop a U.S. National IoT Strategy* with time-bound goals for sector-specific IoT deployments over the next 3 to 5 years. These deployments will not only address critical societal issues and save tax payer dollars, but also will demonstrate U.S. leadership. A National IoT Strategy will help align IoT stakeholders and incentivize innovation, ultimately creating value for society by increasing efficiencies and productivity, creating jobs, sustaining our environment, and improving quality of life in our cities and towns.
5. *As part of our National IoT Strategy, encourage Public-Private Partnerships (PPPs)* to address societal problems and accelerate more rapid deployment of IoT solutions. Government and industry collaboration can be one of our Nation's best assets to accelerate the adoption of a world-class IoT ecosystem. Viable PPPs will make IoT deployments an appealing investment for both government and industry, while ensuring scalability and sustainability of infrastructure and technological innovation over the long term. Notably, countries like China,[21] the UAE,[22] Malaysia,[23] Germany[24], Brazil[25] and others are moving aggressively ahead on IoT deployments—establishing national IoT plans and blueprints establishing time-bound measurable goals, investing substantial funding in IoT research and deployments, and launching PPPs to jumpstart these opportunities and quickly enable IoT scale. As these other countries have recognized, a vibrant and state-of-the-art IoT ecosystem is critical to a nation's global competitiveness and economic stability in the 21st century. By adopting and implementing a National IoT Strategy, the U.S. can seize the leadership position in this next evolution of computing.

Public-Private Partnerships—Market Segment Focus

Specifically, over the next 3 to 5 years, the U.S. should focus on industry vertical segments with the potential to have the most impact: transportation, cities (generally communities, urban and rural), and buildings. Here are proposed PPPs for these market segments:

Smart Transportation PPP: The transportation segment is predicted to be valued at more than $351 billion by 2025, with a CAGR of 19.6 percent (2012–25).[26] In FY 2012, the Federal Agency fleet consisted of more than 650,000 vehicles, which collectively drove over 5 billion miles, consumed nearly 400 million gallons of fuel, and had operating costs of approximately $4 billion.[27] The U.S. Postal Service fleet alone is over 190,000 vehicles.[28] Intel recommends encouraging an IoT Smart Transportation PPP around the USPS fleet or another considerably sized government fleet to implement IoT solutions and benchmark increases in fuel economy, logistics and driver efficiency, and improvements in customer service. Focus areas could include, but are not limited to, fleet and freight management, passenger optimization, auto-

---

[21] China's Ministry of Industry and Information Technology is implementing a three-year (2013–15) action plan to establish a National innovation demonstration area of sensor networks in Wuxi, actively promoting pioneer projects of applications such as intelligent manufacturing, agriculture, transportation, medical systems, and environmental protection: *http://www.usito.org/news/miit-emphasize-iot-rd-sensors-and-chips-2014.*

[22] The Telecommunications Regulatory Authority, in collaboration with the Prime Minister's Office, is working to announce The National Plan for UAE Smart Government Goals: *http://www.tra.gov.ae/news_The_TRA_to_announce_The_National_Plan_for_UAE_Smart_Government_Goals-636-1.php.*

[23] Eyeing a role in global IoT, Malaysia opens CREST centre in Penang (Feb. 2, 2015), *http://www.mis-asia.com/tech/applications/eyeing-a-role-in-global-iot-malaysia-opens-crest-centre-in-penang/#sthash.enmSihPu.dpuf.*

[24] "As part of its High-Tech Strategy ("Ideas. Innovation. Prosperity.") to consolidate German innovation leadership, Germany is making significant R&D investment in the Internet of Things and new services for the diverse application areas within this new connected world." *http://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Smarter-business/smart-products-industrie-4.0.html*

[25] Smart-city to be deployed by Telefonica/VIVO, ISPM in Brazil *http://www.smartgridtoday.com/public/Smartcity-to-be-deployed-by-TelefonicaVIVO-ISPM-in-Brazil.cfm*

[26] *Strategic Opportunity Analysis of the Global Smart City Market: Smart City Market to be Worth a Cumulative $3.3 Trillion by 2025,* Frost & Sullivan (Sept. 2013) ("Frost & Sullivan"), *http://www.frost.com/prod/servlet/report-brochure.pag?id=M920-01-00-00-00.*

[27] *Federal Motor Vehicle Fleet Report FY 2012, http://www.gsa.gov/portal/mediaId/181179/fileName/FY_2012_Federal_Fleet_Report.action.*

[28] *Delivery Vehicle Fleet Replacement* (June 10 2014) Office of the Inspector General United States Postal Service *[https://www.uspsoig.gov/sites/default/files/document-library-files/2014/dr-ma-14–005.pdf]*

matic train protection and control systems and advanced driver assistance and safety.

Impact—Logistics and Transportation was a $1.3 trillion industry in the U.S. in 2012, and represented 8.5 percent of GDP. With almost 9 percent of the U.S. labor force employed in the transportation sector and the U.S. spending roughly $160 billion annually on highway infrastructure (about ¼ funded by the Federal Government), a more efficient and effective trucking industry has the potential to yield significant savings to the U.S. economy. For example, the commercial trucking industry in the U.S. uses about 50 billion gallons of fuel each year. A 7 percent increase in fuel efficiency results in more than 3.5 billion gallons of fuel saved. Imagine if we set a national goal for 25 percent of the Federal Fleet in 3 years, and 50 percent in 5 years, be retrofitted with IoT transportation solutions, not just for telematics but to increase fuel economy by a minimum of 5 percent, with incentives for higher efficiency.

Approach—Consistent with existing national goals to improve the fuel efficiency of American trucks—thereby bolstering energy security, cutting carbon pollution, saving money, and spurring manufacturing innovation[29]—this proposed PPP would leverage private sector and academia IoT expertise in "Intelligent Transportation" solutions. The PPP would accelerate efforts by Congress, DOT, DOC, DOE, EPA, and U.S. commercial fleet managers to increase engine efficiency and fuel economy of large fleets traveling our Nation's roads and highways. It would realize direct economic savings including increased fuel efficiency, reduction in carbon dioxide emissions, labor savings, improved driver safety, accident savings, productivity and distribution proficiency, and logistics tracking effectiveness. The PPP also would provide insights into improvements and new business models for the U.S. transportation sector at large, leading to more satisfied employees and customers. Notably, this PPP would be an early step toward the ultimate goal of an autonomous trucking industry; the estimated savings to the U.S. freight transportation industry from autonomous vehicles is $168 billion per year, with savings from labor ($70 billion), fuel efficiency ($35 billion), productivity ($27 billion), and accident savings ($36 billion).[30] Funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One possibility could be for public and private partners to share in the transportation fuel savings. For example, if the PPP were to reduce a department', or commercial end user operator's fleet, fuel expenses by 7 percent, the department (operator) could allot 2 percent of that savings to the (other) private partners over a specified period of time until the (other) private partners recoup their upfront investment plus some incremental percent of return. The department operator would retain the remaining percentage of the savings, after which time, the department and U.S. taxpayers (operator) would retain 100 percent of the fuel savings benefit in perpetuity.

Smart Cities PPP: Today's cities consume two-thirds of the world's energy.[31] By 2025, 37 cities worldwide will each have a population of greater than 10 million.[32] To address the escalating demands of existing and future residents, cities are looking for ways to introduce more technology to become "smarter" about the use of limited resources and more flexible in responding to residents' needs. Examples of "Smart Cities" capabilities could include but are not limited to: City Sensing including monitoring and providing IoT data to improve air quality, noise pollution, ambient light, weather, and traffic flow; smart parking which is using IoT to "smartly" guide citizens to open parking spaces; smart roads that enable "smart" traffic navigation and roadside service; smart emergency response which facilitates "smart" public and residential community alert and response for vulnerable areas; and smart energy/grid that facilitates "smart" renewable energy and distributed power.

Impact—IoT technologies could realize direct economic savings for cities and municipalities (and their local tax base) due to more efficient city planning and man-

---

[29] *Improving the Fuel Efficiency of American Trucks—Bolstering Energy Security, Cutting Carbon Pollution, Saving Money and Supporting Manufacturing Innovation,* White House (Feb 18, 2014), *http://www.whitehouse.gov/the-press-office/2014/02/18/fact-sheet-opportunity-all-improving-fuel-efficiency-american-trucks-bol.*

[30] *Autonomous Cars: Self-Driving the New Auto Industry Paradigm,* Morgan Stanley Research (Nov. 6, 2013), available at *http://www.morganstanley.com/public/11152013.html.* The authors indicate that $1.3 trillion is a base case estimate and indicate a bear case scenario of $0.7 trillion savings per year in the U.S. and a bull case scenario of $2.2 trillion per year.

[31] *World Urbanization Prospects The 2011 Revision,* United Nations Department of Economic and Social Affairs (March 2012), *http://esa.un.org/unpd/wpp/ppt/CSIS/WUP_2011_CSIS_4.pdf.*

[32] Nate Berg, *The Uneven Future of Urbanization* (April 9, 2012), *http://www.citylab.com/housing/2012/04/uneven-future-urbanization/1707/.*

agement. Results would include improvement in city residents' quality of life, health, and safety. Some examples of this benefit could include more efficient traffic flow, real-time public notifications of pollution "hot spots," and early detection and correction of chemical and gas leaks in aging city infrastructure.

Approach—Consistent with the goals of NIST's Smart America and Global Cities Team Challenges[33]—to use IoT solutions to improve services, promote economic growth, and enhance quality of life—this proposed PPP would leverage private sector IoT expertise in deploying "Smart Community" solutions. These IoT solutions would accelerate local government and municipality efforts to improve urban management and planning in a variety of ways. For example, the PPP could provide a model to improve operational efficiencies and safety across existing and new city infrastructure by utilizing air quality and traffic flow data to enable sustainable traffic management and planning, and create an innovative tool for urban growth management and planning. The funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One opportunity may include public and private partners to share in new revenue streams by leveraging the IoT sensor network infrastructure to deliver new services to city residents. For example, if the PPP were to deliver new services to city residents (i) via the city sensor network or (ii) by sharing the real-time data generated by the city sensor network, the city could share the new revenue stream with the private partners. The city (and its taxpayers) would enjoy the benefits of improved traffic flow, air quality, and safety, and avoiding the hefty cost to rebuild city infrastructure.

Smart Buildings PPP: The smart building segment is predicted to be valued at almost $249 billion by 2025, with a CAGR of 4.1 percent (2012–25).[34] The U.S. Government owns or manages more than 900,000 buildings or other structures across the country making it the Nation's largest landlord. Smart building examples could include, but are not limited to, Smart Government Buildings enabling "smart energy" (HVAC) management, water flow and usage, predictive maintenance/mechanical operations and building security, and smart military bases facilitating the integration of systems and logistics for "smart" traffic flow, people flow, air quality, retail commerce operations, personnel safety and parking.

Impact—The proposed PPP would help the U.S. save on energy expenses while reducing carbon pollution. The U.S. Government—and thus U.S. taxpayers—would realize direct (and possibly significant) economic savings due to improved efficiency in consumption, distribution, and management of energy and utilities across Federal Government buildings and installations. The PPP also would provide insight into savings opportunities and consumption planning for other Federal properties, as well as state and local government properties. In addition, the PPP would introduce new business models that could increase efficiencies and offer new revenue streams for building owners in the public and commercial sectors, while improving services for building tenants and residents.

Approach—Consistent with the goals of the Better Buildings Challenge, to realize building energy savings of 20 percent or more over 10 years[35] and other current initiatives, this proposed PPP would leverage private sector IoT expertise in "Smart Building" IoT solutions to accelerate the U.S. Government efforts to improve operational efficiencies across Federal buildings and/or military installations. Imagine if we set a national goal for 25 percent of Federal Government buildings to be retrofitted with IoT solutions in three years, and 50 percent to be retrofitted with IoT solutions in five years, to increase energy efficiency by a minimum of 20 percent. Upfront funding for the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. Benefits from the PPP also would be shared among public and private sector partners over the short-and long-term, ensuring PPP viability and creating a win-win scenario. One possibility in this case could be for public and private partners to share in the Federal building/installation's energy and utility savings. For example, if the PPP were to reduce a department's energy and utility expenses by 20 percent, the U.S. Government could allocate 10 percent of that savings to the private partners over a specified period of time until the private partners recoup their upfront investment plus some incremental percent of return, and the U.S. Government (U.S. taxpayers) would retain the remaining 10 percent of the savings. After which

[33] *http://www.nist.gov/cps/sagc.cfm*

[34] Frost & Sullivan.

[35] Administration Announces 14 Initial Partners in the Better Buildings Challenge, White House (June 30, 2011), *http://www.whitehouse.gov/the-press-office/2011/06/30/obama-administration-announces-14-initial-partners-better-buildings-chal.*

time, the U.S. Government would retain 100 percent of the energy and utility savings benefit.

Conclusion

Intel appreciates the opportunity to share our perspective on the enormous opportunity of the IoT and a proposed strategy for U.S. leadership in the next evolution of computing.

The CHAIRMAN. Thank you, Mr. Davis.

Mr. Donny?

STATEMENT OF LANCE DONNY, FOUNDER AND CHIEF EXECUTIVE OFFICER, ONFARM

Mr. DONNY. Chairman Thune, Ranking Member Nelson, and members of the Committee, my name is Lance Donny, and I want to thank you for the opportunity to appear before you today and share my thoughts on how connected devices and data will enable farmers to meet global agricultural challenges.

I am the Founder and CEO of OnFarm, a company focused on solving the interoperability and use of devices and data in agriculture.

I grew up on a farm, my family's farm, in California. And I have spent more than 20 years in technology and the last half dozen in leading companies in agriculture. In that time, I have overseen thousands of connected devices and have studied how technology has both succeeded and failed the farmer.

It is clear—and the time is now—agriculture is on the march to adopt and use technology. All of it will be connected. And this trend will enable farmers to make better decisions about how they grow. It will allow them to be globally competitive, and it will be the driving force to meet a global food demand.

My testimony aims to highlight challenges and opportunities as we move to adopt devices and data in ag. One is a means to increase agriculture production and profitability. Two, to help farmers adopt and easily use technology, and third, to advocate for smart, modern policies that spur adoption, avoid unnecessary regulation, and enable U.S. farmers to be globally competitive.

Since the 1950s, farming has doubled production through the use of supplemental nitrogen, irrigation systems, and mechanization of harvesting and planting. But those advances, while momentous, will not suffice to meet the global food demand. By 2050, 9.5 billion people on the planet will require 70 percent more food than we produce today. We will not succeed at meeting this challenge by adding new acres, using more nitrogen or more water.

Connected devices and data fundamentally change how the industry works, and agriculture is no different. It will not escape that trend. Agriculture has moved into the information age.

Data is everywhere. It drives decisions and enables farmers to adopt and be globally competitive. In the day of $3 and $4 corn, farm prosperity will occur using technology and data as a competitive advantage against farmers that do not.

There are two core and interconnected concepts for the Internet of Things in agriculture. First is the connected device itself. Today we see sensors on nearly every part of the farm: the soil, plants, equipment, people, drones, and satellites. Sensors are the first step to better farm management and provide important field data, but

sensors on their own will not allow the farmer to change how they farm.

If you ask a farmer today how much data they have, you will almost always hear too much or it is overwhelming. This flood of data has already surpassed most farmers' capability of managing it. Analytics or big data systems create order and provide insights to keys to delivering the promise of technology in agriculture.

Together, connected devices and analytics give farmers the ability to monitor and use information to manage resources, and as the demand for food increases, these solutions will be the tool that farmers use to help global demand.

In good years, farmers can grow more and more efficiently. In difficult years, like the last several in California due to the drought, connected devices and analytics enable farmers to monitor their fields, to apply the right amount of water at the right time as the crop needs it.

Technology studies have shown the possibilities of increasing yields by a third while reducing water consumption by 20 percent.

Unfortunately, technology can often be cost-prohibitive to farmers. In order to ensure we are globally competitive, we must help growers adopt technology. I support innovation and grants that can dramatically reduce the cost of technology and increase the adoption for the farmer. With modest efforts, we can solve fundamental problems. Today technology is still too costly for farmers. We can and should support them in how they adopt it.

Two, we must help farmers access broadband. In many rural areas, broadband is not available to them, and wireless or cellular coverage is not available on many farms. We can and should accelerate the availability of low-cost, long-range communication to ensure that we move data out of the farm to the cloud as easy as from your Fitbit to the WiFi.

I support a common sense approach to data rights, such as the American Farm Bureau's Privacy and Security Principles that enable the marketplace, the farmer, and the market, to solve conflicts of data and data ownership quickly and easily.

Technology has shown the ability to increase yields, reduce inputs, and enable more productive and sustainable farms. If we achieve technology adoption on a wide scale in the U.S., we can meet global food needs. We can help U.S. farmers maintain their superior position globally, and we can ensure the next generation of farmer is as successful as their parents' generation.

Thank you again for your time today. I look forward to your questions.

[The prepared statement of Mr. Donny follows:]

PREPARED STATEMENT OF LANCE DONNY, FOUNDER AND CHIEF EXECUTIVE OFFICER, ONFARM

Chairman Thune, Ranking Member Nelson, and Members of the Committee my name is Lance Donny. I want to thank you for the opportunity to appear before you today and share my thoughts on how connecting devices and data will enable farmers to meet global agriculture challenges.

I am the Founder and Chief Executive Officer of OnFarm, a company focused on solving the interoperability and use of devices and data in agriculture.

I grew up on my family's farm in California. I've spent more then 20 years in technology and the last half dozen leading companies in agriculture. In that time

I've overseen thousands of connected devices and have studied how technology succeeds and often fails farmers.

It is clear, and the time is now, Agriculture is on the march to adopt and use technology, all of it connected, and this trend will enable farmers to make better decisions about how they grow, it will allow them to be globally competitive, it will be the driving force to meeting global food demand.

My testimony aims to highlight challenges and opportunities as we move to adopt connected devices and data:

1. as a means to increase agriculture production and profitability;
2. to help farmers afford and easily adopt technology; and
3. to advocate for smart, modern policies that spur adoption, avoid unnecessary regulation, and enable U.S. agriculture to be competitive globally.

Since the 1950s farming has doubled production through the use of supplemental nitrogen, irrigation systems, and mechanization of planting and harvesting.

But those advances, while momentous will not be sufficient to meet the growing global demand for food. By 2050 over 9.5 Billion people on the plant will require 70 percent more food then we produce today. We will not succeed at meeting this challenge by adding new acres, using more nitrogen or more water.[1]

Connected devices and data fundamentally change how people and industries work and agriculture has not escaped that change.

Agriculture has moved into the information age.

Data is everywhere. It drives decisions and enables farmers that adopt it to be globally competitive. In the day of $4 corn, farm prosperity will occur using technology and data as a competitive advantage against those farmers who don't.

There are two core and interconnected concepts for the Internet of Things in Agriculture. First, is the connected device itself. Today we see sensors on nearly every part of the farm: from soil moisture, to plants, equipment, and people. Sensors are the first step to better management and provide important field data, but sensors on their own will not allow the farmer to change the way they farm.

If you ask a farmer today how much data they have, you will almost always hear "too much" or "it's everywhere". This flood of data has already overwhelmed farmers. Analytics or "Big Data" software that create order and provide insights is the key to delivering the promise of the Internet of Things.

Together, connected devices and analytics give farmers the ability to monitor and use information to manage resources. And as the demand for food increases these solutions will be the tool that farmers use to help meet global demands.

In good years farmers can grow more and more efficiently. In difficult years, like the last several in California due to the drought, connected devices and analytics enable farmers to monitor their fields and to apply the precise amount of water when and where the crop needs it.

Technology studies have shown the possibilities for increasing yields by 33 percent while we reduce water consumption by 20 percent.[3] Unfortunately that technology can often be cost prohibitive. In order to ensure U.S. farmers are globally competitive we must help farm adoption.

I support both innovation and grants that can dramatically reduce cost and increase adoption. With modest efforts we can solve these fundamental challenges. Today;

1. technology is still too costly for many farmers; we can and should support innovations and incentives that can improve adoption;
2. many farms have no broadband access and cellular coverage is unreliable; we can and should accelerate the availability of low-cost long range communication technology to ensure we can move data from the field to the cloud on every farm; and
3. I support a common sense approach to data rights such as the American Farm Bureau's Privacy and Security Principles[2] that will enable the marketplace to solve conflicts quickly and efficiently.

Technology has shown the ability to increase yield, reduce inputs, and enable more profitable and sustainable farms. If we achieve technology adoption on a wide scale, we can meet global food needs, we can help U.S. farmers maintain global competitiveness, and we can ensure the next generation of farmer is as successful as their parents' generation.

Thank you again for inviting me today, I look forward to your questions.

References

1. "Towards Smart Farming—Agriculture Embracing the IoT Vision"—Beecham Research Ltd., January 2, 2015, *http://www.beechamresearch.com/download.aspx?id=40*
2. "Privacy and security Principals for Farm Data"—The American Farm Bureau Federation, December 19, 2014 *http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf*
3. "NEEA Technical Advisory Group Report—NW Agriculture Irrigation Energy Efficiency Initiative"—Northwest Energy Efficiency Alliance, January 26, 2015
4. "10 Policy Principles for Unlocking the Potential of the Internet of Things"—Center for Data Innovation, December 4, 2014 *http://www.datainnovation.org/2014/12/10-policy-principles-for-unlocking-the-potential-of-the-internet-of-things/*
5. "The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020," ABI Research, August 20, 2014, *https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect.*
6. "Agriculture Water Conservation in the Lower Flint River Basin of Georgia"—Flint River Basin Partnership
7. "Ag-Tech Challenges and Opportunities for Sustainable Growth"—Kauffman Foundation, April 2014 *http://www.kauffman.org/~/media/kauffman_org/research%20reports%20and%20covers/2014/04/agtechwhitepaper_42314_final2.pdf*
8. "Agriculture Gets Smart: The Rise of Data and Robotics"—The Cleantech Group, May 2014 *http://info.cleantech.com/Ag-Get-Smart-Report-Submit.html*

The Problem

The Food and Agricultural Organisation of the UN (FAO) predicts that the global population will reach 8 billion people by 2025 and 9.6 billion people by 2050. In order to keep pace, food production must increase by 70 percent by 2050.

However there are several barriers to fulfilling this imperative, including:

- The slow-down in productivity growth
- The limited availability of arable land
- Climate change
- The increasing need for fresh water
- The price and availability of energy, particularly from fossil fuels
- The impact of urbanisation on rural labour supply – the average age of farmers is increasing with fewer young people going into the industry.

According to a recent report by the UN's Intergovernmental Panel on Climate Change (IPCC), there will be a number of effects of climate change on agriculture. These include an increase in extreme weather events such as heavy rainfall, more intense storms and heat waves, all of which can reduce crop yields. Heavy rainfall can lead to flooding and waterlogging of the soil, whilst in dry parts of the world, water shortages could become more acute. Climate change can also give rise to environmental consequences, such as changes to seasonal events in the life cycle of plants and animals.

Agriculture also consumes 70 percent of the world's fresh water supply; hence water management will go hand in hand with assuring food security.

In order to counter these challenges, the FAO recommends that all farming sectors should be equipped with innovative tools and techniques, particularly digital technologies.

How Will Precision Farming Help?

Precision agriculture aims to optimise the yield per unit of farming land by using the most modern means in a continuously sustainable way, to achieve best in terms of quality, quantity and financial return.

Precision agriculture makes use of a range of technologies that include GPS services, sensors and big data to optimise crop yields. Rather than replace farmer expertise and gut feeling, ICT-based decision support systems, backed up by real time data, can additionally provide information

Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com. info@beechamresearch.com. USA 617 272 1262. Europe +44 (0)845 533 1758.

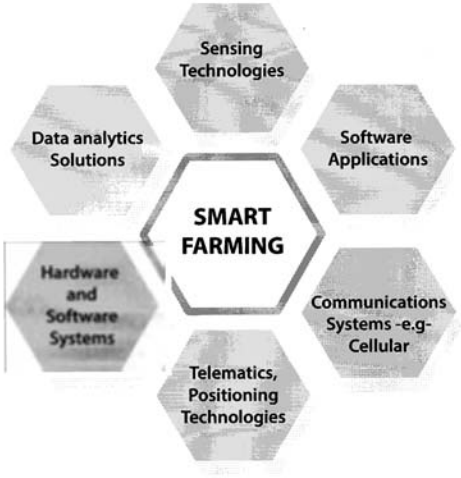
concerning all aspects of farming at a level of granularity not previously possible. This enables better decisions to be made, resulting in less waste and maximum efficiency in operations.

The disciplines and skills now required for agriculture include robotics, computer-based imaging, GPS technology, science-based solutions, climate forecasting, technological solutions, environmental controls and more. Hence to make the best use of all these technologies, it is essential to train farmers and farm managers in their use.

Precision agriculture is sometimes known as 'smart farming', an umbrella term for easier comparison with other M2M based implementations such as smart metering, smart cities and so on. Precision agriculture is a specialist methodology in itself. It is based on sensor technologies whose use is well established in other industries, e.g. Telematics for fleet management, environmental monitoring for pollutants, eHealth monitoring in patients, buildings management for farm silo monitoring and so on.

For all M2M implementations, IT systems gather, collate, analyse the data and present it in such a way as to initiate an appropriate response to the information received. For farmers and growers, a wide variety of information regarding soil and crop behaviour, animal behaviour, machine status, storage tank status emanating from remote sites is presented for action by the farmer.

The chart below show the different types of technologies involved in smart farming.



Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com. info@beechamresearch.com. USA 617 272 1262. Europe +44 (0)845 533 1758.

Application Areas of Smart Farming

The set of technologies used in smart farming is complex, to reflect the complexity of activities run by farmers, growers, and other sector stakeholders. For the purposes of this report, smart farming is structured in the following seven application areas:

1. Fleet management – tracking of farm vehicles
2. Arable farming, large and small field farming
3. Livestock monitoring
4. Indoor farming – greenhouses and stables
5. Fish farming
6. Forestry
7. Storage monitoring – water tanks, fuel tanks

The Smart Farming Ecosystem

The complexity of smart farming is also reflected into the ecosystem of players. They can be classified in the following way:

- Technology providers – these include providers of wireless connectivity, sensors, M2M solutions, decision support systems at the back office, big data analytical systems, geomapping applications, smartphone apps
- Providers of agricultural equipment and machinery (combines, tractors, robots),farm buildings, as well as providers of specialist products (e.g. seeds, feeds) and expertise in crop management and animal husbandry
- Customers: farmers, farming associations and cooperatives
- Influencers – those that set prices, influence the market into which farmers and growers sell their products.

The range of stakeholders in agriculture is broad, ranging from big business, finance, engineering, chemical companies, food retailers to industry associations and groupings through small suppliers of expertise in all the specialist areas of farming.

The end users of precision farming solutions include not only the growers but also farm managers, users of back office IT systems. Not to be forgotten is the role of the veterinary in understanding animal health. Also to be considered are farmers co-operatives, which can help smaller farmers with advice and funding.

The cost of smart farming is still high for any but the largest farms. Farm offices now collect vast quantities of information from crop yields, soil-mapping, fertiliser applications, weather data, machinery, and animal health; these are all factors that influence farming such as soils, nutrition and weather.

Data is the fundamental building block of smart farming, whether the data comes from a soil sample or a satellite correction signal. For example, data points collected can highlight both spatial and temporal variability within a field. Many factors can contribute to this variability; understanding the effect each factor has can only be measured and managed using statistical analysis of the data.

Everyday farming applications are starting to move into the cloud, with the aim of delivering benefits in terms of data access, synchronisation, storage and even cost to the farmer. The rising use of smartphones and tablets on farms means that apps can be used to cache data offline until it can be synchronised; data need no longer be tied to a single computer in a single location.

Partnerships are vital to the value chain, since not even the largest suppliers can fulfil all the needs of the customer by themselves and must cooperate to achieve this.

More complex partnerships are being forged involving cross sector collaboration, with each partner bringing different skills and experience. Partner organisations may be large or small, local or international.

Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com. info@beechamresearch.com. USA 617 272 1262. Europe +44 (0)845 533 1758.

Government and Other Stimuli

The adoption of smart farming solutions is not rapid. The reasons for this are primarily cost – only large farms can afford the investment, and the industry is by nature conservative. In Germany for example, some two thirds of the farms are small to medium sized. For illustrative purposes, we are categorising farms under 10 hectares as small, and over 50 hectares as large

That said, government agencies are stimulating adoption of new technologies through subsidies and projects.

Between 2007 an 2013, the EU allocated €95 billion to the European Rural Development Fund to help modernise the agricultural industry. During the same period, the European Regional Development Fund provided €350 billion for developing rural areas in the wider sense.

Examples of national programmes to promote precision agriculture include:

- UK – Engineering Solutions to enhance agri-food production supported by various government agencies
- Germany – Farming 4.0
- Netherlands – Dike Monitoring Project
- Spain – Projects on irrigation management and viticulture.

Drivers and Barriers

Drivers and barriers to the adoption of precision agriculture are listed below. They include business and market factors as well as technology factors.

Business and Market Drivers	Technology Drivers
Urgent need to reduce waste and increase efficiency	M2M based monitoring and tracking becoming more mainstream across industries
Need to address soil erosion from intensive farming	Reducing costs of sensors, connectivity
Help from public funding and projects	Improving data management technologies to manage tidal wave of M2M data
Need to respond to climate change and environmental deterioration	Farmers becoming more familiar with everyday IT use
Business and Market Barriers	**Technology Barriers**
Return on investment not easy to prove and precision agriculture installations are few and fragmented.	Rural wireless and broadband coverage patchy
Shortage of new blood in the industry	Standards for sensor networks and datacomms still under development
Uncertainty inherent in the industry e.g. weather events, political issues elsewhere in the world	Specialist agricultural software still maturing
Questions to be resolved regarding ownership of the data collected	Uncertainty as to how to treat and safeguard data

Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com. info@beechamresearch.com. USA 617.272.1262. Europe +44 (0)845 533 1758.

Opportunities for Players

MNOs can reach customers in the agriculture industry by partnering with agricultural equipment makers e.g. Deutsche Telekom with CLAAS, Orange Business Services with Dacom.

The vendors and dealers of agricultural machinery with global operations will partner an MNO that provides international coverage, i.e. a global SIM. Furthermore, embedded SIMs are more practicable for sensors located in remote fields. The GSMA is working towards a standard for embedded SIMS that will allow the M2M market to grow.

Sensor makers can partner with providers of M2M management platforms. Sometimes these expand their capabilities from sensor maker to M2M platform provider.

For agri equipment makers, embedding intelligence into the design and operation of machines will allow sensor information to be combined with the knowledge of the farmer, truly closing the loop of precision agriculture.

Towards Smart Farming – Agriculture Embraces the Internet of Things

The notion of 'the connected car' is well established. What makes precision agriculture special is the IT system at the other end of the supply chain, the decision support system at the back office. Whilst the technology is still in its infancy, the notion of 'the connected farm' is coming closer, particularly if the seven types of farming activity we have listed above are somehow connected not only to each other, but also to a raft of historical data such as weather events, climate, economics, product information and specifications, machine settings etc.

This is what the Internet of Things is all about, connecting systems so as to allow an integrated, multidimensional view of farming activities, enabling deeper understanding on how the whole ecosystem works. Precision farming would become 'decision farming'.

From an M2M perspective, the agricultural sector is still considered a minor sector. However, M2M technologies and all the technologies around the Internet of Things vision are key enablers for the transformation of the agricultural sector towards the smart farming vision. The more immediate impact of M2M technologies in agriculture are around providing remote connectivity between sensors in the field and farm information management systems. However we anticipate that the use of sensors in farming will spread to adjunct areas, such as environmental monitoring, land management, and food traceability. This is a consequence of the greater public focus on issues such as food safety and wildlife preservation.

For these reasons, we believe that the use of precision agriculture is bound to grow, not least because of the urgency of the problems the world faces regarding food security in the long term. However, because the technology is in its infancy and not widely understood, this growth will be slow at first compared with sensor based technologies in other industries. This is because of the lack of a vision shared by all stakeholders and their governments as to how to bring together the needs of agriculture with business opportunities. In our report, Beecham Research supplies some forecasts for global wireless and satellite M2M connections from 2012 to 2020.

It is also important to learn the lessons from other large scale 'smart' project rollouts, notably the smart metering projects ongoing in European countries. These are aimed for completion or near completion by around 2020, with smart meters replacing existing ones in homes and business premises. The UK government for one is taking great pains to ensure that a full regulatory framework exists to support the programme and that the full legal implications are understood. These touch on customer privacy, ownership of the data collected, and whether it is permissible for this data to be repurposed for other uses. These issues are equally relevant to the agriculture industry. A similar framework needs to be implemented to reap the best advantages from 'smart farming'.

Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com. info@beechamresearch.com. USA 617.272.1262. Europe +44 (0)845 533 1759.

The full report on Smart Farming will be released beginning Q1 2015

Visit **www.beechamresearch.com** or contact **info@beechamresearch.com** for more information.

Beecham Research Beecham Research Ltd. is an internationally recognized thought leader in the M2M/Internet of Things market. Based in Cambridge UK and Boston, MA, USA, it is a leading technology market research, analysis and consulting firm specializing in the worldwide M2M/Internet of Things market. Our clients include major network operators, hardware/software and infrastructure vendors, distributors /resellers, solution providers and technology adopters. This has now extended into consumer markets with development of the Internet of Things, in particular including Beecham's new report on Wearable Technology published recently. Our research methods include extensive survey work worldwide in multiple languages, based on deep technical knowledge combined with fresh market insight in both business and consumer markets. Recent research has included two market-leading studies on M2M Cloud-based platforms and a worldwide study of the Satellite M2M market for the European Space Agency.

Copyright © 2014 Beecham Research Ltd. All rights reserved. http://beechamresearch.com info@beechamresearch.com USA 617 272 1262 Europe +44 (0)845 533 1758

AGRICULTURAL WATER CONSERVATION IN THE LOWER FLINT RIVER BASIN OF GEORGIA

By investing in "smarter" irrigation, farmers are conserving water while enhancing productivity and yields.

Improving the efficiency of agricultural water use is a shared goal of farmers, researchers and conservationists. Since 2000, these groups have leveraged significant resources to develop and deploy new conservation based technologies in the Lower Flint River Basin of southwest Georgia. The goal is to move innovative agricultural water conservation practices from the research laboratory to the working farm so as to determine economic feasibility, field functionality and conservation impact. Projects are funded through contributions from farmers and cost–share programs. Farmers in the Lower Flint River Basin of Georgia are employing (5) key water conservation measures:

1. *Low pressure drop nozzle retrofits with end gun shut-off:* Savings are generated by applying irrigation water at a lower pressure nearer the soil surface to reduce evaporation and wind drift losses; installing end gun controls to keep irrigation inside the field boundary; and, repairing leaks. *Retrofits (LDR) reduce water use by up to 22.5 percent.*
2. *Variable rate irrigation:* Savings are generated by removing non-crop areas from irrigation; coordinating application amounts with variations in soil type and field topography; and, eliminating double application due to pivot overlap. *Variable rate irrigation (VRI) reduces water use by an average of 15 percent.*
3. *Advanced irrigation scheduling:* Savings are generated by identifying precise periods of time in which a farmer can irrigate less by using objective field data such as soil moisture, soil temperature, crop growth stage and localized ET. *Advanced irrigation scheduling (AIS) reduces water use by up to 15 percent.*
4. *Conservation tillage:* Savings are generated by using a cover crop and leaving plant residue in the field, which modifies plant rooting structure and physiology to enable more efficient water use by crops; improves water holding capacity in the soil; increases water infiltration rates; and, reduces soil temperature, evaporative loss and field run-off. *Conservation tillage (CT) reduces water use by up to 15 percent.*
5. *Sod based rotation:* Savings are generated by incorporating a rotation of a warm season perennial grass into a conservation tillage based production system which yields improved soil quality and water holding capacity, and increased water infiltration and retention. *Sod based rotation (SBR) reduces water use by up to 30 percent.*

   Note: These measures, while in many cases complementary, are not necessarily additive as per the savings generated. Water conservation estimates are based on an average application rate of 13 acre inches per field in a dry year. Estimated reductions in water use are based on field experience, ongoing research and the *Project Report 32: Irrigation Conservation Practices Appropriate for the Southeastern United States.* Average cost per acre to deploy is $100–LDR, $175–VRI, $40–AIS, $40–CT and $400–SBR. Many of these practices create economic and environmental benefits beyond water conservation which help to offset per acre cost.

Who we are? This information is provided by David Reckford, *Flint River Basin Partnership;* Calvin Perry, *UGA C.M. Stripling Irrigation Research Park;* Rad Yager, *UGA Cooperative Extension;* Jim Marois and David Wright, *UF/IFAS Extension;* Wilson Faircloth, *USDA–ARS;* Richard Barrett, *USDA–NRCS;* and, Marty McLendon, *Flint River SWCD.*

Why the Lower Flint? Incorporating 27 counties in southwest Georgia, the Lower Flint is one of the most diverse and ecologically rich river systems in Georgia. Together with the upper part of the Apalachicola, the area is home to the highest density of reptile and amphibian life in the United States, and four federally protected mussel species—the Fat threeridge, Gulf moccasinshell, Oval pigtoe and Shinyrayed pocketbook. The area is also one of the most agriculturally intensive regions in Georgia with more than 40 percent of the Basin's land mass producing $2 billion in farm based revenue annually. Irrigation is central to production with 6,250 center pivot systems in operation.

The Flint River Basin Partnership was formed by the Flint River Soil and Water Conservation District, Natural Resources Conservation Service and The Nature Conservancy to promote agricultural water conservation in the Lower Flint.

neea

Technical Advisory Group Report

NW Agricultural Irrigation Energy Efficiency Initiative

January 26, 2015

NORTHWEST ENERGY EFFICIENCY ALLIANCE

Presentation Objectives

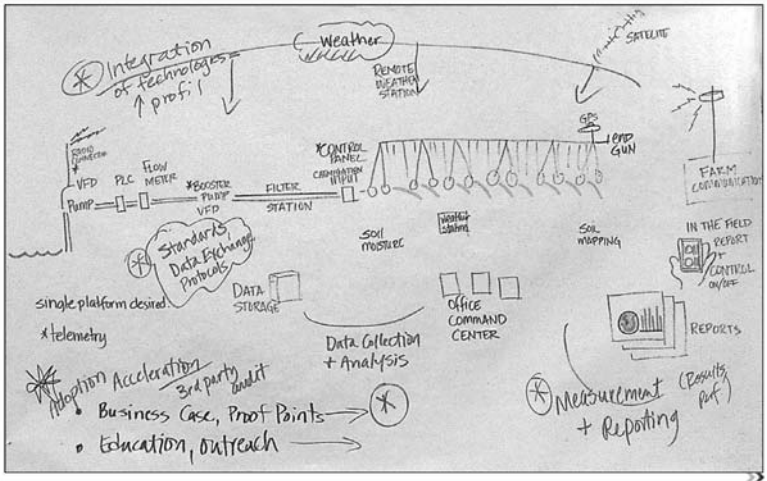
- Review Highlights & Lessons Learned
  - 2014 Demonstration Results
  - Technology & Solutions
  - Data Standards
- Get Your Feedback
- Describe the Road Ahead

THANK YOU

Want to Know More?

Full report will be available at:
http://neea.org/reports

We've Come a Long Way



neea

NEEA's Agricultural Irrigation Initiative

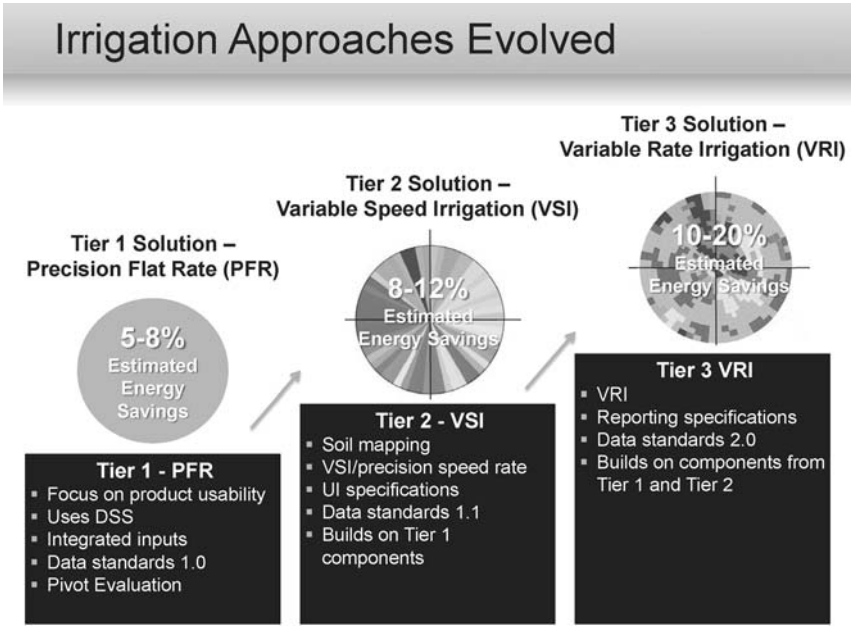
Goal

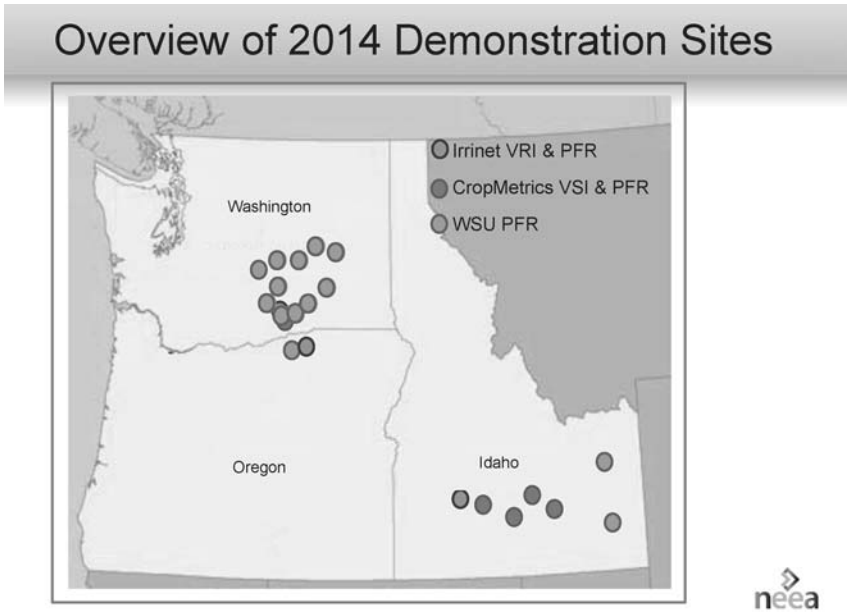
Economic enhancement through 20% Agricultural Irrigation energy efficiency by 2020

Key Benefits

Improve yield uniformity
Decrease energy consumption
Improve energy intensity
Increase profit per acre
Drive productivity through technology

neea


Irrigation Approaches Evolved
Tier 1 Solution – Precision Flat Rate (PFR)
5-8% Estimated Energy Savings
Tier 1 - PFR
Focus on product usability
Uses DSS
Integrated inputs
Data standards 1.0
Pivot Evaluation
Tier 2 Solution – Variable Speed Irrigation (VSI)
8-12% Estimated Energy Savings
Tier 2 - VSI
Soil mapping
VSI/precision speed rate
UI specifications
Data standards 1.1
Builds on Tier 1 components
Tier 3 Solution – Variable Rate Irrigation (VRI)
10-20% Estimated Energy Savings
Tier 3 VRI
VRI
Reporting specifications
Data standards 2.0
Builds on components from Tier 1 and Tier 2


Overview of 2014 Demonstration Sites
Irrinet VRI & PFR
CropMetrics VSI & PFR
WSU PFR
Washington
Oregon
Idaho
neea

VRI Results: What Worked, What Didn't

Report from Jan 2014 Tag:

What Works As Is

- Remote Rx uploaded
- VRI/VSI fully operational

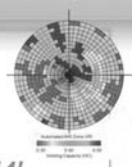
What Can Work, But…

- Moisture probe data quality
- Telemetry reliability
- Yield map data quality
- VRI Usability

What Doesn't Work Now

- EC maps → HC & PAW maps
  - No working VRI maps
- Grower cooperation
- Cost is a barrier

Report from Jan 2015 Tag:



= Major progress in 2014!

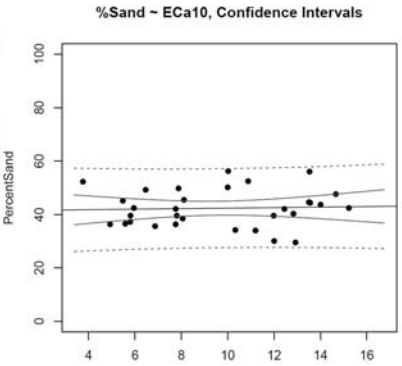
- Good lead on cause of problem
- Improved reliability

- Irrinet generated useful maps
- OSU identified EC root cause
- Take smaller incremental steps

neea

Soil Mapping: Motivation

- Precision Irrigation requires accurate PAW
- Precision Irrigation with VRI requires a ***map*** of PAW
- Several sites showed poor correlation between texture and EC_a → PAW not accurate

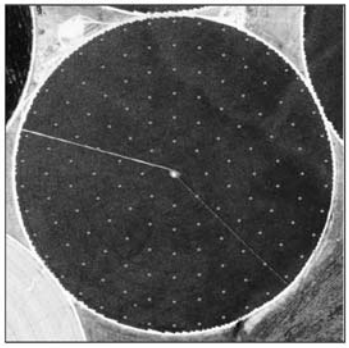


Correlation between EC_a and % Sand
Ideal correlation would show most points on straight line

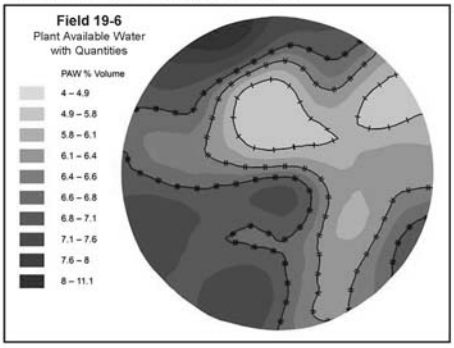
neea

Soil Mapping: Experiment

Grid sampling of soil properties



Map of PAW from grid samples

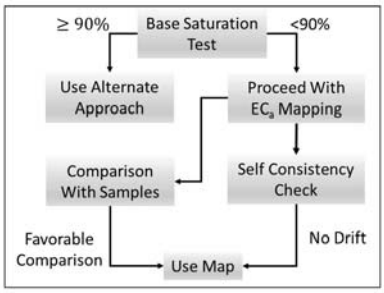


- Process performed at three locations
- ECa map data analyzed for self-consistency
- Grid maps were compared with ECa maps to identify soil properties that confound the correlation between ECa and measured physical properties

11

Soil Mapping : Conclusions

- Soil mapping can be used in a wide variety of conditions
- Some soils in Columbia Gorge region can complicate accuracy of ECa maps
- Test of Base Saturation and self-consistency test must be used to validate ECa maps

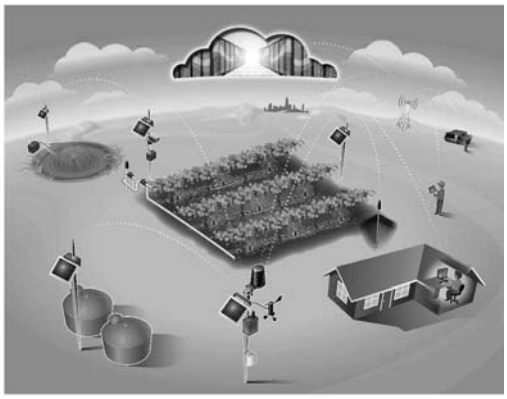


For more detail, see *Using Soil Electrical Conductivity Mapping for Precision Irrigation in the Columbia Basin* report

12

Telemetry Improvements

- Data all season
- Going forward
  - Realistic range
  - Use “meshing”
  - Use “whip” antennas
- For more details, see *Instrumentation and Hardware Best Practices in Precision Agriculture*



neea

Telemetry Improvements

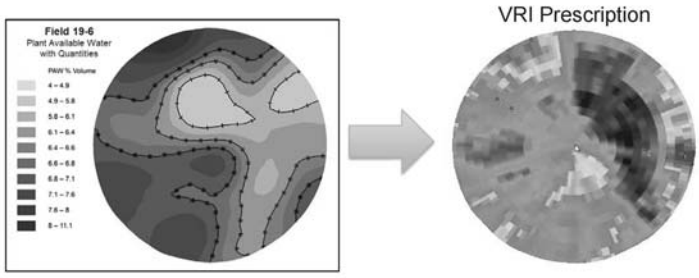
- Data all season
- Going forward
  - Realistic range
  - Use “meshing”
  - Use “whip” antennas
- For more details, see *Instrumentation and Hardware Best Practices in Precision Agriculture*

neea

Creating Usable VRI Prescriptions

When EC Mapping was problematic, alternative methods proved useful

- Used EC Maps to generate Rx on farms 19 and 21
- Used Texture Grid Maps to generate Rx on farm 20.



neea

Final Results for VRI in 2014

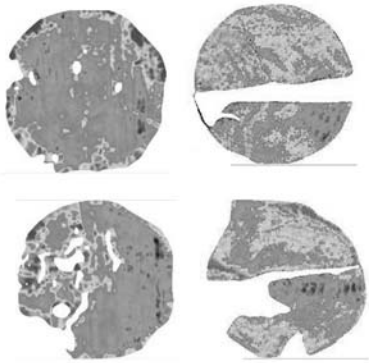
- Farm 19: diverted water to potatoes, shut off irrigation 6 weeks early
- Farm 20: field to field, year to year variations swamp out any measurable improvement
- Farm 21: operational mistakes led to pivot getting stuck in the same place repeatedly.

neea

Fields Highly Suited to VRI

Multi-Crop

Lava Outcrops



For more detail on VSI, visit *Irrigation Delivery Strategies* report

neea

VSI Results: What Worked, What Didn't

Report from Jan 2014 Tag:

What Works As Is:

- VSI installed on time
- Experiment started on time

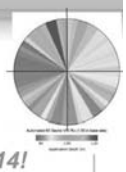
What Can Work, But…

- ★ Capacitance probe data?
- ★ VSI ROI?

What Doesn't Work Now:

- ★ EC Map data quality
- ★ Irrigation schedules
- Calculated Total Energy?
- ★ Yield improvement?

Report from Jan 2015 Tag:



★ = *Major progress in 2014!*

- Used NP as backup
- VSI case studies sold growers More Details

- OSU solved questions
- Much better grower engagement
- Final report is past due
- 4 of 5 show significant gains More Details

New!

- Prototype Pivot Evaluation More Details

neea

Compelling VSI Demo Results

- Farm 15 corn: Operational issues prevented grower from using any recommendations.
- Farm 16 corn: Increased yield 33% over historic high on one field.
- Farm 17 wheat: no yield improvement, but dramatic decrease in mold.
- Farm 17 potatoes: 33% increase in yield over historic high
- Farm 18 barley: 14% increase in yield compared to record high, with 7-8 fewer irrigation rotations.

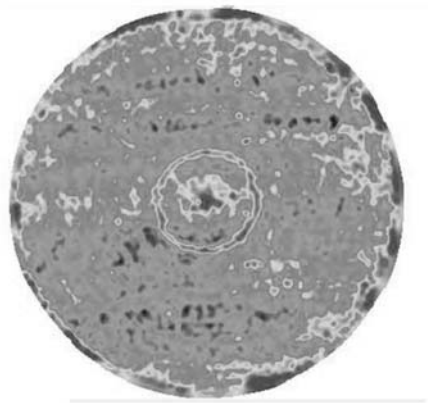
➢ 4 out of 5 demos show compelling case for improvement

➢ VSI and Irrigation Scheduling services are growing like gang-busters

For more detail, see *Irrigation Delivery Strategies* report

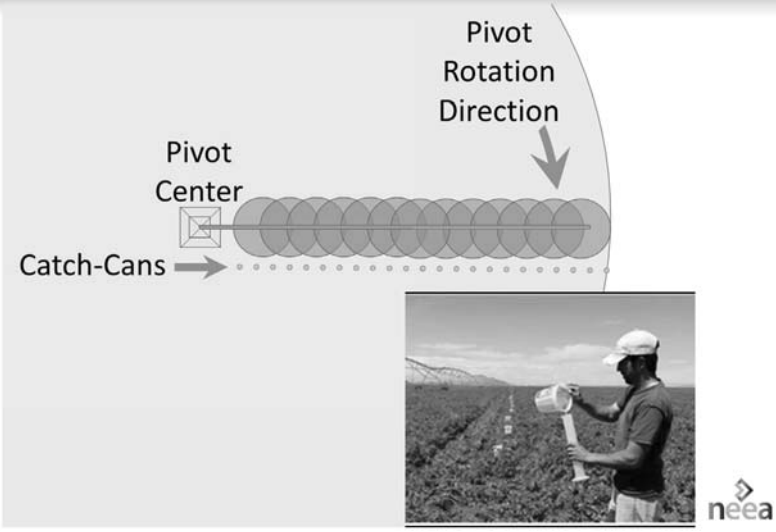
neea

Pivot Evaluation



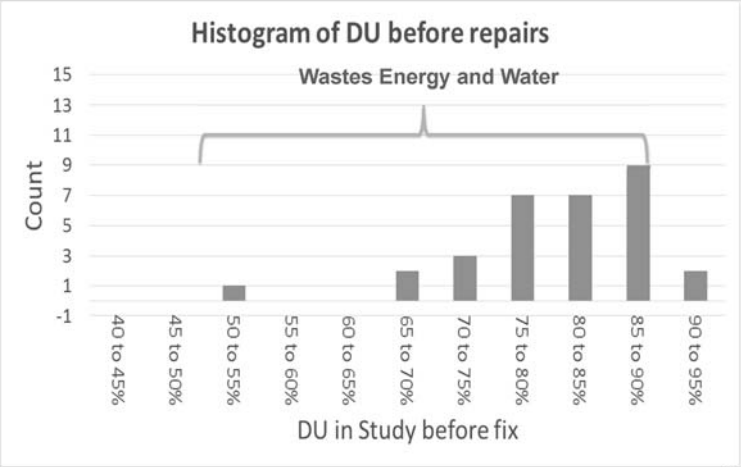
neea

Pivot Evaluation Method:



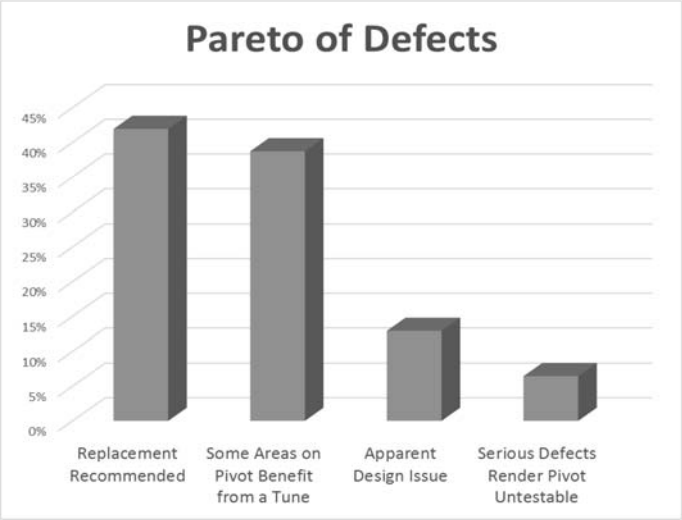
neea

Distribution Uniformity (DU)



neea

Every Pivot in Study Would Benefit

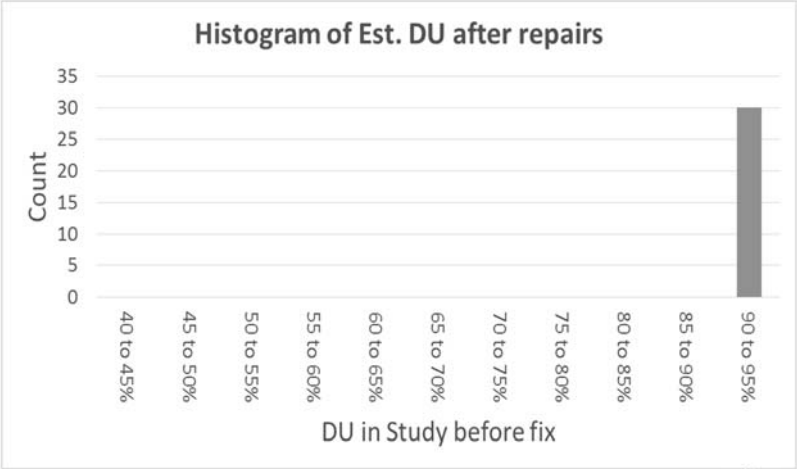


Key Insight: Pivot Tuning

≅

Every pivot studied would benefit from a "tune-up".

With Proper "Tuning" Expected Result



For more detail, visit *Pivot Evaluation Best Practices Report*

neea

PFR Results: What Worked, What Didn't

What Works As Is:

- 3 approaches tested:
  - WSU Demos w/ Irrigation Scheduler Mobile (ISM) on 15 fields
  - CropMetrics Demos on 6 fields
  - Irrinet Demos w/ ProbeSchedule on 2 fields
- When tools are used, all appear to generate significant savings
  - Field 20-8 showed 30% water savings (Irrinet)

What Can Work, But…

- As straightforward as ISM is, it is still to complicated for mass adoption
- Automating as-applied-water would accelerate adoption
- Impossible to keep growers from applying PFR recommendations to Reference Fields
- For CM, savvy growers did their own VSI on PFR fields

neea

Data Exchange Standards

PAIL Data Exchange Standards

- Completed PAIL Phase 1
- Alpha Test at two sites
- Submitting to AgGateway Standards & Guidelines and ASABE
- Launching PAIL 2

AgGateway

LINDSAY CORPORATION
OBSERVANT
Cropletics
VALLEY
CAMPBELL SCIENTIFIC
CROP IMS
Ranch Systems
ONFARM
DECAGON DEVICES
IRROMETER
Simplot
MapShots
Ag Connections
AgSense
IRRINET LLC
AGRIAN
MONSANTO
RPE
Zed XXV
JOHN DEERE
neea

PAIL Phase 1 Completion

29

Irrigation system (not restricted to pivots) setup, configuration, performance specification
- ✓ Location and geometry of the irrigation system
- ✓ End gun, corner arm specification
- ✓ Flows and pressure

Field and environmental information
- ✓ Location
- ✓ Soil conditions
- ✓ Local and regional weather conditions & forecasts

Irrigation system operation, control, and status
- ✓ Schedules (how much and when)
- ✓ Irrigation work orders – still a couple of issues to resolve
- ✓ Error reporting
- ✓ Reporting on how much, and where, water was applied

neea

Data Standards Phase 2 Scope

- Other irrigation technologies
  - Surface Irrigation
  - Drip Irrigation
  - Laterals
  - Traveling guns and wheel lines
  - Solid Sets
- Flow Meters
- Pumps
- Energy
- Common Climate Data Formats
- Beta Test- looking for sites

For more detail, see *Data Exchange Standards* report

neea

Strategy Shift & Wrap Up

- Incorporated feedback from our funders
- Identified gap of technical maturity of components
- NEEA will re-scope the Agricultural Irrigation Initiative and focus on scanning market-ready discrete technologies

neea

Next Steps

Emerging Technologies

Pivot Evaluation (small to large)

Data Standards

- Publish & Socialize PAIL, Phase 1
- Develop PAIL, Phase 2
  - Includes BETA testing

neea

Ongoing Role of TAG

Review relevant final reports
- Provide feedback
- Deep dive into Lessons Learned?

- Meet twice yearly
- Review progress on PAIL 2 Data Standards
- Review/give guidance on next scanning activities

Always open for unsolicited proposals
- Send to Geoff Wickes or to http://neea.org/get-involved/submit-your-idea

---

Want to Know More?

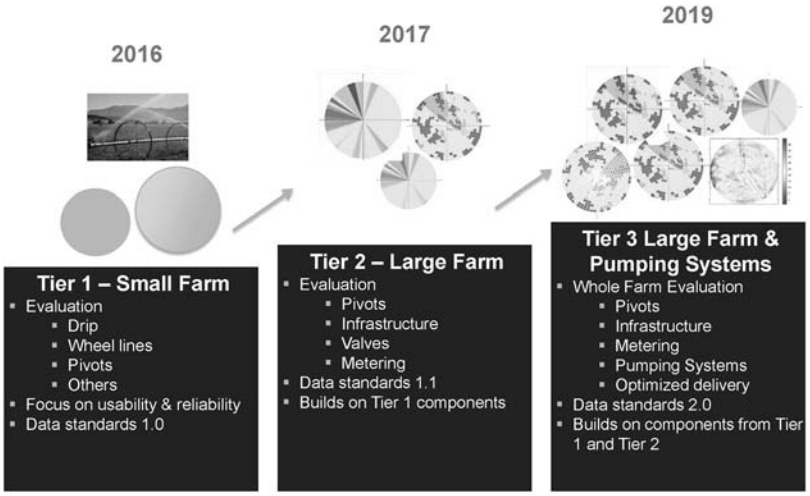
Dive on in at: http://neea.org/reports

- Discover *The Future of Irrigation*
- Orient yourself with an *Overview of Center Pivots*
- Go deep with *Irrigation Delivery Systems*
- Improve your game with *Hardware Best Practices*
- Get involved with *Grower Experiences*
- Dig into a *Soil Primer*
- Get the dirt on *Soil Mapping*
- Contain yourself with *Catch-Can Tests*
- Compute the *Business Case & Economic Model*
- Fix your attention on *Pivot Evaluation*
- Come together with *Data Exchange Standards*

Back-Up Slides

neea

Potential Scanning 2015: Pivot Evaluation



10 Policy Principles for Unlocking the Potential of the Internet of Things

Center for Data Innovation

By Daniel Castro & Joshua New / December 4, 2014

The success of the Internet today can be credited in part to policymakers actively taking a role to ensure its growth, and this same approach should to be applied to build the Internet of Things.

Summary: "The Internet of Things" encapsulates the idea that ordinary objects will be embedded with sensors and connected to the Internet. To date, most discussion of the Internet of Things has highlighted the technology; to the extent it has addressed policy, the focus has been largely negative (i.e., how to limit the supposed risks from deployment). In contrast, this report highlights principles that policymakers in all nations need to apply in order to maximize the considerable promise of the Internet of Things for economic growth and social well-being. Of two conflicting approaches to the Internet of Things, neither: the "impose precautionary regulations" nor the counter "leave it completely up to the market" will allow societies to gain the full benefits from the Internet of Things revolution. This report presents ten principles to help policymakers establish policies and programs to support and accelerate the deployment and adoption of the Internet of Things.

The Internet of Things encapsulates the idea that ordinary objects—from thermostats and shoes to cars and lamp posts—will be embedded with sensors and connected wirelessly to the Internet. These devices will then send and receive data which can be analyzed and acted upon. As the technology becomes cheaper and more robust, an increasing number of devices will join the Internet of Things. Though many of the changes to everyday devices may be subtle and go unnoticed by consumers, the long-term effect could ultimately have an enormously positive impact on individuals and society. A connected world is capable of anything from improving personal health to reducing pollution to making industry more productive. The Internet of Things offers solutions to major social problems, but this vision of a fully connected world will not be achieved without initiative and leadership from policymakers to promote its deployment and avoid pitfalls along the way.

The potential size and scope of the Internet of Things is enormous, with over 16 billion devices estimated to be in use today, and many more to come.[1] By 2020, the total worldwide count is expected to reach over 40 billion.[2] This growth is visible across practically every industry. By 2020, the number of wearable devices will surpass 100 million, the number of Internet-connected cars will exceed 150 million, and the number of connected wireless lights will reach 100 million—to name just a few.[3]

The magnitude of the benefits brought by the Internet of Things is also impressive, and this technology may improve nearly every aspect of life. Consider the benefits of smart homes. Connected devices that automatically regulate electricity usage based on whether anyone is home can cut energy usage and bills.[4] Smart meters can send dynamic price signals to smart appliances to reduce peak energy consumption.[5] Connected sensors can improve home safety by detecting fires and other emergencies more quickly and reliably than traditional methods, alerting authorities sooner.[6] Blinds that automatically detect and filter out sunlight, smart heating and cooling systems that can maintain different rooms at different temperatures, and lighting that automatically adapts to time of day and can be controlled from a smartphone will make home life more comfortable than ever before.[7]

Connected devices can also provide consumers important new insights about their health and fitness. Companies are designing wearables for every stage of life from smart "onesies" with embedded sensors that help parents monitor their infants' health to activity sensors that allow elderly adults to live safely and independently. Wearable biometric monitors can help individuals track their health, monitor chronic medical conditions, and improve health care outcomes.[8] In addition, fitness trackers such as FitBit and Nike FuelBand can help consumers be more active and engage in healthy behaviors.[9]

Local leaders can help build smart cities by integrating the Internet of Things into public buildings and infrastructure, including roadways, transit systems, and utilities. These technologies can help make cities safer, more sustainable, and more resilient while also providing new economic opportunities for their residents. For example, networked sensors can monitor the structural integrity of bridges and highways in real time to prevent catastrophes from happening and encourage cost-savings through timely preventative maintenance.[10] And, intelligent transportation sys-

tems can make roads safer, facilitate traffic flow, and make public transportation more efficient.[11]

Industries that restructure their practices around the Internet of Things can improve productivity and sustainability. With everything from networked assembly lines that track every screw turn to ensure quality control and safety to connected supply chains that reduce downtime and ensure transparency in material sourcing, the Internet of Things will increase industry competitiveness.[12] The increased capacity for data collection from the Internet of Things brings benefits as well. Insurers can use actuarial models that factor in data from connected devices to better understand risk and reduce costs for their customers. Companies can monitor and enhance the safety of their workers in real time and prevent accidents.

Overall, global spending on the Internet of Things is predicted to grow to approximately $3 trillion by 2020.[13] Of course, any capital equipment represents a cost, not a benefit. In that businesses and consumers purchase technology only if benefits exceed costs and because many benefits extend beyond the immediate purchasers to the entire network, the overall economic benefits from the Internet of Things will be even more significant.[14]

As technological barriers decrease and adoption of the Internet of Things takes off, its potential benefits depend in part on how policymakers respond to this technology. There are four main approaches policymakers could employ regarding the Internet of Things:

1. Precautionary regulations: Some policymakers focus on the potential risks associated with the Internet of Things and want to regulate it accordingly. These policymakers believe that preemptive regulations will increase consumer trust and therefore increase adoption, but the reality is that heavy-handed rules would likely imposes costs, limit innovation, and slow adoption.
2. No intervention: Some policymakers resist laws and regulations for the Internet of Things because they believe the free market operating independently of government interventions achieves the maximum possible consumer benefit. However, by avoiding all interventions, policymakers miss the opportunity to proactively support the deployment of the Internet of Things.
3. Indigenous innovation: Some policymakers view the Internet of Things as an opportunity to create export opportunities for domestic firms. These policymakers may endorse policies that hinder foreign companies from competing in the domestic market, such as adopting national technical standards rather than adopting international ones.[15] Such policies are anti-competitive and create fragmented markets for the Internet of Things.
3. Technology champions: Some policymakers have taken a proactive role in accelerating the development and deployment of the Internet of Things, such as by funding research on sensor networks, creating pilot projects for smart cities, preventing over-regulation of wearable health technologies, and providing incentives for smart grid deployment. These policymakers see government as a critical partner in promoting the benefits that come from using these technologies.

Recognizing the inherent shortcomings and limitations of some of these approaches is crucial to developing sound policy for the Internet of Things. The status of the Internet of Things as an emerging technology necessitates a policy framework that is fully cognizant of its benefits, allows for future innovation, and responsibly protects against misuse without restricting its capacity to deliver social, civic, and economic benefits.

10 Policy Principles for the Internet of Things

1. Chart the Course for Adoption

Every nation should develop a strategic roadmap to guide the deployment and adoption of the Internet of Things. In addition to a comprehensive roadmap, national agencies involved in specific sectors can develop targeted action plans for particular industries. In the United States, for example, the Department of Housing and Urban Development should develop an action plan to promote smart homes, and the Department of Energy should develop a plan to improve energy efficiency with connected devices. The private sector will be more likely to embrace the Internet of Things if government leaders are paving the way for deployment.

Policymakers should actively work to overcome barriers to adoption, such as security risks or a lack of interoperability. For example, electronic health records should be able to integrate data from wearable medical devices and the government can promote industry adoption of voluntary cybersecurity principles to protect consumer data. Since many of the benefits from the Internet of Things will occur with wide-

spread adoption, policymakers should promote efforts to develop global, industry-led standards and oppose efforts to develop nation-specific standards. To maximize the potential benefits of data analytics, developers should also be able to easily share and integrate data across organizational, political, and geographic boundaries.

2. Lead by Example

The government should be an early adopter of the Internet of Things to demonstrate the benefits of the technology. From sewers to streetlights, government agencies should make "smart" the default for all new investments and allocate funding for smart city demonstration projects. For example, all government infrastructure projects should incorporate the Internet of Things into their design. Investing in smart technology for public infrastructure projects will increase safety, reduce maintenance costs, and improve operations. In addition, these projects will generate valuable data that should be made available to the public.

To maximize the benefits of the Internet of Things, government agencies should restructure their practices around the new capabilities offered by the technology. Public services that incorporate connected sensors can provide important benefits to the public. For example, the City of Buffalo, New York uses sensor-equipped snow plows to respond to citizens' snow-clearing requests more quickly and to target problem areas more efficiently.[16] And, government agencies that perform inspections of equipment and facilities can use the Internet of Things to perform their duties more quickly and effectively. For example, the U.S. Department of Agriculture (USDA) approved new regulations to allow advanced imaging sensors to evaluate food safety and quality. As a result, a single poultry food safety inspector can now process 175 birds per minute, up from a previous speed of 35 birds per minute, a substantial gain in efficiency.[17]

3. Look to Partnerships to Overcome Obstacles

Many Internet of Things projects will benefit from government agencies establishing partnerships with both the private sector and others in government. In particular, funding these types of projects can be challenging for cities with limited budgets. For example, a city may not have the budget to install smart streetlamps, even if they would end up paying for themselves in energy savings. Innovative partnerships whereby the private sector pays for, builds, and manages certain technology projects while receiving a portion of the savings can allow local leaders to deliver the Internet of Things and its benefits in situations where budget constraints would have otherwise impeded progress. For example, the City of Mumbai, India partnered with a smart metering company to help with its failing water infrastructure that was leaking 50 percent of its water a day. For the same amount of money the government would have spent patching new leaks without ever improving the overall integrity of the system, the partnership with the metering company cut the water loss in half.[18]

4. Reduce Regulatory Barriers and Delays for Getting Smart Devices to Market

A lengthy and cumbersome regulatory review process that increases the time to market for smart devices can discourage entrepreneurs from developing new and potentially lifesaving products. Wearable technologies can allow individuals to spend less time in the hospital, receive better treatments, and more easily monitor their personal health. Since subjecting these technologies to lengthy regulatory review processes can delay these benefits from reaching consumers, policymakers should work to ensure that these processes are as efficient as possible. Moreover, most of these technologies will undergo continuous innovation and improvement and the regulatory review process should allow for, and encourage, upgrades. In a clear example of a review process with room for improvement, it takes on average over two and a half years for the U.S. Food and Drug Administration to approve a low-risk medical device, compared to an average of seven months in Europe.[19] These delays can cost a company an average of $500,000 per month and discourage entrepreneurs from bringing products to market.[20] While consumer safety should remain a top priority, the human cost of delaying lifesaving technology should not be ignored.

5. Minimize the Regulatory Cost of Data Collection

Policymakers should create laws and regulations that allow businesses and governments to build products and services efficiently, using the highest quality, most complete data possible. For example, obtaining explicit consent for data collection would be an unnecessary cost for the vast majority of applications of the Internet of Things that pose no real threat to consumer welfare. Regulations requiring individuals manually to give consent to data collection would impose costs on companies that ultimately would be passed on to consumers. Instead, the standard method of data collection for the Internet of Things should be "opt out"; this would ensure that

the data is accurate, complete, and useful, yet still provide those who wish not to share their data that option.

Similarly, policymakers should recognize that consumers do not benefit from being inundated with notices, especially since most data collection would be routine and insignificant. Rather than require that all devices directly notify consumers of their policies and terms of service, companies should simply make this information available to those who wish to read it. This type of shift is especially important since many devices that will make up the Internet of Things will have only a small display or no display at all.

6. Make It Easy to Share and Reuse Data

The Internet of Things will generate an unprecedented quantity of data, and policymakers should be careful not to equate simple data sharing with harmful misuse. Data collected from connected devices offer a myriad of potential benefits to consumers, clinicians, researchers, government agencies, and commercial entities, and if these datasets are shared, these benefits are multiplied. There may be one primary reason to collect data, but one hundred good applications of this data beyond its initial purpose. In order to maximize the social and economic benefits of information, data users of all kinds acting in good faith must be able to share and reuse data with ease.

As governments at the municipal, state, and Federal levels integrate connected devices into public infrastructure and government services, the de-identified data they collect should be treated as a public resource and shared with the public accordingly. Making this data easy to access, such as through portals and application programming interfaces (APIs), and free to reuse without restrictions creates tremendous opportunity for private-sector innovation, academic research, and improvements in government transparency.[21] The City of Chicago, which has been integrating the Internet of Things into city infrastructure and services as part of its Array of Things project, has made over 600 machine-and human-readable datasets freely available online.[22] With this new resource, citizens have been able to more easily navigate public transit, the city's pest-control agency has reduced the rat population, and the police have created predictive models to fight crime more effectively.[23]

Since the full potential benefits of the Internet of Things will not be realized until data from interconnected technology are widely used, policymakers should incentivize both individuals and the private sector to share data. For example, governments can support the development of new tools and techniques to properly de-identify different types of data so that they are still useful for analysis.[24] Where possible, companies should be encouraged to provide consumers access to their data to stimulate the development of new applications. For example, the U.S. Department of Energy's green button initiative gives consumers access to their energy usage data and allows them to share their data with third-party developers who provide services such as virtual energy audits.[25] Policymakers should also work to ensure data can flow across borders and eliminate digital barriers to trade, such as data residency requirements and other localization policies.

7. Relentlessly Pursue Better Data

With ever-higher-quality sensors and an increasing number of them, the Internet of Things allows for the capture of an unprecedented quantity and quality of data. Policymakers should continue to invest in opportunities to collect more granular, timely, and complete data. Government agencies should use better data to better monitor internal processes and improve productivity and outcomes. For example, police departments can use sensors to better monitor the safety of their officers in real time and to hold officers responsible for their actions. Port authorities can use sensors to better protect the border by tracking containers and shipments coming into the country. Better data enables not only a more effective government, but a more transparent one as well.

8. Reduce the "Data Divide"

Policymakers should encourage widespread adoption of connected devices, from wearable fitness trackers to sensors on street corners, to close the "data divide"—the social and economic inequalities that may result from a lack of collection and use of data about an individual or community.[26] The goal of policymakers should be to ensure that no groups are systematically excluded from data collection activities so that all individuals have the opportunity to obtain the social and economic benefits of data.

Policymakers should work to develop programs to ensure that all communities can benefit from the Internet of Things. For example, funding for smart city infrastruc-

ture should be made available to a diverse set of neighborhoods, including low-income ones.

9. Use Data to Tackle Hard Problems

While the Internet of Things offers many economic benefits, policymakers need to ensure that opportunities to use these devices to address important social issues, such as health care and public safety, are also a top priority. For example, aggregate data from personal fitness devices can provide health officials with unprecedented insights into public health. Tracking changes in biometric readings across a city could even help identify the spread of deadly outbreaks, helping public officials better contain diseases and start treating sick individuals earlier. As Google's CEO and co-founder Larry Page has noted, public squeamishness over mining of health data likely costs around 100,000 lives a year.[27] Policymakers should support efforts to collect and aggregate data on a large scale to solve collective problems.

Networked sensors can detect flooding and trigger emergency responses more quickly.[28] Wearable technologies and sensors on street corners can give new insights onto air quality on a block-by block-basis and help develop strategies to curb pollution.[29] The list of ways public welfare could be enhanced by the Internet of Things is long, but if it is to be fully effective in addressing these problems, policymakers should shift their focus to the problem-solving capabilities of smart devices.

10. Where Rules Are Needed to Protect Consumers, Keep Them Narrow and Targeted

Many technologies are often met with fear, uncertainty, and doubt, especially by those who are unfamiliar with them or opposed to change. Policymakers cannot afford to succumb to these forces if they expect to enable society to take full advantage of the Internet of Things. In particular, policymakers should be extremely cautious about regulating on the basis of purely speculative concerns that might not even come to pass, especially when doing so might curtail substantial economic and social benefits, many of which are already being realized today.[30] Most hypothetical concerns are likely to never become realities if factors such as market forces, cultural norms, and new technologies, intervene. In addition, existing laws, such as anti-discrimination statutes, often protect individuals from certain types of abuses and harms.

However, policymakers should intervene promptly if specific problems arise. In doing so, they should be careful to ensure that their rulemaking targets specific, demonstrated harms. Attempting to erect precautionary regulatory barriers for purely speculative concerns is not only unproductive, but it can discourage future beneficial applications of the Internet of Things. For example, privacy activists raised objections when several cities made plans to install gunshot detection equipment in public spaces. However, the effectiveness of these technologies in reducing gun crime has proven to be incredibly valuable to law enforcement.[31]

Conclusion

These ten policy principles serve as a blueprint for Internet of Things policies that promote adoption, increase the value of data collected from connected devices, and maximize the benefits of the Internet of Things for consumers, government, and industry. While many of the future challenges of the Internet of Things may still be unknown, a policy framework built around these principles should maximize the benefits from the Internet of Things. The success of the Internet today can be credited in part to policymakers actively taking a role to ensure its growth, and this same approach should to be applied to build the Internet of Things.

References

1. "The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020," ABI Research, August 20, 2014, *https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect.*

2. Ibid.

3. Jolyon Barker, Paul Lee, and Duncan Steward, "Technology, Media & Telecommunications Predictions 2014," Deloitte, 2014, *http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tech nology-Media-Telecommunications/gx-tmt-predictions-2014.pdf* and Keith Bloomberg, "The Race to Market the Connected Car," Automotive News, January 10, 2014, *http://www.autonews.com/article/20140110/OEM06/301109910/the-race-to-market-the-connected-car,* "100 Million Internet Connected Wireless Lights by 2020," ON World, November 20, 2013, *http://onworld.com/news/100-Million-Internet-Connected-LED-Lights-by-2020.html.*

4. Ilana Greene, "Smart Houses Help Reduce Energy Use and Save Money," Huffington Post, December 19, 2013, *http://www.huffingtonpost.com/ilana-greene/smart-houses-help-reduce-__b__4472919.html.*

5. Austin Harney, "Smart Metering Technology Promotes Energy Efficiency for a Greener World" Analog Dialogue, Volume 43–01, January 2009, *http://www.analog.com/library/analogdialogue/archives/43-01/smart__metering.pdf.*

6. Juhwan Oh, Zhongwei Jiang, and Henry Panganiban, "Development of a Smart Residential Fire Protection System, Advances in Mechanical Engineering, Volume 2013, 2013, *http://www.hindawi.com/journals/ame/2013/825872/*.

7. Jason Chen, "Home Automation! What You Need to Know to Not Be Dumb," Gizmodo, September 27, 2010, *http://gizmodo.com/5647352/home-automation-what-you-need-to-know-to-not-be-dumb*.

8. Joshua New, "Healthcare Insurance Regs Must Keep Up With Tech Advances," Center for Data Innovation, October 13, 2014, *http://www.datainnovation.org/2014/10/healthcare-insurance-regs-must-keep-up-with-tech-advances/*, Neil Versel, "Lively, a new eldercare monitoring system focused on social connections, heads to Kickstarter," Mobi Health News, April 16, 2013, *http://mobihealthnews.com/21650/lively-a-new-eldercare-monitoring-system-focused-on-social-connections-heads-to-kickstarter/* and Dana Wollman, "The Internet of Toddlers: Inter Shows Off a Smart Baby Onesie," Engadget, January 7, 2014, *http://www.engadget.com/2014/01/07/intel-smart-baby-onesie/*.

9. Kira Newman, "The 'Quantified Self' Is Only the First Step to Better Health," Tech Cocktail, May 28, 2013, *http://tech.co/quantified-self-better-health-2013–05*.

10. "Wireless Structural Monitoring System Deployed in Korea," University of Illinois, November 30, 2009, *http://cee.illinois.edu/node/1022*.

11. "Smart Cities are Built on the Internet of Things," Lopez Research, 2014, *https://www.cisco.com/web/solutions/trends/iot/docs/smart_cities_are_built_on_iot_lopez_research.pdf*.

12. Daniel Castro and Mark Doms, "Data is the Key to the Factory of the Future," Center for Data Innovation, October 2, 2014, *http://www.datainnovation.org/2014/10/data-is-the-key-to-the-factory-of-the-future/* and Udaya Shankar, "How the Internet of Things Impacts Supply Chains," Inbound Logistics, 2014, *http://www.inboundlogistics.com/cms/article/how-the-internet-of-things-impacts-supply-chains/*.

13. "Finding Success in the New IoT Ecosystem: Market to Reach $3.04 Trillion and 30 Billion Connected 'Things' in 2020, IDC Says," International Data Corporation, November 7, 2014, *http://www.idc.com/getdoc.jsp?containerId=prUS25237214*.

14. Peter C. Evans and Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, November 26, 2012, *http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf*.

15. Robert Atkinson, "ICT Innovation Policy In China: A Review," Information Technology and innovation Foundation, July 2014, *http://www2.itif.org/2014-china-ict.pdf*.

16. Brian Heaton, "Internet of Things Helps Buffalo, Other Cities with Snow Removal," Government Technology, November 19, 2014, *http://www.govtech.com/data/Internet-of-Things-Helps-Buffalo-Other-Cities-with-Snow-Removal.html*.

17. Jenni Spinner, "Headwall inks deal with USAFA on poultry inspection," FoodProductionDaily.com, May 2, 2014, *http://www.foodproductiondaily.com/Safety-Regulation/Headwall-inks-deal-with-USDA-on-poultry-inspection*.

18. Jim Polson, "Water Losses in India Cut in Half by Smart Meters: Itron," Bloomberg, March 15, 2013, *http://www.bloomberg.com/news/2013–03-15/water-losses-in-india-cut-in-half-by-smart-meters-itron.html*.

19. Alan McQuinn, "Commercial Done Companies Fly Away from FAA Regulations, Go Abroad," Inside Sources, September 30, 2014, *http://www.insidesources.com/commercial-drone-companies-fly-away-from-faa-regulations-go-abroad/*.

20. Sandeep Rao, "Medical device approval plagued by unhealthy delays," Baltimore Sun, February 24, 2011, *http://articles.baltimoresun.com/2011–02–24/news/bs-ed-fda-regulations-20110224_1_diseased-heart-valves-cardiology-fda*.

21. Joshua New, "Will Obama be the Last Open Data President?," Center for Data Innovation, November 11, 2014, *http://www.datainnovation.org/2014/11/will-obama-be-the-last-open-data-president/*.

22. Brenna Berman, "2013 Open Data Annual Report," City of Chicago, 2013, *http://report.cityofchicago.org/open-data-2013/*.

23. Josh Taylor, "Chicago's smart city: From open data to rat control," ZD Net, October 15, 2014, *http://www.zdnet.com/chicagos-smart-city-from-open-data-to-rat-control-7000034726/*.

24. Daniel Castro, Ann Cavoukian, "Big Data and Innovation, Setting the Record Strati: Deidentification Does Work," Information Technology and Innovation Foundation, June 16, 2014, *http://www2.itif.org/2014-big-data-deidentification.pdf*.

25. Nick Sinai and Matt Theall, "Expanded 'Green Button' Will Reach Federal Agencies and More American Energy Consumers," White House Office of Science and Technology Policy, December 5, 2014, *http://www.whitehouse.gov/blog/2013/12/05/expanded-green-button-will-reach-federal-agencies-and-more-american-energy-consumers*.

26. Daniel Castro, "The Rise of Data Poverty in America," Center for Data Innovation, September 10, 2014, *http://www2.datainnovation.org/2014-data-poverty.pdf*.

27. Alex Hern, "Google: 100,000 lives a year lost through fear of data-mining," June 26, 2014, *http://www.theguardian.com/technology/2014/jun/26/google-healthcare-data-mining-larry-page*.

28. "Smart Water: wireless sensor networks to detect floods and respond," Libelium, September 5, 2011, *http://www.libelium.com/smart_water_wsn_flood_detection/*.

29. Davey Alba, "This Wearable Detects Pollution to Build Air Quality Maps in Real Time," Wired, November 19, 2014, *http://www.wired.com/2014/11/clarity-wearable* and Martin LaMonica, "Greenbiz 10: What you need to know about the Internet of Things," GreenBiz, May 14, 2014, *http://www.greenbiz.com/blog/2014/05/12/greenbiz-101-what-do-you-need-know-about-internet-things.*

30. Daniel Castro and Travis Korte, "A Catalog of Every 'Harm' in the White House Big Data Report," Center for Data Innovation, July 15, 2014, *http://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-the-white-house-big-data-report/.*

31. Dan Keating, David Fallis, and Andras Petho, "ShotSpotter detection system documents 39,000 shooting incidents in the District," Washington Post, November 2, 2013, *http://www.washingtonpost.com/investigations/shotspotter-detection-system-documents-39000-shooting-incidents-in-the-district/2013/11/02/055f8e9c-2ab1-11e3-8ade-a1f23cda135e_story.html.*

About the Authors

Daniel Castro is the director of the Center for Data Innovation where he leads the Center's research efforts. Mr. Castro is also a senior analyst at the Information Technology and Innovation Foundation. Previously, he worked as an IT analyst at the Government Accountability Office. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Joshua New is a policy analyst at the Center for Data Innovation. He has a background in government affairs, policy, and communication. Prior to joining the Center for Data Innovation, Joshua graduated from American University with degrees in C.L.E.G. (Communication, Legal Institutions, Economics, and Government) and Public Communication.

About the Center for Data Innovation

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. Based in Washington, D.C., the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute proudly affiliated with the Information Technology and Innovation Foundation.

AgTech: Challenges and Opportunities for Sustainable Growth

Ewing Marion Kauffman Foundation—April 2014

Suren G. Dutia

Table of Contents

Foreword

I. Introduction

II. Global Challenges

III. Overview of the AgTech Sector

IV. The Investment Case for AgTech

V. Opportunity for AgTech in the U.S. Heartland

VI. Recommendations

VII. Conclusions

VIII. Acknowledgements

Foreword

The information technology revolution has prompted flights of fancy among some observers who seem to think we have transcended the physical bounds of economic activity. Terms such as the "weightless economy," the "intangible economy," and others suggest that we are moving toward an economy with little connection to the more humdrum things that characterized the economy of yesteryear.

Yet even the intangible economy has an inescapable physical foundation: agriculture. We are still human, after all, and the extent to which we can exploit digital technologies is determined by whether or not we can produce enough food—efficiently and sustainably—to support ourselves. On this single factor, perhaps more than any other, hangs the fate of our economies and societies.

Because of this, our two organizations have supported the production of this white paper, which explores the potential for higher levels of innovation, entrepreneurship, and productivity in agricultural technology (AgTech). The challenges facing agricultural production in the next generation are formidable, and we believe that AgTech requires higher levels of policy attention, public research, and private investment to set agriculture on a path toward greater efficiency and sustainability. Suren Dutia and his colleagues have provided here a good overview of the AgTech landscape, and where untapped opportunities may exist.

The Donald Danforth Plant Science Center's mission is to improve the human condition through plant science. Specifically, the Center's research aims to feed the hungry and improve human health, preserve and renew the environment, and position the St. Louis region as a world center for plant science. Access to its state-of-the-art core facilities gives AgTech businesses a crucial advantage toward achieving success, and its annual Ag Innovation Showcase brings together investors, entrepreneurs, and business leaders to establish new collaborative ventures in agriculture and related industries.

At the Ewing Marion Kauffman Foundation, one of our principal areas of interest is entrepreneurship. We are particularly interested in identifying opportunities for greater entrepreneurial entry and growth in specific sectors of the American economy.

Entrepreneurs are problem solvers, and twenty-first century agriculture has no shortage of problems that, looked at another way, are opportunities for innovation. We look forward to the next steps that follow from this paper, and to recruiting other organizations to join us in promoting entrepreneurship and innovation in AgTech.

Sam Fiorello
Chief Operating Officer and Senior Vice President for Administration
Donald Danforth Plant Science Center

Dane Stangler
Vice President of Research and Policy
Ewing Marion Kauffman Foundation

I. Introduction

In this white paper, we provide an overview of a new emerging economic sector: sustainable agricultural technology or, more simply, "AgTech." This sector has the potential to completely reshape global agriculture, dramatically increasing the productivity of the agriculture system while reducing the environmental and social costs of current ag production practices. Given that we must produce more food in the next forty years than during the entire course of human history to date, and must do so on a planet showing signs of severe environmental stress, AgTech innovations will be absolutely essential. We believe humanity can rise to the occasion and overcome these monumental global challenges, but to do so will require sustained attention, significant investment, and AgTech-specific entrepreneur support systems to help spur innovation in the field.

Our purpose in writing this paper is threefold. First, we seek to increase awareness of the productivity and sustainability challenges of the food system and inspire entrepreneurs to enter the field. Total demand is expected to rise 70 percent by 2050, and current growth rates in agriculture are not sufficient to meet this goal. However, the ag sector faces an even greater challenge because of the uncertainty posed by climate change on future production and constraints posed by the limited availability of land, water, and other key resources. These twin challenges of productivity and sustainability translate to countless opportunities for innovation across the complete value chain, from inputs and agricultural production to transport, processing, distribution, storage, and waste disposal. Visionary entrepreneurs will have the ability to solve pressing societal challenges while capturing the economic value of their new AgTech products and processes.

Our second purpose is to help increase the flow of capital to investments in AgTech. The agriculture sector as a whole is one of the world's largest economic sectors, with net farm income of around $120 billion and farm assets at around $2 trillion with little leverage. Yet there has been relatively little investment in AgTech compared with other industries like clean energy. Venture capital firms compiling portfolios of new AgTech companies are seeing more startups seeking funding than available capital, and other investor groups thus far have not entered the field in significant numbers. Given the size of the potential market and the vital societal need for agricultural innovation, we expect that investors soon will realize the opportunity of AgTech and invest substantially in this emerging field.

Our third purpose is to highlight the need for regional AgTech entrepreneur support systems to accelerate innovation. We believe that the American heartland provides an ideal example of a region poised to make great strides forward in developing an entrepreneurial sector for AgTech. The heartland has some of the world's best growing conditions and natural resources, and currently produces 27.2 percent of the world's corn, 29.75 percent of its soybeans, 6.7 percent of its beef, and 6.9 percent of its pork, making this region an epicenter of global agricultural activity. The heartland houses some of largest and most progressive agricultural companies in the world, looked upon as leaders in their field. The heartland is blessed with highly developed transportation networks along its waterways and railroads, allowing for efficient logistics and transport of ag products. In addition, the heartland has world-class AgTech research capabilities with its land-grant universities and city-level clusters of expertise, such as plant sciences in St. Louis and animal sciences in Kansas City. Given the overall AgTech entrepreneurial activity in the region and the large number of significant multinational players, the American heartland can be a powerful influence in driving the objectives of the AgTech revolution. Taken together, these resources indicate a regional competitive advantage in AgTech, similar to what the Silicon Valley cluster has provided for the IT industry. For these reasons, we believe a concerted effort to develop a regional AgTech entrepreneurial support system will result in immense benefits for the region itself and set an example for other agricultural communities across the world.

We hope this paper launches a larger dialogue on the monumental challenge of sustainable food production for the next forty years and opportunities for the AgTech sector to help solve this challenge. We look forward to hearing your thoughts and ideas on these important topics.

II. Global Challenges for Agriculture: Producing More With Less Impact

> *Over the next 40 years, land, energy, water, and weather constraints will place unprecedented pressure on mankind's ability to access its most basic goods—food, fuel, and fiber. Humanity must now produce more food in the next four decades than we have in the last 8,000 years of agriculture combined. And we must do so sustainably.* ("The 2050 Criteria," World Wildlife Fund)

The global agricultural system faces tremendous challenges. The United Nations Food and Agriculture Organization (UN FAO) projects that food production must increase by 70 percent over the next forty years to satisfy increasing demand due to population growth and rising economic prosperity (Conforti, 2011). The main challenge of global agriculture often is framed in terms of feeding a growing population, which is expected to increase from seven billion people today to approximately nine billion in 2050.

At the same time, there is limited opportunity to expand the land used in agricultural production, and agriculture also must deal with environmental risks such as climate change. To succeed in sustainably increasing food production, major innovations in AgTech are required that increase agricultural productivity and improve the efficiency and resiliency of the entire food system.

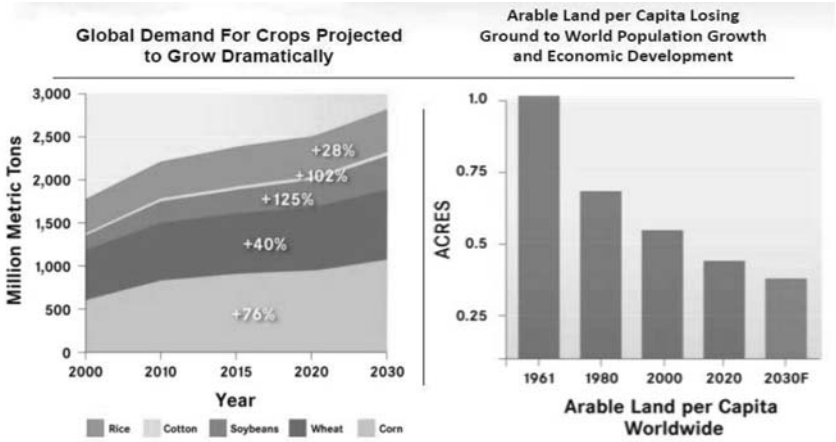


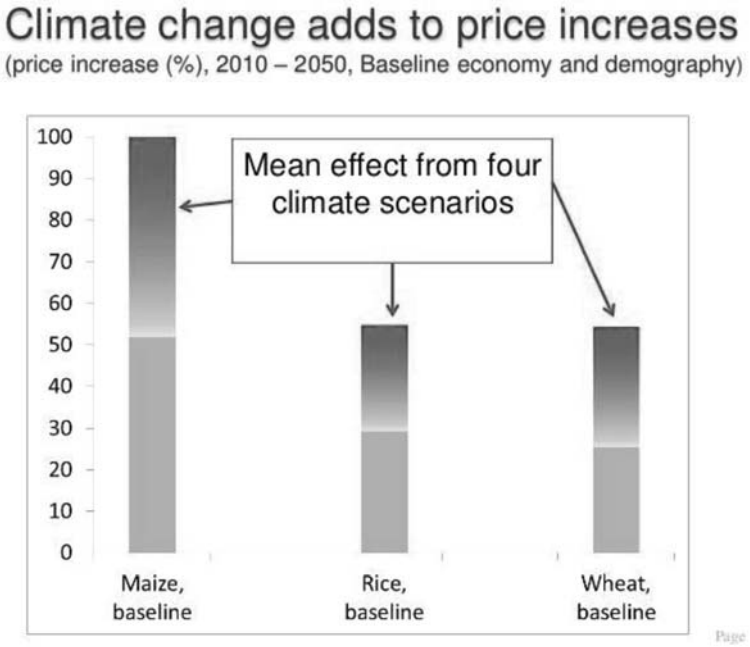
Figure 1. Projections for rising global demand for crops and declining arable land per capita.

While many variables will determine the food demanded in 2050 and the ease with which that food can be produced, the general trends suggest that we will need significantly more food while facing an increasingly hostile environment due to climate change and diminishing resources. Projections from IHS Global Insights show large increases in the global demand for corn and soybeans, while the amount of arable land per capita continues to decline due to population growth and urban development. The UN FAO projects that both per capita and total demand for cereals, meat, and oil crops will rise by 2050, with little increase in the amount of arable land. Climate change will pose a large challenge to these projections: the International Food Policy Research Institute (IFPRI) projects that climate change impacts will nearly double the price of corn, rice, and wheat. Figures 1–3 showcase these projections.

Key Variables Influencing Agricultural Production from UN FAO's "World Agriculture Towards 2030/2050: The 2012 Revision"

	2005/2007	2050
Population (million)- UN 2008 Revision	6 592	9 150
Population (million)- UN 2010 Revision	*6 584*	*9 306*
kcal/person/day	2 772	3 070
Cereals, food (kg/capita)	158	160
Cereals, all uses (kg/capita)	314	330
Meat, food (kg/capita)	38.7	49.4
Oilcrops (oil. equiv.), Food (kg/cap)	12.1	16.2
Oilcrops (oil. equiv.), all uses (kg/cap)	21.9	30.5
Cereals, production (million tonnes)	2 068	3 009
Meat, production (million tonnes)	258	455
Cereal yields (tonnes/ha; rice paddy)	3.32	4.30
Arable land area (million ha)	1 592	1 661

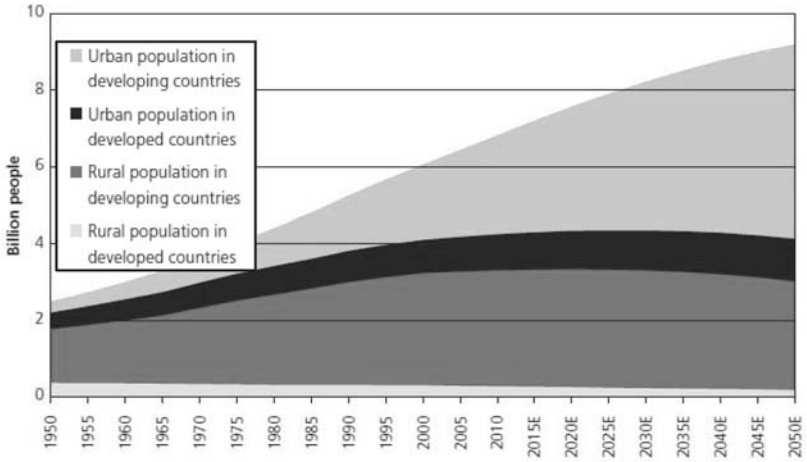
Source: HIS Global Insights, Agriculture Division.
Figure 2. Projections for key agricultural variables in 2050.



Source: IFPRI, "Food Security, Farming, and Climate Change to 2050," policy seminar, December 1, 2010.
Figure 3. Projected impact of climate change on crop prices.

Recently, Oxfam commissioned modeling to make estimates about what food prices would look like twenty years from now, and determined that under normal circumstances, food commodity prices are likely to increase about 50 percent between now and 2030. And if estimates of climate change are factored in, food prices could be up to 100 percent higher than they are at present. This would put enormous pressure on the world's population and especially its poor.

Source: World Population Prospects: The 2010 Revision. United Nations, New York, 2011.



Source: Alexandratos & Bruinsma, "World Agriculture Towards 2030/2050: The 2012 Revision," UNFAO, 2012.

Figure 4. UN projections for urban and rural changes in population *Projected changes in global mean consumption*

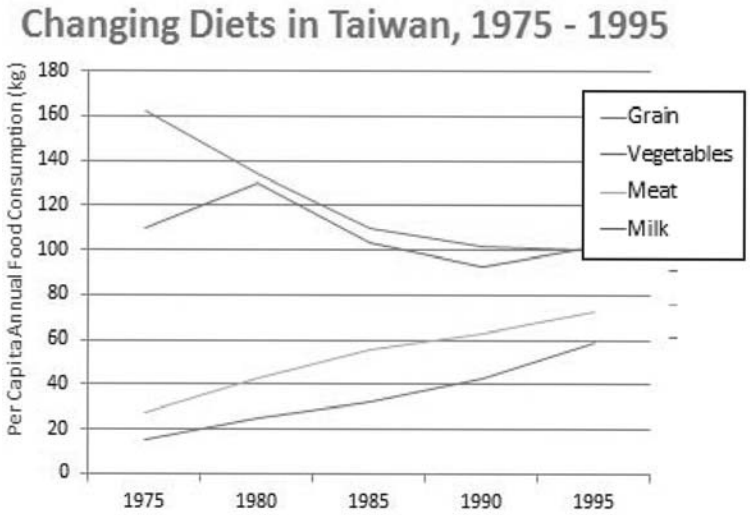
The Key Demand Drivers: Population Growth, Rising Incomes, and Demand for Renewable Energy

However, the food shortfall challenge will be made even more difficult by the demographic shift in incomes occurring as the population rises; not only will there be more people overall, but more wealthy people who demand more food with greater resource requirements.

Figure 4 shows that the fastest growing segment of world population is urban in the developing world. Billions of people already have moved from the rural country side into rapidly growing megacities, and billions more are expected to make this transition over the next forty years.

As they gain affluence through rising incomes, the emerging middle classes of the developing world are consuming more meat, fish, dairy, and processed foods, all of which require higher levels of input resources and much higher levels of overall agricultural production.

As a case study of rising affluence driving changes in dietary preferences, consider Taiwan. Between 1975 and 1990, Taiwan's GNI per capita rose from $3,368 to $8,325. In this same period, per capita annual meat consumption rose from 30 kg to 70 kg (see Figure 5). A similar trend emerged in China over the past thirty years, with annual per capita meat consumption growing from 9 kg to 58.2 kg.



Sources: Taiwan Council of Agriculture, China Statistical Yearbookand Nomura Global Economics.

Figure 5. Changing dietary preferences in Taiwan.

A consequence of this rapid growth in meat intake is that China now consumes twice as much meat as the United States. Figure 6 shows the total consumption of meat in China relative to the United States. While Chinese per capita meat consumption currently sits at 58.2 kg per year, U.S. per capita meat consumption is double that at 120.2 kg per year. With increasing populations, even small shifts in meat consumption in the developing world can have large aggregate impacts on total demand.

Source: Basch *et al.,* "Harvesting Opportunities for a Sustainable Food Supply."

Figure 6: Total meat consumption in the United States and China.

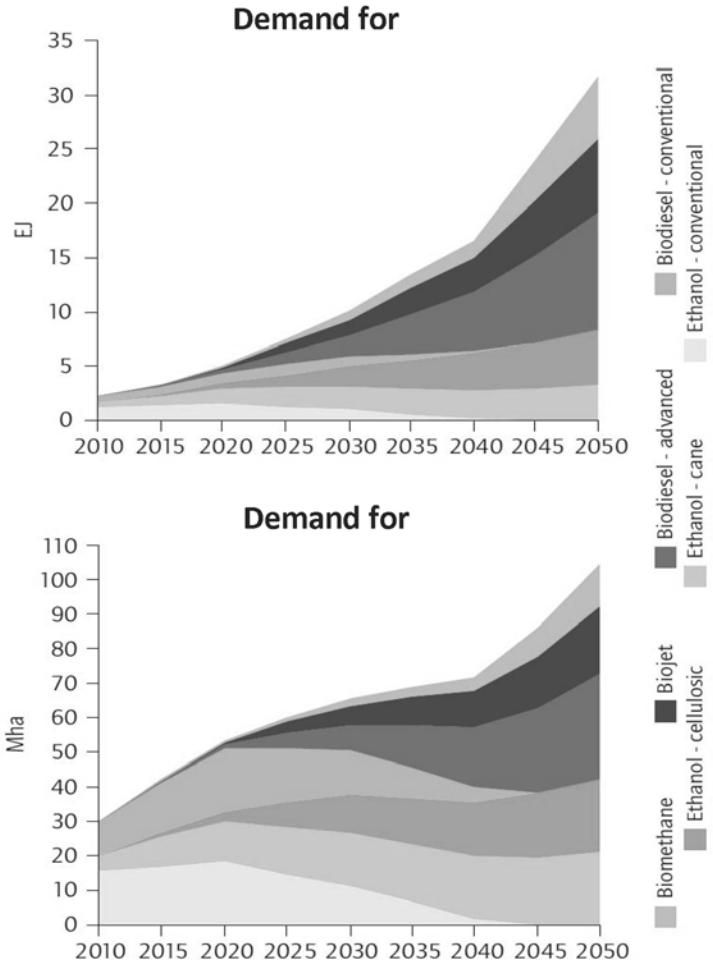
Increased demand for meat poses a host of challenges to the global agricultural system, as livestock requires up to 8 kilograms of feed for every kilogram of meat produced (see Figure 7 for requirements based on type of meat). Significantly more water is required to produce a kilogram of meat than a kilogram of plant crops.

Protein Source	Number of kg of feed required for every kg of meat
Beef	8
Lamb	5
Pork	2.5
Poultry	1.5
Fish	1.2

Source: Basch *et al.,* "Harvesting Opportunities," SAM Robeco 2012.
Figure 7. Animal feed requirements per kg of protein.

Meat production's high energy, water, and other resource costs thus lead to direct competition between crops grown for direct human consumption and crops grown as inputs for raising livestock or fish in aquaculture.

Biofuels also will be a huge source of competition for diminishing resources available for food production. According to the International Energy Agency, biofuel production will see an 800 percent increase between now and 2050. While much of that biofuel will come from nonfood crops and second-generation production techniques such as cellulosic ethanol, most of the current supply of biofuels and production in the near term will provide direct competition with resources used to grow crops for human consumption and feed for livestock. Projected growth in biofuel demand also is expected to require more than triple the land currently used for production, as shown in the bottom graph of Figure 8, further intensifying competition between food crops and biofuel crops.



Source: International Energy Agency, "Technology Roadmap: Biofuels for Transport," 2011.
Figure 8. Demand for biofuels (top) and resulting demand for land (bottom).

Planetary Boundaries and the Risk Posed to Agriculture

In order to continue sustainably, agriculture must exist within a stable environment. Like other biological systems, agriculture is dependent upon earth's biosphere for resources, such as water and soil. Much of current agriculture also is dependent on manmade inputs like synthetic fertilizer. However, global environmental challenges threaten the sustainability of these inputs.

Recent advances in earth systems science have yielded a new understanding of processes that threaten the stability of the earth's current biosphere conditions. A landmark 2009 study in the journal *Nature* first proposed the concept of "planetary boundaries," geophysical thresholds that, if crossed, could be dangerous for humanity (Rockstrom *et al.,* 2009). Some of these planetary boundaries, such as climate change and biodiversity loss, are fairly well known. Other boundaries, such as the nitrogen cycle and global land use change, have received relatively little attention as issues of global concern. The full list of planetary boundaries and their proposed constraints is included in Figure 9 below.

PLANETARY BOUNDARIES Ag activities impact the six starred planetary boundaries.

	Earth-system process	Parameters	Proposed boundary	Current status	Pre-industrial value
*	Climate change	(i) Atmospheric carbon dioxide concentration (parts per million by volume)	350	387	280
		(ii) Change in radiative forcing (watts per metre squared)	1	1.5	0
*	Rate of biodiversity loss	Extinction rate (number of species per million species per year)	10	>100	0.1–1
*	Nitrogen cycle (part of a boundary with the phosphorus cycle)	Amount of N_2 removed from the atmosphere for human use (millions of tonnes per year)	35	121	0
*	Phosphorus cycle (part of a boundary with the nitrogen cycle)	Quantity of P flowing into the oceans (millions of tonnes per year)	11	8.5–9.5	-1
	Stratospheric ozone depletion	Concentration of ozone (Dobson unit)	276	283	290
	Ocean acidification	Global mean saturation state of aragonite in surface sea water	2.75	2.90	3.44
*	Global freshwater use	Consumption of freshwater by humans (km^3 per year)	4,000	2,600	415
*	Change in land use	Percentage of global land cover converted to cropland	15	11.7	Low
	Atmospheric aerosol loading	Overall particulate concentration in the atmosphere, on a regional basis		To be determined	
	Chemical pollution	For example, amount emitted to, or concentration of persistent organic pollutants, plastics, endocrine disrupters, heavy metals and nuclear waste in, the global environment, or the effects on ecosystem and functioning of Earth system thereof		To be determined	

Source: Rockstrom *et al.,* "A Safe Operating Space for Humanity," *Nature* 461 (2009).
Figure 9. Planetary boundaries relevant to the global agriculture system.
* *Proposed Planetary Boundaries (starred are relevant to ag, red have been crossed)*

Six of the proposed planetary boundaries are especially relevant to global agriculture:

- *Climate change:* modern agriculture produces several greenhouse gases, including carbon dioxide, methane, and nitrous oxide. Agriculture contributes 13.5 percent of global GHG emissions (IPCC, 2007).
- *Biodiversity loss:* agriculture depends on a unique ecosystem of bacteria, fungi, and other microorganisms present in the soil, and this ecosystem often is disrupted by modern agriculture activities.
- *Nitrogen cycle:* the production of nitrogen-based fertilizer through the Haber-Bosch process removes roughly four times the atmospheric N_2 recommended in the proposed boundary.
- *Phosphorus cycle:* the mining of finite sources of P and its concomitant application as fertilizer with subsequent erosion into rivers, estuaries and oceans. Nitrogen and phosphorus contribute to eutrophication.
- *Global freshwater use:* freshwater usage can grow only by 1,400 km − 3 per year, and agricultural production accounts for roughly 92 percent of total human water usage (Hoekstra & Mekonnen, 2012).
- *Global land use:* agricultural cropland is 11.7 percent of total global land cover and must not exceed 15 percent, leaving limited land available for agricultural expansion.

Demand for food, fiber, and energy will continue to rise throughout the coming decades, and agriculture's impact on planetary boundaries also likely will rise. How-

ever, crossing the planetary boundaries is not sustainable in the long term, as it will trigger geophysical shifts that will decrease agricultural production and lead to other devastating impacts. Ultimately, humanity must operate within the planetary boundaries to allow for a stable global environment and a sustainable civilization.

AgTech innovations can help to reduce or even eliminate the negative global environmental impacts of agriculture by reducing the fossil fuel, fertilizer, water, and land requirements for food production. Increasing resource efficiency can help to ensure a more sustainable and more productive food system.

The Dream of the "Evergreen Revolution"

The goal of increasing agricultural production by 70 percent while not pushing the global environment beyond the nine planetary boundaries presents an unprecedented challenge for humanity. We believe innovation in AgTech has the potential to meet both of these challenges, but we will need a new revolution in sustainable agricultural production for this to happen.

The Green Revolution of the mid-twentieth century provides a recent example of what can happen through technological innovation. In the 1960s, scientists grew increasingly concerned about the growing world population and warned that mass famines were imminent. Yet since 1960, the world population has doubled while the food supply has tripled (UN Food and Agriculture Organization, 2012). Even more astounding, land under cultivation only grew by 12 percent from 1960 until today; most of the growth in yields came from increases in productivity. The Green Revolution saved many ecosystems from destruction, for without this dramatic increase in productivity, hungry nations likely would have converted more rainforests and wetlands to cropland.

However, the Green Revolution had large environmental consequences. Improvements in yields from the Green Revolution required heavy usage of fertilizer, disrupting the nitrogen cycle and leading to eutrophication and "dead zones" of oxygen-deprived, largely lifeless areas in the ocean. Green Revolution increases in yields also relied on chemical herbicides and pesticides, contributing to local air and water pollution. In addition, Green Revolution crops demanded large amounts of irrigated water, which in some areas has dramatically lowered water tables and depleted aquifers. Finally, the various technologies used in the Green Revolution, from fertilizer to herbicides to irrigation, all require large amounts of fossil fuel energy, leading to further greenhouse gas emissions and climate change.

Our new agricultural revolution must be an "evergreen revolution," one that increases food production while ensuring environmental sustainability. It must go further than reducing agriculture's negative impacts; ultimately, agriculture must positively contribute to the global environment.

Johan Rockstrom, lead author of the group of scientists who created the planetary boundaries concept, proposes the following global goals for an "evergreen revolution" (Rockstrom & Karlberg, 2010) in Figure 10 below:

Goals for an "Evergreen Revolution"

Food Production: increase total food production by 70 percent by 2050.

Climate: turn global agriculture from a net carbon source to a carbon sink.

Nitrogen: reduce yearly atmospheric N_2 converted to fertilizer by 75 percent.

Water: keep global consumption of freshwater below 4,000 km^3/year. Current consumption is 2,600 km^3/year, leaving 1,400 km^3 remaining.

Land use: cropland can only expand from 12 percent to 15 percent of Earth's surface.

THE MAIN TAKEAWAY:
Sustainable higher yields must be achieved by increasing productivity.

Source: Rockstrom & Karlberg, "The Quadruple Squeeze: Defining the safe operating space for freshwater use to achieve a triply green revolution in the Anthropocene," Ambio 39 vol. 3 (2010), 257–65.

Figure 10. Global goals for an "evergreen revolution" in agriculture.

Meeting these goals requires AgTech innovations that can produce food with significant improvements in resource efficiency. To put it another way, we will need to produce more units of output with fewer units of input. Through innovations along the entire agriculture value chain, we can increase the productivity of our farming systems while simultaneously transforming agriculture into a source of environmental health. But achieving the dream of the evergreen revolution will not be easy; it will require sustained investment, increasing collaboration and enlightened public policy. We also must know the current progress of innovations in AgTech, the subject of the next section of this paper.

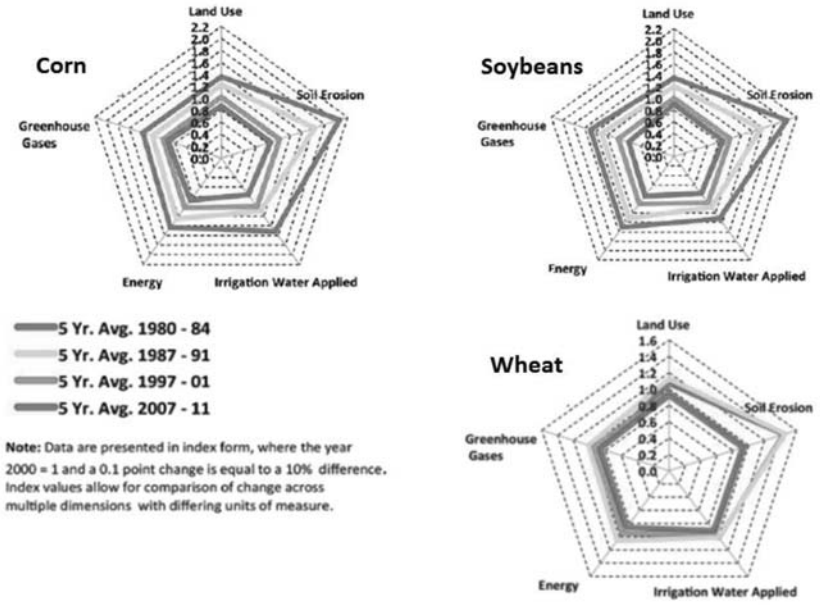
III. An Overview of the AgTech Sector

The global imperatives presented by the soaring demand for food and the danger of crossing planetary boundaries underscore the need for an "evergreen revolution" in agriculture. This revolution largely will be driven by innovations in sustainable agriculture technologies. In this paper, we refer to this sector as "AgTech," with a clear implication of environmental, social, and economic value. AgTech describes innovative technologies in the agricultural sector that demonstrably enhance the sustainability of the practice by increasing productivity, improving the efficiency of resource use, and reducing ecological impacts. They also yield sustained or enhanced profitability to investors by increasing the long-term value of ag production.

Global agricultural production is far from monolithic, and involves many different production methods ranging from the advanced technology and high-yield mainstream U.S. model to low-yield subsistence farming, with many variations in between. In this paper, we will focus solely on advanced technology agricultural production, as we believe that this is the best method to produce 70 percent more food while also respecting the planetary boundaries for climate change, biodiversity, nitrogen, water, and land. With this focus, our view of AgTech will center on North America, where adoption of advanced technology for agriculture is most prevalent.

Recent trends in U.S. agriculture illustrate the potential for improvements in AgTech to move us toward meeting the global imperatives of the "evergreen revolution." Figure 11 indicates changes in environmental impact of three U.S. crops (corn, soy, and wheat) over the last twenty-five years. While productivity has risen for these three crops, the environmental impact of growing them has decreased. Corn and soybeans show greater improvement than wheat because of the adoption of biotechnology products and techniques made possible by these products, such as no-till agriculture.

However, these diagrams also represent the environmental impact per unit of production, meaning that as production has increased, the total aggregate environmental impact still has continued to rise. As the planetary boundaries framework shows, rising aggregate environmental impacts are not sustainable. Further innovations in AgTech will be necessary if the U.S. agriculture sector is to achieve full environmental sustainability at the production levels needed to meet the world's growing demand.



Source: Field to Market, *2012 Environmental and Socioeconomic Indicators Report.*

Figure 11. Resource efficiency and environmental sustainability improvements for three U.S. crops.

The AgTech Value Chain

In order to better understand the potential for AgTech innovations, we crafted an AgTech value chain diagram that traces inputs to their final products. This value chain contains seven intermediary steps: physical inputs, information inputs, plant farming, animal farming, bio-based processing, food processing, and logistics (see Figure 12). The value chain can produce three final products: fossil-fuel substitutes (such as biofuel), plant-based food, and animal-based food. Each of the steps in the supply chain has inefficiencies and environmental impacts that must be improved if global agriculture is to reach the goals of an "evergreen revolution." Thus, each step in the value chain has the potential for innovation.

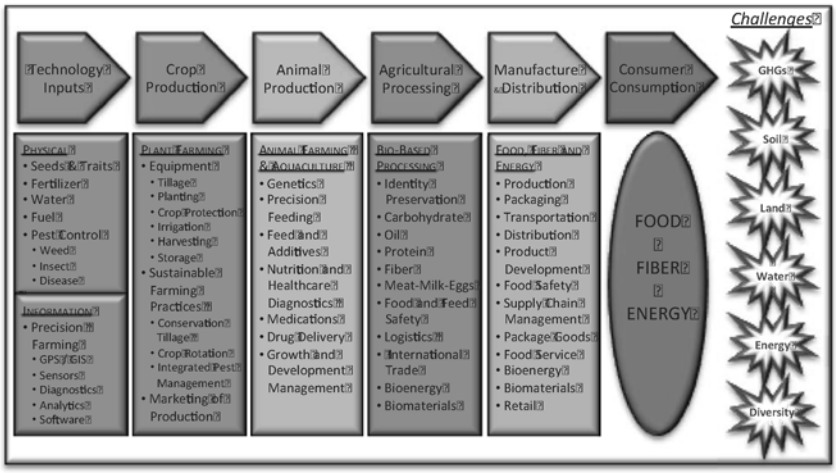
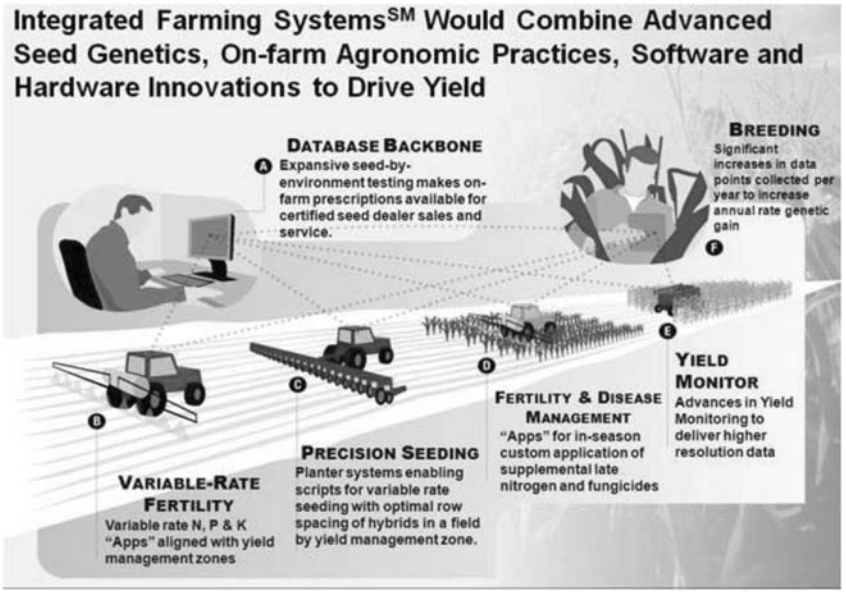


Figure 12. The AgTech value chain.

One Vision for AgTech: Integrating Genetics, Physical Inputs, IT, and Smart Machinery

Innovations in AgTech do not need to be constrained to only one step in the value chain; rather, the most disruptive breakthroughs in AgTech may come from combining innovations in multiple areas. One particular exciting illustration of this combination is an idea known as "integrated farming systems" that will integrate genetics, physical inputs, IT sensing, and smart machinery. Through advances in software and environmental testing, farmers will be able to create custom field prescriptions for seeds, fertilizer, pest controls. Smart machinery then will carry out the prescribed treatment, all the while collecting further data that will provide feedback to the farmer. This data also will allow seed and farm input companies to develop custom products for farmers. Figure 13 demonstrates this AgTech vision.

The idea of "integrated farming systems," which currently is being advanced by several established companies and by entrepreneurs, still is in early development. This idea of combining advances in genetic engineering, information technology, and smart machinery likely will be pursued by many established companies and startups due to the vast potential for investment and innovative new products in these three areas.



Source: "Precision Planting/Monsanto Field Scripts program," *Precision Planting* 2012.

Figure 13: An illustration of "Integrated Farming Systems," a vision of potential AgTech innovations.

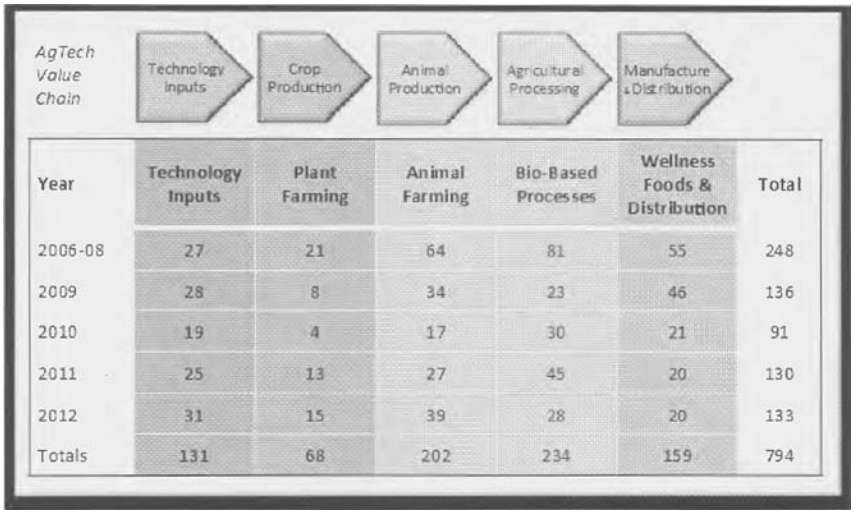
Examples of AgTech Startup Activity

To provide an overall state of the innovation ecosystem for AgTech, we analyzed a dataset from the agriculture venture capital group Cultivian of over 900 AgTech startup companies from around the world. This dataset consists of companies that Cultivian considered investing in for their funds, and was obtained through direct contact, conferences, referrals and other methods. We have removed any identifying information from the data and present only aggregate information.

We categorized each of the startup companies by its position in the AgTech value chain. After sorting the data, we were left with 738 companies that fit within the value chain framework. The database also contains the year that Cultivian first became aware of the venture or when the venture was seeking investment. We used this as a proxy to signify the year when the venture perceived itself as mature enough to seek funding. From this data, we created Figure 14, which summarizes Cultivian's deal flow from 2006 until 2012.

From this dataset, it is evident there is robust stream of new business startup activity occurring across the agricultural value chain in technology inputs, crop production, animal production, processing, and manufacture and distribution. This in-

novation activity has occurred over a sustained period of six years, averaging 132 startups per year for a single venture firm.



Year	Technology Inputs	Plant Farming	Animal Farming	Bio-Based Processes	Wellness Foods & Distribution	Total
2006-08	27	21	64	81	55	248
2009	28	8	34	23	46	136
2010	19	4	17	30	21	91
2011	25	13	27	45	20	130
2012	31	15	39	28	20	133
Totals	131	68	202	234	159	794

Figure 14. Summary of Cultivian AgTech dataset.

To showcase some of the many innovation opportunities in the AgTech sector, we chose four examples of startup companies from different steps in the AgTech value chain. The quoted description for each company comes directly from Cultivian's portfolio website.

Information Technology Inputs
AquaSpy: IT and irrigation

"AquaSpy develops, manufactures, markets and distributes moisture sensors and smart information technology for the irrigation market. Its intelligent water monitoring systems have broad agricultural applications and are designed to help farmers manage and reduce irrigation costs."

Physical Technology Inputs
Divergence: Genomics and pest control

"Divergence is a research and development company employing comparative and functional genomics to identify compounds, proteins, and genes to control parasitic nematode infections in plants, animals, and people." Divergence was wholly acquired by Monsanto in 2011.

Plant Production
Harvest: Robotics for ag activities

"Harvest develops novel robotics and materials handling systems for agriculture and greenhouse applications."

Bio-Based Processing
Allylix: Bio-based production technique of terpenes

"Allylix Inc. develops terpene products and their derivatives for the flavor and fragrance, food ingredient, pharmaceutical, agricultural and biofuel markets. Allylix's technology produces high-value natural terpenes in greater quantities, of higher quality, and at significantly lower cost than traditional sources."

While we believe that these four companies are a good representation of the diversity of activity in the AgTech sector, the inclusion of these companies should not be taken as an endorsement.

AgTech and the Controversy Surrounding Genetically Modified Foods

We would be remiss if we did not acknowledge an ongoing debate around genetically modified (GM) foods. GM foods have been sold commercially for about two decades in the United States and there is broad scientific consensus that GM foods do not pose greater risk than conventional foods. However, a simmering debate remains about the potential adverse impacts these products could have on the environment and human health, with public opinion deeply divided over safety concerns.

While we recognize the importance of reviewing a wide range of scientific studies and opinions on the use of GM foods, it is beyond the scope of this white Paper. However, we should note that no major scientific body ever has found that GM foods pose a risk to public health. The U.S. National Academy of Science noted that after billions of meals served with GM ingredients, "no adverse health effects attributed to genetic engineering have been documented in the human population." European scientific agencies agree with this conclusion, and the scientific advisor to the European Commission has stated that "there is no more risk in eating GMO food than eating conventionally farmed food."

Further, scientific analysis of the environmental impact of GM crops has, to date, not found evidence of environmental harm caused by the products. Instead, a U.S. National Academy of Science 2010 report, "Impact of Genetically Engineered Crops on Farm Sustainability in the United States," found that GM crops reduced agriculture's environmental impact, reducing insecticide and toxic herbicide use; increasing the use of conservation tillage and no-till farming; reducing carbon emissions and soil runoff; and improving soil quality. Given the monumental challenge of sustainably producing 70 percent more food over the next forty years, we believe that no potential tools should be excluded. Without the use of GM foods or other biotech products, meeting the global agriculture challenge will become significantly more difficult.

As outlined in this paper, it is our strong belief that during the twenty-first century, humankind will be confronted with an extraordinary set of challenges. It is essential that we improve food, feed, fiber, and energy production while reducing environmental impact and enhancing societal development. Meeting these challenges will require new knowledge generated by continued scientific advances, the development of appropriate new technologies, and a broad dissemination of this knowledge and technology, along with the capacity to use it, throughout the world. It also will require that wise policies be implemented through informed decision making on the part of national, state, and local governments in each nation. Regulatory oversight of technology development should continue to be science-based, while recognizing the responsibility of government, industry, and the scientific and medical communities to educate the public and improve availability of unbiased information.

Genetically modified foods have the potential to solve many of the world's hunger and malnutrition problems, and to help protect and preserve the environment by increasing yield and reducing reliance upon chemical pesticides and herbicides. Yet there are many challenges ahead for governments, especially in the areas of safety testing, regulation, international policy, and food labeling. Many people feel that genetic engineering is the inevitable wave of the future and that we cannot afford to ignore a technology with such enormous potential benefits. However, we must proceed with caution to avoid causing unintended harm to human health and the environment as a result of our enthusiasm for this powerful technology.

The AgTech space has the unique opportunity to gain ground by counteracting the fearmongering about genetically engineered crops and bringing about more openness, education, and transparency while working with farmers and innovators. While biotech advances in medicine and pharmaceuticals have been well received by the public, individuals view innovations in plants and food more skeptically. We must bring about a broad-based understanding of the enormous challenges that lie ahead to create meaningful change. It is essential to bring a congruence of pragmatic innovators, humanitarians, and environmental organizations together with entrepreneurs and ag companies to achieve the common objective of producing adequate food for the next century.

IV. The Investment Case For AgTech

The AgTech sector has tremendous opportunities for investment. The demand for sustainable food, fiber, and energy production has been growing throughout the twenty-first century, making agriculture a stable and reliable investment. Below are five reasons why we believe AgTech innovation is a smart investment:

1. Grain consumption is increasing worldwide.
2. Demand for sustainable energy is growing.
3. Access to quality arable land and soil is constrained.
4. Access to adequate water quality and quantity is decreasing.
5. Current cultural practices are not sustainable in the face of increasing environmental challenges.

Figure 15 provides a glimpse of the various demand drivers and supply constraints for the entire agriculture system. Because of the factors shown on the figure's right side, demand for agricultural products will continue to rise, while the supply constraints will make meeting the demand extremely difficult. AgTech innovations that help meet these challenges will offer investors and entrepreneurs a fertile opportunity for investment and invention.

Figure 15. Demand drivers and supply constraints in the agricultural system.

Logistics, which coordinates the movement of ag products and support availability and the timely balance of supply and demand, is another area essential to the success of AgTech innovations. Because of its critical role, we have given logistics special prominence in the above graphic.

Some Areas of Opportunity for Ag Tech Investment

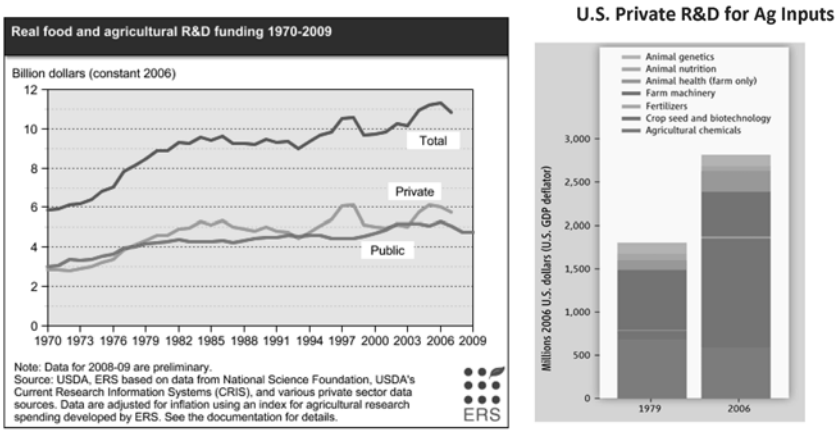
The AgTech sector holds many opportunities for investment, with innovation needed throughout the entire value chain. Specific areas available for investment in this sector include:

- Animal Nutrition & Health
- Aquaculture
- Bioenergy
- Biological Pest Control
- Biomaterials
- Bionutrition
- Biotechnology
- Crop Nutrition
- Crop Protection
- Decision Support Technologies
- Feed Efficiency
- Fertilizer Efficiency
- Food Traceability and Safety
- Food Storage and Preservation
- Information Systems
- Integrated Pest Management
- Irrigation Efficiency
- Land Management
- Machinery
- Precision Agriculture
- Robotics
- Seeds and Genetics

- Soil Amendments
- Soil Health
- Sustainable Production Systems
- Technology Transfer
- Urban Agriculture
- Water Quality and Preservation
- Waste Mitigation and Manure Management

Changes in U.S. Public and Private AgTech R&D Spending

Throughout most of the twentieth century, much research and innovation in agriculture was funded with public money. Since the early 1980s, however, public expenditures on agriculture R&D have stagnated, even as demand for ag products continues to rise. As public funding has ebbed, new flows of capital from the private sector have increased. This is particularly evident in developed countries like the United States, where private spending on agriculture R&D has been consistently higher than public spending for the past three decades. The decline in public R&D is a trend affecting primary research in the United States for all types of science and is not just an issue for AgTech. However, the needs and opportunities present in the AgTech sector deserve special attention from policymakers (see Figure 16).



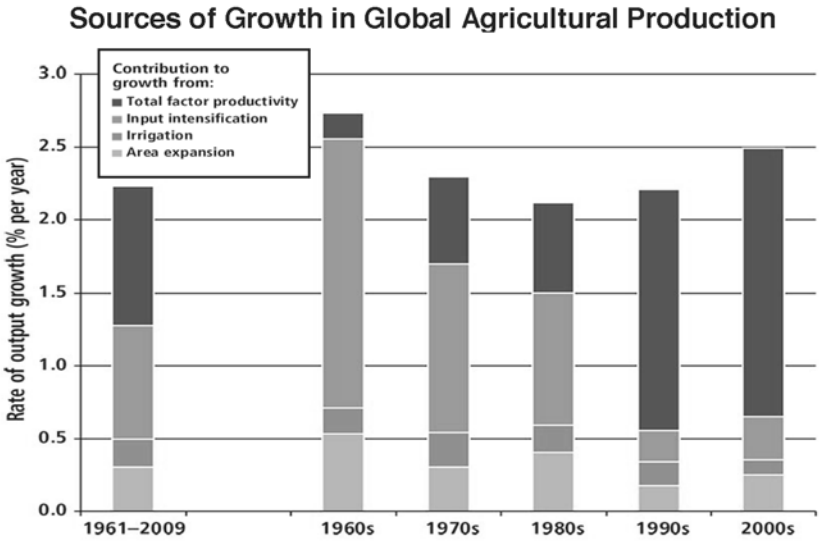
Sources: (above left) USDA, "Background: Agriculture Depends on Research and Technology Development," 2012; (above right) Fuglie *et al.,* "The Contribution of Private Industry to Agricultural Innovation," *Science* 338, no. 6110 (2012).

Figure 16. Trends in public and private AgTech R&D spending in the United States.

The growth of private R&D spending on AgTech illustrates a simple and, on its face, obvious point: investing in AgTech offers solid opportunities for innovation and value creation. Corporations and private investors largely are rational in their decision making, generally only investing capital when they have a high degree of confidence of a good return. When entrepreneurs and private industry develop business models that capture the value of needed AgTech innovations, they have a tremendous opportunity to achieve high returns. Indeed, this has happened with the development of biotechnology. The right-hand graphic in Figure 16 shows the dramatic increase in private R&D spending in crop seed and biotechnology between 1979 (shortly before the U.S. Supreme Court allowed for patenting of biotechnology traits) and 2006; this research spending occurred because of the opportunity to capture value from novel applications of genetic engineering.

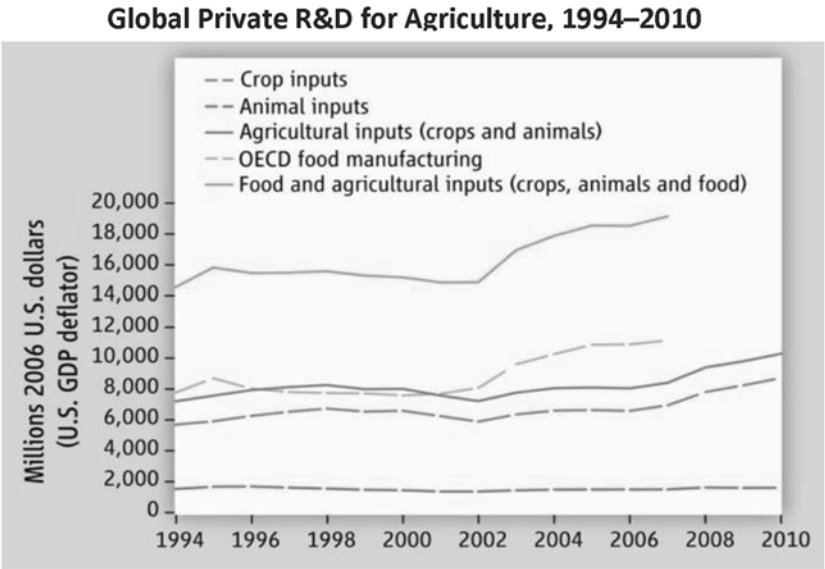
The Important Contribution of Private R&D Spending to Global Agricultural Growth

Global gains in agricultural productivity realized during the Green Revolution of the 1960s, 1970s, and 1980s were driven by input intensification and crop-area expansion. In comparison, the productivity gains achieved in the 1990s and 2000s largely were driven by innovations (total factor productivity) and less from input intensification or new land being brought into cultivation. Figure 17 highlights the shift away from heavy spending on increasing fertilizer and pesticide inputs to investments in genetic engineering and other high-tech improvements that increased yields with fewer units of input. This trend towards greater resource efficiency is encouraging, but much more needs to be done.



Source: Fuglie *et al.*, "Productivity Growth and Technology Capital in the Global Agricultural Economy," *Productivity Growth in Agriculture* 2012.
Figure 17. Relative contributions to growth in global agricultural production.

With public R&D spending in advanced developed countries stagnating or declining, private investment may be the best way to spur further innovations in AgTech and achieve the growth in production needed to sustainably meet the rising demand for ag products. Figure 18 demonstrates that private sector investment in food and agriculture has increased steadily in the past decade, reaching $8 billion annually for crop inputs and $2 billion annually for animal inputs by 2010. However, private investment must increase even further if advances in innovation are to continue.



Source: Fuglie et al.
Figure 18: Global private investment in food and agriculture research.

Overall Comments on the Future of AgTech Investment

As can be seen from the top-level investment data in Figure 18 and the micro-level Cultivian data, AgTech investments are being made across the supply chain. There also are interrelationships between supply chain categories. For example, the value of new seed traits may not be fully realized without other equipment and information innovations needed to advance precision agriculture. Additionally, advances in logistics will be needed to segregate outputs as crops become optimized for specific uses such as animal production, human nutrition, or bio-based substitutes. Further, as climate change negatively affects current production methods, still more innovations will be needed.

Crucially, demand necessitates innovations. Over the past five years, innovations in agriculture technology (precision ag innovations, data analytics and processing, platforms for the collection and distribution of complex data streams, and IT-driven extensions) are on the rise in the heartland, and in California and North Carolina. Pressing needs and challenges often fuel research and innovative outcomes in various global farming hubs. New Zealand is one of the world's largest producers of dairy as well as lamb and sheep, while Australia is a leading producer of wheat and animal feed. Investment authorities and private wealth funds from Singapore, Dubai, and Qatar are beginning to take notice of geographic centers with farming capabilities, including those in China, Brazil, and Chile.

Government policies, regulations, incentives, and penalties will play an important role in determining the AgTech sector's future. It either could result in growth spurts or constrain innovation and entrepreneurial activity in the sector, and investors will need to stay abreast of how these are impacting returns.

We also want to highlight a potential trend where investors may have a more diverse set of return motivations. Economic returns still dominate, but goals relating to social consciousness and environmental returns also are on the rise. These types of returns always have existed and historically have received philanthropic and government support. However, new sources of capital are emerging that seek environmental and social returns or, at least, having these returns blended with economic returns, including: social entrepreneurship innovations funded by socially conscious investors; declared socially conscious corporations; socially conscious innovator and corporation partnerships; consumers making purchasing choices based upon environmental and social factors; crowd funding; and others. As these trends gain momentum, there may be opportunities in the AgTech sector to translate shared social returns to individual economic returns.

Overall, we see the AgTech sector evolving through an increasing number of agriculture technology entrepreneurs connecting with angel, venture capital, corporate, philanthropic, government, and other investors to create an even more vibrant sector within the global economy. We foresee many "green" opportunities across the supply chain categories to suit the size and characteristics of different entrepreneurs and investor classes. The attributes of a potential investment opportunity and associated return on investment also will be key. As always, the most disruptive and quickly scalable breakthroughs will deliver the most handsome economic, social, or environmental returns. Investors and entrepreneurs will have many opportunities to collaborate given the magnitude of the need and the return opportunities.

V. The Opportunity for AgTech in the U.S. Heartland: An Example of Regional Assets and Expertise to Drive Innovation

While the Ever-Green Revolution is a global challenge and AgTech is broadly applicable across North America, the AgTech innovation required to achieve sustainable increases in productivity will happen through research and entrepreneurial networks at a regional scale. We believe that the American heartland is one of the regions especially well-suited for the challenge of developing a robust innovation ecosystem in AgTech. The American heartland already has the research and innovation hubs needed to develop the new AgTech products and processes, and is beginning to develop the entrepreneurial hubs needed to grow these innovations to scale. But it will need to do more if it hopes to be the center of the emerging AgTech revolution and capture the value of the resulting products and processes.

Defining the U.S. Heartland

For our purposes, we define the U.S. heartland as the collection of midwestern states that generate the highest concentration of agriculture-related economic value in the United States. Commonly referred to as America's heartland, or the Midwest, this region consists of twelve states in the north-central United States: Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin. The area has some of the richest farming land in the world, and has come to be known as the Nation's "breadbasket."

Heartland Net Farm Income = $60.3 B; 51.2% of Total

State	x $1,000	
Iowa	$10,813,218	9.2%
Nebraska	$7,456,742	6.3%
Illinois	$6,099,710	5.2%
Minnesota	$5,784,631	4.9%
Kansas	$5,191,219	4.4%
South Dakota	$4,619,874	3.9%
Ohio	$3,886,437	3.3%
Indiana	$3,803,890	3.2%
Wisconsin	$3,802,732	3.2%
Michigan	$3,347,852	2.8%
Missouri	$3,333,185	2.8%
North Dakota	$2,171,118	1.8%
Heartland	**$60,310,607**	**51.2%**
Rest of U.S.	$57,597,050	48.8%
TOTAL US	$117,907,650	100.0%

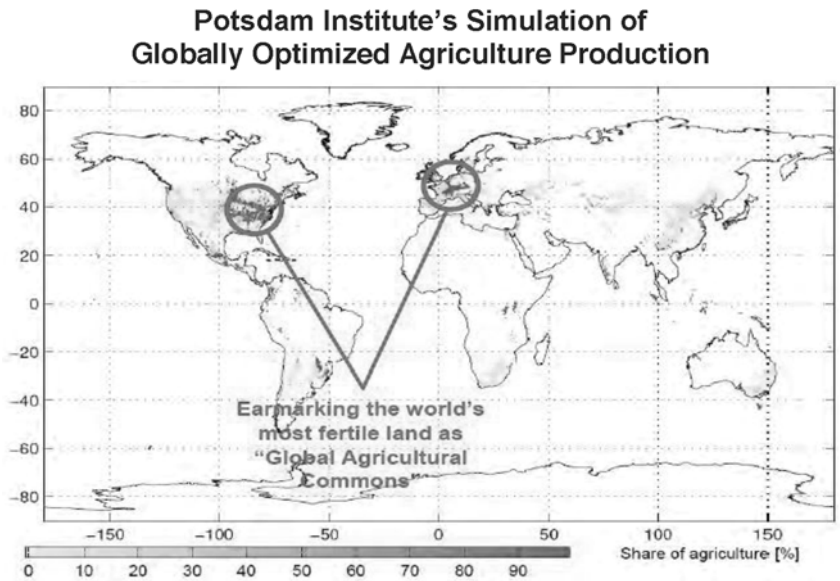
Figure 19: U.S. and heartland region net farm income by state.

As a group, the twelve states listed in Figure 19 generated $60.3 billion in net farm income in 2011, or 51.2 percent of all U.S. net farm income. The heartland produces 85 percent of U.S. corn, 85 percent of U.S. soybeans, 70 percent of U.S. pork, 45 percent of U.S. eggs, 33 percent of U.S. milk, and 30 percent of U.S. beef. This high quantity of production makes the heartland important in global commodity markets, as heartland corn and soy comprise 27.2 percent and 29.75 percent of global production, respectively.

Heartland Assets for AgTech

The heartland is one of the world's most fertile crop production areas, with abundant soil and a climate that currently is amenable to producing large amounts of food. In 2006, a study by the Potsdam Institute for Climate Impact Research simulated what optimal global agricultural production would look based solely on climate, soil, and water constraints, without any regard to existing ag infrastructure. The results of this simulation, displayed in Figure 20 below, show that the U.S. heartland and central Europe are the two most fertile areas in the world. Thus, the heartland's unique geography explains its high concentration of farms of the United States, as shown in Figure 21.

The heartland also has unique advantages in its transportation and processing infrastructure. Goods can be moved by rail, truck, or barge, and transportation networks are concentrated within the region (see Figure 22). Farm products can be shipped from any coast, reaching the Pacific Ocean by rail, the Gulf of Mexico via the Mississippi River, and the Atlantic Ocean via the Gulf of Mexico. Value-added products, such as ethanol or biofuels, can be processed directly in the heartland due to its concentration of processing facilities, as shown in Figure 23.



Source: Kahn & Zaks, "Investing in Agriculture: Far-Reaching Challenge, Significant Opportunity," Deutsche Bank Group, 2009.

Figure 20: Simulation of globally optimized agricultural production.

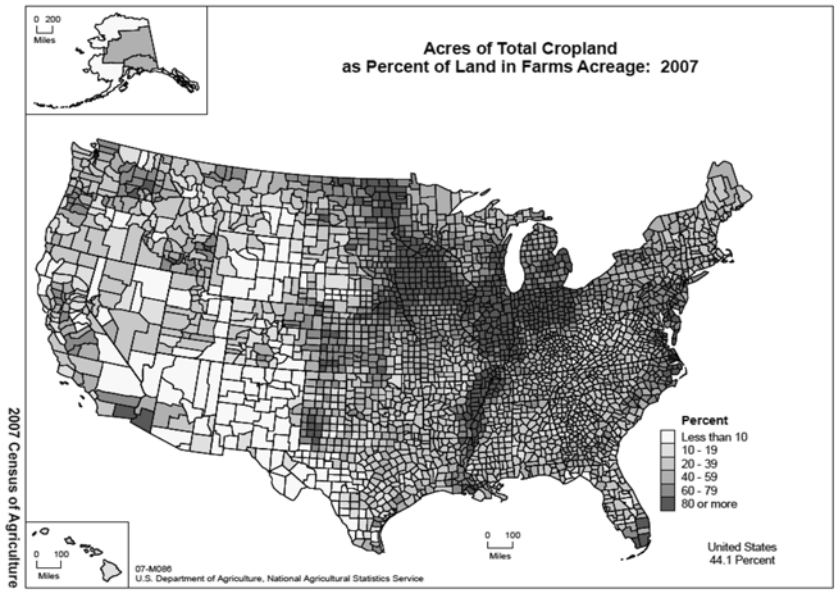
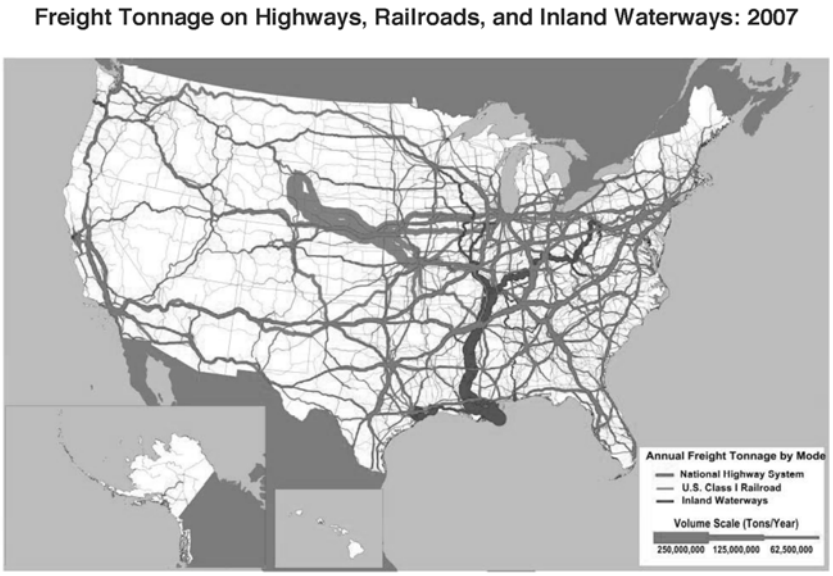
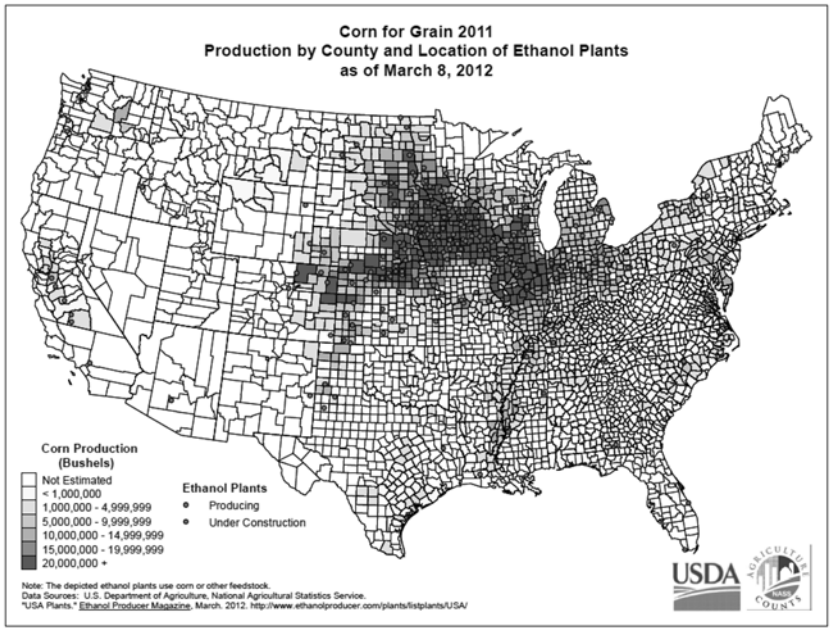


Figure 21. Concentration of cropland in the United States.



Source: "Freight Analysis National Freight Statistics," U.S. Department of Transportation 2007, USDA 2012.
Figure 22. U.S. transportation networks for shipping freight.



Source: "Production by County and Location of Ethanol Plants," USDA, 2012
Figure 23. Location of ethanol processing plants in the United States.

In addition, the heartland has a strong concentration of human capital and research infrastructure focused on AgTech, including land grant public universities and prestigious research institutions. The land grant universities provide a unique

network of cutting-edge basic science platforms, which are catalyst of innovation, knowledge transfer, entrepreneur development and a well-trained workforce.

An Opportunity for the Heartland: Building AgTech Entrepreneur Support Systems

It seems only natural that the heartland would serve as the epicenter for development of a comprehensive innovation ecosystem and entrepreneurial economy around the emerging AgTech sector. However, several factors are holding back such a collaborative effort. First, the heartland does not have a strong regional identity, with various states claiming sole ownership of the "midwestern" identity. This leads to competition between states and a narrowness of vision, only looking within the state's borders for beneficial economic opportunities and preventing larger interstate projects. The heartland also has resisted letting go of its current economic practices, having experienced a very prosperous twentieth century after the rise of organized labor and American superiority in global agriculture. While globalization has upended this established economic model, Americans in the heartland often are hesitant to let go of the recipe that led to success in the past. Finally, the open culture of investment of innovation that exists in places like San Francisco or Boston does not exist in much of the Midwest, which maintains a more stable and sometimes hierarchical social order.

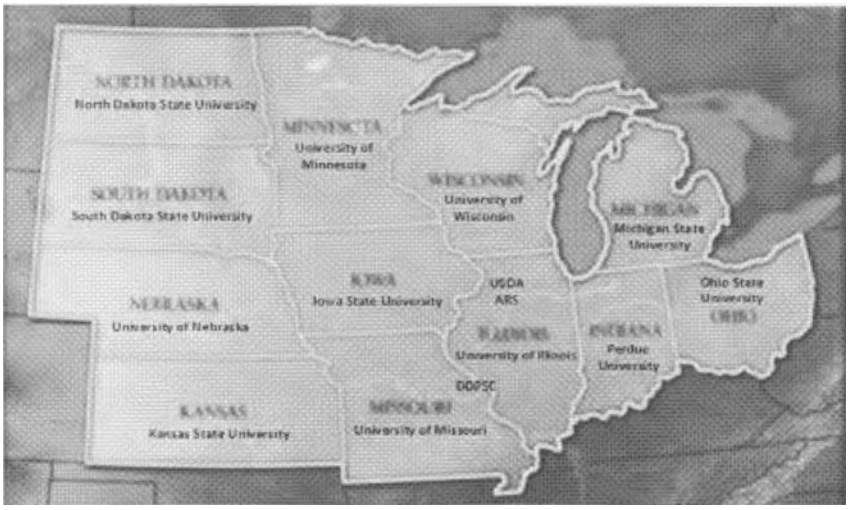


Figure 24: Heartland land-grant universities and research centers.

These cultural dynamics can be a huge obstacle to building successful innovation ecosystems and entrepreneurial economies, but Midwestern cities already are starting to have some success. Two of the most hopeful places for entrepreneurial activity in the AgTech sector are the St. Louis and Kansas City, Missouri, metropolitan areas. St. Louis has invested in institutions like the Danforth Center and BRDG Park, and the combination of its universities and the large AgTech research company, Monsanto, have helped it develop a fairly robust economy around innovations in the plant sciences. Kansas City has focused on animal health, and traditionally has had expertise in the areas of livestock and animal sciences. While Kansas City itself does not have any animal health research centers, the larger region incorporates top-tier veterinary schools at the University of Missouri, the University of Kansas, and Kansas State University. Both cities now are in the early stages of developing more comprehensive entrepreneurial support systems for their respective focus areas.

Some of the world's leading agribusiness, chemical, and farming companies are located in the heartland: Dow Chemicals, an American multinational chemical corporation headquartered in Midland, Michigan; Monsanto, the world's largest seed comp agricultural biotechnology corporation headquartered in Creve Coeur, Missouri; Deere & Company, commonly known by its brand name John Deere, one of the world's largest manufacturers of agricultural machinery, based in Moline, Illinois; the Archer Daniels Midland Company, an American global food-processing and commodities-trading corporation, headquartered in Decatur, Illinois; Cargill, an international producer and marketer of food, agricultural and industrial products

and services, based in Minneapolis; And Procter & Gamble, a multinational consumer goods company headquartered in Cincinnati. These are just a few of the leaders in the agricultural and food spaces, and with their combined forces, they can make a real difference in the amalgamation of clean energy, sustainable agricultural practices and productivity, and advances in new technology. These large players have the potential to create the right ecosystem and inspire new startups in their communities.

Many of the developing nations look up to the U.S. heartland in terms of advances in farming technologies and mechanization of their agriculture sectors. AgTech entrepreneurs and innovators can get a head start by incubating in close proximity to these advanced companies. Similar to the technology prowess of Silicon Valley, the financial leadership of New York, or the entertainment hub of Los Angeles, American's heartland has the right ingredients to be a powerhouse in the agriculture technology space.

VI. Recommendations

We conclude this paper with five major recommendations:

1. Educate and promote the opportunities provided by AgTech.
2. Build and support regional AgTech innovation support systems with "agripreneur" champions.
3. Enable the transition to new technology around the theme of "Green and Lean Efficiency."
4. Engage nonpartisan groups.
5. Develop human capital to meet the needs of tomorrow.

1) Educate and promote the need and opportunity for AgTech and sustainable agriculture.

For entrepreneurs to build AgTech companies, for investors to direct capital to AgTech ventures, and for public officials to promote AgTech development through public policy, they first must know that AgTech exists. They must learn about the major challenges of meeting rising global demand for ag products while staying within the planetary boundaries. And they must realize how the United States, and in particular the heartland, can play a hugely constructive role in moving AgTech forward.

2) Build and support regional AgTech entrepreneur support systems with "agripreneur" champions.

Two sets of factors will be needed to create an AgTech entrepreneur–friendly culture. The first factors needed are social relationships and a collaborative culture, which we believe to be the most essential elements in building an effective entrepreneur support system. The support system should be led by an AgTech entrepreneur champion. This person must serve selflessly for the benefit of the whole, contributing countless hours toward building a system that will help others succeed. The champion must have deep expertise in the area of entrepreneurial activity, but must be willing to set aside his or her ego and let others take credit. Such a champion will create a collaborative, grassroots entrepreneurial culture. As this culture matures, deal quality and volume will grow naturally, creating a scalable culture with many investment opportunities. For AgTech, such a champion must be an "agripreneur," someone completely immersed in the agriculture system across the complete value chain and with deep entrepreneurial experience in agricultural innovation.

Regional agripreneur champions should be consciously and regularly (at least quarterly) connected across regions. The purpose should be to enhance the overall network, and the goal to share ideas about how individual regions are developing and supporting entrepreneurs. As the collective support systems gain momentum, entrepreneurial activity and needed innovations will blossom. Thus, agripreneurs will attract and develop more agripreneurs.

The second set of factors that needs to be created relates to economic development items. These include infrastructure and capital formation. Some of these assets already exist in the some regions and more will be needed as the AgTech entrepreneur culture grows and scales. Economic development investments usually are made regionally and should be guided by direct feedback from agripreneurs.

"Agripreneur" champions particularly are needed in the heartland, where the culture of entrepreneurship and collaboration is not as strong as on the coasts. There already are many AgTech startups in the heartland: in the Cultivian dataset, 305 companies out of the 800 full companies represented in the database were

headquartered in the heartland, and 200 were located in the "corn belt" subregion (Iowa, Illinois, Indiana, Missouri, and Ohio).

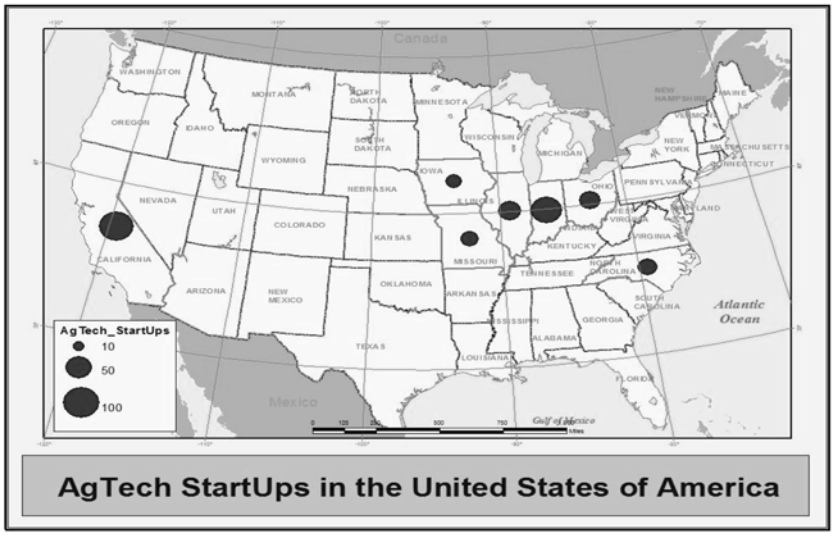


Figure 25. Map showing the number of AgTech startups per state in the Cultivian dataset.

Figure 25 displays the number of AgTech startups in each state, which shows that, overall, AgTech entrepreneurial activity is higher in the heartland than in any other U.S. geographic region. The challenge is that most of this activity appears to be separate or confined by state boundaries. Agripreneur champions will unite the independent startup efforts of AgTech ventures into a movement, and hopefully someday will develop a "Silicon Valley of AgTech" in the American heartland.

3) Enable the transition to new technology around the theme of "Green and Lean Efficiency."

The term Green Revolution was coined in 1968 to indicate revolutionary improvements in crop yield in several Asian countries. Many of these improvements came at the cost of adverse environmental effects in areas subjected to intensive farming. However, where population pressure is high, there is no option except to produce more food. Productivity must increase, but in ways which are environmentally safe, economically viable, and socially sustainable. This has been christened an "evergreen revolution."

We are shifting from scale-driven efficiency to "green and lean" efficiency. After sixty years of chemical control, farming now is entering an era of responsible, transparent, and ecological control, driven in part by consumer demand. AgTech is at the cusp of a new revolution in which innovations in seeds, nutrition, protection, and agronomics are merging. Experts have pointed to similarities with the IT field, in which leading players have embraced convergence and interdependence in Internet search, cloud storage, smartphones, tablets, and PCs, and still carve out their own space to effectively compete. AgTech must go through a similar revolution wherein players will unite to implement state-of-the-art developments in crop nutrition, crop protection, biotechnology, and agronomics, leading to integrated agricultural productivity.

4) Engage nonpartisan groups.

Independent, nonpartisan organizations have the unique ability to bring like-minded people and those with divergent views to the table. Having these organizations take up the cause will help further the common goal of providing nutritious food to a growing population in an environmentally sustainable way. They can be instrumental in providing connectivity to implement agri-tech best practices to farming communities worldwide by fostering networks in which knowledge is shared across communities.

5) Develop human capital to meet the needs of tomorrow.

The solutions that may be available to address the expected food and water shortages likely will require expertise in the development and application of information technology. This expertise currently is not broadly available within the agricultural community and needs to be developed through the whole continuum of our existing learning institutions, including high school, trade schools, community colleges, and higher education institutions.

VII. Conclusion

The task of sustainably increasing global food production is one of the monumental challenges of our time. The framework of an "evergreen revolution" is helpful in reminding us that, while technology has worked to produce more food in the past, we now must produce more food while also eliminating agriculture's negative environmental. A successful evergreen revolution will require many actors, but in particular, it will require entrepreneurs who are passionate about promoting innovation and investment in AgTech.

In short, our overall objectives should be to:

- Increase awareness so that more entrepreneurs and investors can seize this opportunity while helping meet this most basic societal need
- Foster vital communities of AgTech activity across the world focused on "Lean and Green" theme based on unique assets and core competency of each region
- Enable strong networks across communities so that ideas and solutions can flow seamlessly for the benefit of all
- Develop strong educational pillars so that talent and skills are up to par to the challenge at hand.

VIII. Acknowledgements

This white paper would not have been possible without the help of many persons in so many ways. It is the product of tireless dedication, systematic research, constant guidance, and invaluable support rendered by the following people.

At the outset, Sam Fiorello, chief operating officer of the Danforth Center for Plant Science, convincingly identified an opportunity in regard to the research paper, persuaded me to get engaged, agreed to co-sponsor it, and provided thoughtful and invaluable guidance on a regular basis. The germination of this idea for a white paper came from Spencer Maughan, vice president of Venrock Associates in Palo Alto, California. If not for their vision and conviction, the paper would not have been brought to fruition in the first place.

We owe profound gratitude to Adam Hasz, our talented research fellow, who has worked tirelessly and made tremendous research contributions in shaping the foundation of this paper. Without his ingenuity, intellect, passion, commitment, and diligent efforts, we would not have been able to successfully produce this thought-provoking document.

I must express my deepest appreciation and thanks to Ken Harrington, managing director of the Skandalaris Center at Washington University in St. Louis, for his able guidance, many constructive suggestions, and unwavering support since the inception of this research project and through its completion.

In addition, I would like to thank Joseph Cornelius, PhD, for his technical guidance and expertise in global agricultural production systems and sustainability that contributed greatly to this paper.

Special thanks are extended to Andy Ziolkowski and Ron Meeusen from Cultivian Ventures for advice on the research paper approach and for providing access to valuable data that critically facilitated this paper. We also wish to express our sincere thanks to Nandini Taneja, program associate of LARTA, for her contribution in compiling the LARTA data set.

I would like to acknowledge Jason Hall, former director of the Missouri Department of Economic Development, who provided valuable information on the current AgTech activities in Missouri. Also, I would like to thank Kim Young, vice president of the Kansas City Area Development Council, who provided insights on animal health investment activities in greater Kansas City. On the same note, I would like to express my thanks to Tom Overbay, partner at Expedite Animal Health, who patiently provided a detailed overview of the animal health industry and R&D practices observed.

Finally, I would like to express my special thanks to the Ewing Marion Kauffman Foundation for support and encouragement.

SUREN G. DUTIA,
Senior Fellow,
Ewing Marion Kauffman Foundation.

Additional Sources

Bernick, Jeanne. "Ag Goes Natural with Biologics," *Farm Journal AgWeb,* June 21, 2012, *http://www.agweb.com/article/ag_goes_natural_with_biologics/.*

Blumfeld, Jenna. "New GMO-Education Site Funded by Monsanto, Dupont." *New Hope 360 Blog,* July 31, 2013. *http://newhope360.com/blog/new-gmo-education-site-funded-monsanto-dupont.*

Budzynski, Jim. Ag Innovation Showcase. St. Louis, Missouri, September 11, 2013.

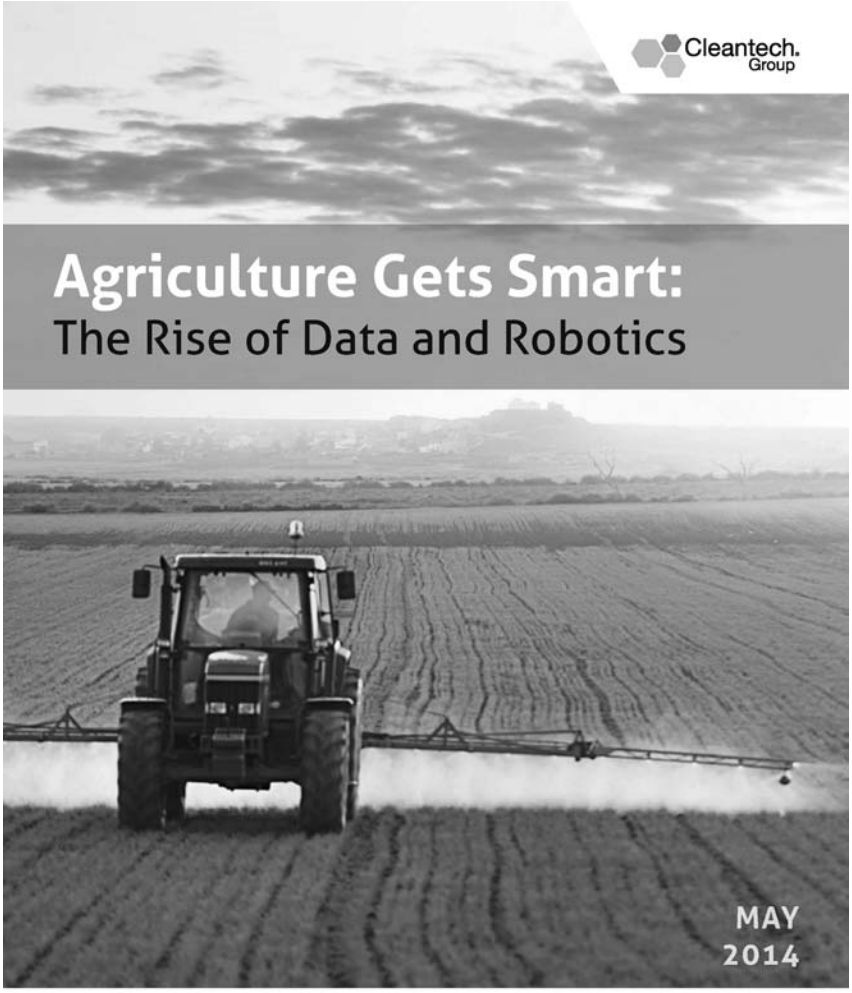
LeClerc, Rob. "Is Agriculture the New Cleantech?" *note from CEO of Agfunder.*

National Public Radio. "Feeding A Hotter, More Crowded Planet." August 12, 2011. *http://www.npr.org/2011/08/12/139579616/feeding-a-hotter-more-crowded-planet.*

http://evergreen-revolution.tripod.com/evergreenrevoldefined.html

---

AGRICULTURE GETS SMART: THE RISE OF DATA AND ROBOTICS



Authors:
Amanda Faulkner, Research Manager, Cleantech Group
Kerry Cebul, Principal, Cleantech Group

Contributor:
Gannon McHenry, Junior Analyst, Cleantech Group

Big Data Meets Agriculture

Big data and agriculture came crashing into the wider consciousness in late 2013 when **Monsanto** placed a billion dollar bet and acquired The **Climate Corporation**, a San Francisco-based provider of agriculture insurance underpinned by data analytics on climate. The company, founded by Google alums and operating in the heart of the Bay Area and the wider Silicon Valley ecosystem, was backed by **Google Ventures**, **Khosla Ventures**, **Founders Fund**, and other top venture firms. It was a major statement by **Monsanto**, a firing of the first shot in a war for dominating the big data and agriculture space. The deal also showed the willingness of a large, established agriculture corporate to spend major dollars to incorporate Silicon Valley innovation DNA into its business. In its press release on the deal, **Monsanto** claimed that data science in agriculture represents a $20 billion opportunity beyond **Monsanto**'s core focus. With that kind of opportunity, **Monsanto** will likely not be the only agriculture giant rushing to capture part of that market share. i3 has tracked partnerships and investments into agriculture companies from corporates ranging from Google to **BP** to **GE** to **Mitsui**, as well as the expected players such as **Syngenta**, **Monsanto**, **DuPont**, and **Cargill**.

Big data is a major area well beyond agriculture, with applications ranging from security to healthcare to retail. McKinsey cited a $300 billion opportunity each year for big data to create value in the US healthcare sector alone. The increases in efficiency through more transparent data trends will have impacts in almost every sector and are driving innovation across a number of markets. Tech companies such as **IBM**, Google, **Oracle**, and **EMC** have already jumped wholeheartedly into this space.

Within this opportunity for data and precision, agriculture is in particular need of these increasing efficiencies. Each acre will need to produce more food while being tended to by a smaller and smaller group of growers. This will mean tailored solutions that ensure that every plant is optimized. Jorge Heraud, the CEO of **Blue River Technology** and a former Director of Engineering and Business Development at **Trimble Navigation**, sees the trend going from field-level management down to plant-level management. He commented that "there has been, over many years, the realization by farmers that there is lots of variability inside a field. The basic unit of management has moved from farm level to field level to small plot areas. I see that as a trend going from bigger to smaller, and see that trend continuing. There is lots of variability within a small area still. I believe this will lead to plant by plant management."

Monsanto is clearly jumping in enthusiastically, with a number of acquisitions tracked in i3 over the past few years. In 2012 **Monsanto** acquired **Precision Planting**, an Illinois-based developer of planting products and solutions that contribute to better seed spacing, better depth control, and better root systems. It then moved onto its big move, acquiring **Climate Corp** in 2013 for around a billion dollars. The spree continued in 2014 with **Climate Corp** acquiring the soil analysis business line of **Solum**. Although the deal was potentially not a great exit for investors, the **Solum** deal showed the continued interest in the space from **Monsanto**.

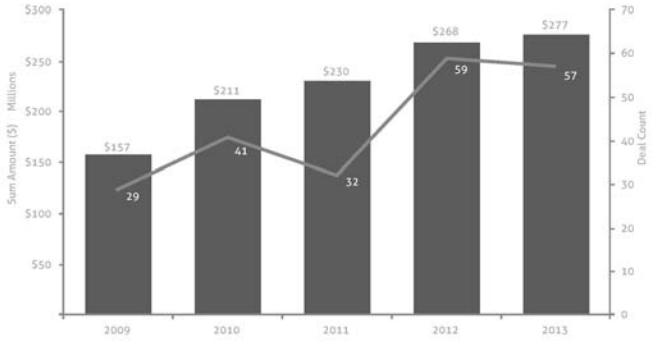
MONSANTO'S DATA ACQUISITION SPREE

Powered by data from i3

Acquisition target	Technology	Commentary
Precision Planting	Developer of planting products and solutions that contribute to better seed spacing, better depth control and better root systems	**Monsanto** acquired **Precision Planting** for $210 million in 2012, beefing up its Integrated Farming Systems unit.
The Climate Corporation	Provider of weather analytics and insurance coverage to protect farmers from the financial impact of climate change	**Monsanto** acquired **Climate Corp** for around $1 billion in 2013, with **Monsanto** noting that data science in ag is a $20 billion opportunity.
Solum	Developer of software and management technology for applications in agriculture	**Climate Corp**, by then a **Monsanto** subsidiary, acquired the soil analysis business of **Solum** for an undisclosed amount.

With the interest from corporates like **Monsanto**, venture firms are realizing the potential for the sector. Agriculture & Food more broadly attracted $277 million across 57 deals in 2013 according to i3. While the largest rounds went to seed genomics and contaminant detection, a number of companies in the big data + agriculture space, including **HydroPoint Data Systems**, **FarmLogs**, and **Harvest Automation**, received VC funding. Corporates are also putting their money where their mouth is, with **Mitsui**, **Syngenta**, and **Westlake Chemical** all making equity investments. With the **Climate Corp** deal in late 2013, we will likely see an uptick in deals across 2014. Already we have seen deals for **Hampton Creek Foods**, **Chromatin**, **Granular**, and others in 2014.

VENTURE AND CORPORATE INVESTMENT IN AGRICULTURE & FOOD



Innovation in Big Data + Agriculture

While corporates are very involved with big data and agriculture, startups are still at the heart of the action, providing solutions across the value chain, from infrastructure and sensors all the way down to software that manages the many streams of data from across the farm. Corporates are already targeting this area heavily, especially in the areas of sensors and positioning systems for farm equipment. Sensors can be used to detect plant- and plot-level soil moisture, fertilizer input, weeds, and disease. For instance, **Libelium** produces sensors for markets ranging from smart grid to healthcare, and specifically for agriculture, sensors to track conditions in vineyards and greenhouses. These sensors are also incorporated into drones and robotics to make those systems more effective. Positioning and guidance systems, or global navigation satellite systems (GNSS), for farm equipment is also becoming standard for farmers, with global position systems (GPS) and differential GPS customary on new farm equipment. These systems allow farmers to program precision planting and chemical inputs for higher precision. The new wave of innovation uses sensors and GNSS to further the efficiency of agriculture with increasingly easy-to-use systems for farmers. More generally, Precision Agriculture and Agriculture Software are the fastest growing areas of agriculture innovation within i3, with new companies coming into the product weekly. In particular, the areas of drones, sensors, and software are growing, while robotics is emerging from its nascency.

DRONES

One of the hottest innovation spaces is drones, or unmanned aerial vehicles (UAVs), that are providing effective and cheap imaging capabilities. By showing variability in irrigation, yields, and pests, the drones give insight into conditions from the plot to plant level. This new breed of drones can fly themselves and provides composite images that are immediately of use to the farmer. Many of these companies are focusing on both the hardware and software, with a particular focus on the software. With drones heading down the path to becoming commodities, the software will ultimately make it useful for farmers to be able to operate without special training, and to gather useful data. Some of the companies at the forefront of this field are **PrecisonHawk**, **Aerial Precision**, **Ceres Imaging**, and **HoneyComb**.

PrecisionHawk is an Indiana-based provider of end-to-end aerial data collection, data management, and data analysis systems. The company's specialty is in its artificial intelligence software for its UAVs, which can fly themselves using flight planning software. The data is then made usable using data review and management, online aerial video management, automated orthomosaic processing, and a cloud platform for accessing the composited and ready-to-use images. Although agriculture is PrecisionHawk's first target market, it is planning to expand to other markets.

Aerial Precision is a maker of multi-copter drones based in Arizona. The company, a division of Roboflight, offers integrated aerial platform that gives agricultural producers easy to fly vehicles providing video and photo images to scout crops, making farming operations more precise and better managed.

Ceres Imaging is a California-based provider of solutions to farmers that help optimize water and nitrogen use. The company is piloting its system with California growers and partnering with UC Davis.

HoneyComb is an Oregon-based developer of UAVs for use in farming and forestry. The company's hardware product, AgDrone UAS, can be equipped with a variety of cameras including thermal, spectral, and visible. The company's software product provides mapping and analytics and provides data that allows farmers to detect crop deficiencies and better allocate resources.

ROBOTICS

Artificial intelligence is also being used to incorporate robotics into agriculture. Robotics can provide a labor replacement as agriculture struggles with an aging farm workforce and decreasing amounts of immigrant labor. Jorge Heraud, the CEO of **Blue River Technology** and a former Director of Engineering and Business Development at **Trimble Navigation**, sees the next yield increase breakthrough coming from making every plant productive, with "the challenge being where the robotic applications appear first and which area are most in need of robotics. Plant by plant care can provide a tremendous increase in yield, decrease input requirements, and improve agricultural sustainability." **Blue River Technology** is a California-based provider of robotics for agriculture. The company uses cameras, computer vision, and machine learning algorithms to provide an efficient lettuce thinning process.

BRINGING IT ALL TOGETHER

With all of these technologies, from sensors to UAVs, gathering data, the next step is to bring it together in one easy-to-use system for farmers. One challenge to bringing all the data together in a useful way is the wireless infrastructure present in many rural areas. For areas not covered by the big carriers like AT&T and Verizon, getting data from sensors to a central software system is extremely difficult. **Intelligent Wireless Networks** is a company tackling this problem by developing specialized WiFi networks in rural and farming communities. Not only can the farmers get the data without sending someone to collect it from each sensor, it provides in-field connectivity for the many farmers who now work primarily from phones and tablets.

Once all this data has made it to a central location, it needs to be useable. Lance Donny, the CEO of **OnFarm**, comments that "many farmers are frustrated with their data in different places, making it hard to run their operation from anywhere but the office." That is where companies like **OnFarm** come in. The company offers a cloud-based platform that enables the integration of data from multiple sources and an open network of solution providers. Farmers can select the information they need from soil, plant, weather, and equipment solutions and have a single system to plan, manage, and control their field operations. Like **OnFarm**, **Granular**, the recent spin-off from **Solum**'s acquisition by **Climate Corp** and **Monsanto**, develops a cloud-based software platform for planning, production, marketing, and accounting in production agriculture.

Taking the data one step further, companies like the **Climate Corp** are using publically available data and making it useful for farmers. **Climate Corp** uses public data to inform its big data analytics, which provide the basis for its insurance plans for farmers. The **Climate Corp** also offers field-level data from **Precision Planting**.

WHAT'S NEXT?

Despite all these drivers, from climate change to increasing populations, and myriad technologies addressing these markets, there are many challenges to fully implementing big data in agriculture. One of the early issues in scaling these technologies is farmer concern over data ownership. Just as users of Facebook and Google worry about who owns their personal and search data, farmers are wary of technology without establishing who owns the data from sensors, drones, and software. Lance Donny, CEO of **OnFarm**, comments that "farmers are becoming increasingly concerned about who owns the data generated on their farms, who can access it, and for what reason. Significant opportunities exist for data analysis that drives increased efficiencies in agriculture, but data ownership and privacy in agriculture, like other industries, is complex and companies will have to consider the right balance between what's confidential to the farm and what data can be used to enhance their solution." Although this issue of data ownership will likely not prevent growers from adopting these technologies, companies working in this space will have to have clear guidelines and maker growers feel confident in the security of their data.

One unknown in this space will be which corporates ultimately dominate it. **Monsanto** has clearly put a flag in the ground and aims to be a leader. Companies like **Syngenta**, **Dow**, **Bayer**, and John Deere will likely participate in these trends. However, they may be competing with more traditional data and tech firms, such as Google and **IBM**, who see agriculture as a new market to apply their technology. Will the next billion dollar acquisition of a big data + agriculture company come from **Monsanto** or Google?

With all the corporates jumping into the space, most are looking to partner or invest in companies that can help them leapfrog competitors and incorporate Silicon Valley DNA into these agriculture giants. New companies are forming all the time and are equally hungry to meet the investors and corporates. These partnerships, investments, and acquisitions will be the defining force shaping the big data + agriculture space in the years to come.

Want to find more agriculture innovation?
Use an i3 Campaign!

Developing your pipeline is hard
- Corporates have to manage technologies needs for global operations
- Company discovery and vetting takes time, and has low conversion rates
- It's often difficult to differentiate between the top innovators

We have access to great entrepreneurs
- Leverage i3 to broadcast your current needs to targeted groups of entrepreneurs
- Tap our network of 60,000+ entrepreneurs and innovation stakeholders worldwide
- Use our team to do your initial vetting

Simple process, great results
- We reach out to select groups of entrepreneurs
- Entrepreneurs answer a personalized questionnaire to speed up the initial validation process
- We tier the results and deliver direct introductions with the 5-10 best fits in just 5 weeks

Free trial: i3connect.com

"i3 is a fantastic tool. We use i3 to connect with and understand startups in the evolving M2M market. Startups recently vied for a spot on our latest i3 List: many look promising and the top 10 were all new prospects for me. I'm excited to have access to this tool going forward"

Gil Demeter
Senior Associate
Qualcomm Ventures

The CHAIRMAN. Thank you, Mr. Donny.

Mr. Thierer?

STATEMENT OF ADAM D. THIERER, SENIOR RESEARCH FELLOW, MERCATUS CENTER, GEORGE MASON UNIVERSITY

Mr. THIERER. Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the policy implications of the Internet of Things. My name is Adam Thierer, and I am a Senior Research Fellow at the Mercatus Center at George Mason University where I study technology policy.

My message here today is condensed from a recent book, as well as a forthcoming law review article on the Internet of Things. My research focuses primarily on the privacy and security implications associated with the Internet of Things and wearable technology in particular.

The three general conclusions of my work are as follows.

First, the Internet of Things offers compelling benefits to consumers, companies, and our country's national competitiveness that will only be achieved by adopting a flexible policy regime for this fast-moving space.

Second, while there are formidable privacy and security challenges associated with the Internet of Things, top-down or one-size-fits-all regulation will limit innovative opportunities.

Third, with those two points in mind, we should seek out alternative and less costly approaches to protecting privacy and security that rely on education, empowerment, and targeted enforcement of existing legal mechanisms. Long-term privacy security and protection requires a multifaceted approach incorporating many flexible solutions.

I will briefly discuss each point.

First, the Internet of Things will benefit the "3 Cs" of consumers, companies, and our country. Consumers will benefit from more of their devices being networked, sensing, and communicating. It offers us more choices and convenience, especially for personal health and productivity. Companies will benefit from increased efficiencies and the ability to offer a staggering array of new product and service options to their customers. And our country will benefit by maintaining our global competitive advantage in the digital economy.

The magnitude of the opportunity here is breathtaking. Technology analysts and economic consultancies have predicted economic benefits in the trillions of dollars.

The positive effects of the Internet of Things will reverberate throughout every sector of the economy, and as Progressive Policy Institute economist Michael Mandel notes, it has the "potential to help revive the high-growth economy." It will revolutionize manufacturing, health care, energy, transportation, retailing, and various government services.

But if America hopes to be a global leader in the Internet of Things, as it has been for the Internet more generally over the past 2 decades, then we will have to get public policy right first.

America took a commanding lead in the digital economy because in the mid-1990s, Congress and the Clinton administration crafted

a nonpartisan vision for the Internet that protected permissionless innovation, or the idea that experimentation with new technologies and business models should generally be permitted without prior approval.

Congress embraced permissionless innovation by passing the Telecom Act of 1996 and rejecting archaic analog era command-and-control regulations for this exciting new medium.

And the Clinton administration embraced permissionless innovation with its 1997 Framework for Global Electronic Commerce, which outlined a clear vision for Internet governance that relied upon civil society, voluntary agreements, and ongoing marketplace negotiations.

This nonpartisan blueprint, sketched out almost 2 decades ago for the Internet, is every bit as sensible today as we begin crafting a policy paradigm for the Internet of Things.

Again, the first order of business is for policymakers to send a clear green light to entrepreneurs letting them know that our Nation's default policy position remains "innovation allowed." Second, we should avoid basing our policy interventions on hypothetical worst-case scenarios or else best-case scenarios will never come about. Our policy regime, therefore, should be responsive, not anticipatory.

Of course, privacy- and security-related challenges remain that deserve our attention. Data is going to be moving fluidly across so many platforms and devices that it will be difficult to apply traditional Fair Information Practice Principles in a rigid regulatory fashion for every conceivable use of these technologies.

Specifically, it will be challenging to achieve perfect notice and choice in a world where so many devices are capturing volumes of data in real time. Moreover, while data minimization remains a worthy goal, if it is mandated in a one-size-fits-all way, it could limit many life-enriching innovations.

Law must still play a role, but we are going to need new approaches.

Policymakers can encourage privacy and security by design for the Internet of Things and its developers, but these best practices should not be mandated as top-down controls. Flexibility is essential.

More privacy-enhancing tools, especially robust encryption technologies, will also help, and Government officials would be wise to promote those tools instead of restricting them.

Increased education is also essential, and Government should help get out the word about inappropriate uses of these technologies.

Existing privacy torts and existing targeted rules, like Peeping Tom laws, will also likely evolve to address serious harms as they develop.

Finally, the Federal Trade Commission will continue to play an important backstop role using its Section 5 authority to police unfair and deceptive practices. The FTC has already been remarkably active in encouraging companies to live up to the privacy and security promises they make to their consumers, and that will continue.

In closing, we should never forget that no matter how disruptive these new technologies may be in the short term, we humans have

the extraordinary ability to adapt to technological change and bounce back from adversity. That same resilience will be true for the Internet of Things.

We should remain patient and continue to embrace permissionless innovation to ensure that the Internet of Things thrives and American consumers and companies continue to be global leaders in the digital economy.

Thank you.

[The prepared statement of Mr. Thierer follows:]

PREPARED STATEMENT OF ADAM D. THIERER, SENIOR RESEARCH FELLOW, MERCATUS CENTER, GEORGE MASON UNIVERSITY

Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the policy implications of the Internet of Things. My name is Adam Thierer, and I am a senior research fellow at the Mercatus Center at George Mason University, where I study technology policy.

My message today is condensed from a recent book [1] and a forthcoming law review article [2] on the Internet of Things, which refers to a world full of "smart" devices equipped with sensing and networking capabilities.

My research focuses primarily on the privacy and security implications of the Internet of Things and wearable technology. The three general conclusions of my work are as follows:

1. First, the Internet of Things offers compelling benefits to consumers, companies, and our country's national competitiveness that will only be achieved by adopting a flexible policy regime for this fast-moving space.
2. Second, while there are formidable privacy and security challenges associated with the Internet of Things, top-down or one-size-fits-all regulation will limit innovative opportunities.
3. Third, with those first two points in mind, we should seek alternative and less costly approaches to protecting privacy and security that rely on education, empowerment, and targeted enforcement of existing legal mechanisms. Long-term privacy and security protection requires a multifaceted approach incorporating many flexible solutions.

I will discuss each point briefly.

Benefits of IoT

First, the Internet of Things will benefit the "3-Cs" of consumers, companies, and our country:

- *Consumers* will benefit from more of their devices being networked, sensing, and communicating. The Internet of Things offers us more choices and convenience, especially for personal health and productivity.
- *Companies* will benefit from increased efficiencies and the ability to offer a staggering array of new product and service options to their customers.[3]
- And our *country* will benefit by maintaining our global competitive advantage in the digital economy.

---

[1] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2014).

[2] Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the *Richmond Journal of Law and Technology* 21, no. 6 (2015), *http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.*

[3] Michael E. Porter and James E. Heppelmann, "How Smart, Connected Products Are Transforming Competition," *Harvard Business Review,* November 2014, *https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.*

The magnitude of this opportunity is breathtaking.[4] Technology analysts and economic consultancies have predicted economic benefits in the *trillions* of dollars.[5]

The positive effects of the Internet of Things will reverberate throughout every sector of the economy, and as Progressive Policy Institute economist Michael Mandel notes, it "has the potential to help revive the high-growth economy."[6] It we let it, it could revolutionize manufacturing, health care, energy, transportation, retailing, and various government services.

Getting Policy Right

If America hopes to be a global leader in the Internet of Things, as it has been for the Internet more generally over the past two decades, then we first have to get public policy right.

America took a commanding lead in the digital economy because, in the mid-1990s, Congress and the Clinton administration crafted a nonpartisan vision for the Internet that protected "permissionless innovation"—the idea that experimentation with new technologies and business models should generally be permitted without prior approval.[7]

Congress embraced permissionless innovation by passing the Telecommunications Act of 1996 and rejecting archaic Analog Era command-and-control regulations for this exciting new medium.[8]

The Clinton administration embraced permissionless innovation with its 1997 "Framework for Global Electronic Commerce," which outlined a clear vision for Internet governance that relied on civil society, voluntary agreements, and ongoing marketplace experimentation.[9]

This nonpartisan blueprint sketched out almost two decades ago for the Internet is every bit as sensible today as we begin crafting a policy paradigm for the Internet of Things.[10]

Again, the first order of business is for policymakers to send a clear green light to entrepreneurs letting them know that our Nation's default policy position remains "innovation allowed." Second, we should avoid basing policy interventions on hypothetical worst-case scenarios, or else best-case scenarios will never come about.[11] Our policy regime, therefore, should be responsive, not anticipatory.

Flexible Solutions

Of course, privacy-and security-related challenges exist that deserve attention. Data is going to be moving fluidly across so many platforms and devices that it will

---

[4] Emily Adler, "The 'Internet of Things' Will Soon Be a Truly Huge Market, Dwarfing All Other Consumer Electronics Categories," *Business Insider,* July 10, 2014, *http://www.businessinsider.com/internet-of-things-will-soon-be-a-truly-huge-market-dwarfing-all-other-consumer-electronics-categories-2014-7.*

[5] Gil Press, "Internet of Things by the Numbers: Market Estimates and Forecasts," *Forbes,* August 22, 2014, *http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts.*

[6] Michael Mandel, "Can the Internet of Everything Bring Back the High-Growth Economy?" (Policy Memo, Progressive Policy Institute, Washington, D.C., September 2013), 9, *http://www.progressivepolicy.org/2013/09/can-the-internet-of-everything-bring-back-the-high-growth-economy.* ("No one can predict the ultimate course of innovative technologies, but it appears that the Internet of Everything has the potential to help revive the high-growth economy.")

[7] Adam Thierer, "Embracing a Culture of Permissionless Innovation" (Cato Online Forum, Cato Institute, Washington, D.C., November 2014), *http://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.*

[8] Adam Thierer, "The Greatest of All Internet Laws Turns 15," *Forbes,* May 8, 2011, *http://www.forbes.com/sites/adamthierer/2011/05/08/the-greatest-of-all-internet-laws-turns-15.*

[9] Specifically, the Clinton framework stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry." It also argued that "governments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce." White House, "The Framework for Global Electronic Commerce" (July 1997), *http://clinton4.nara.gov/WH/New/Commerce.*

[10] Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," *Forbes,* February 12, 2012, *http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm.*

[11] As analysts at the Center for Data Innovation correctly argue, policymakers should only intervene to address specific, demonstrated harms. "Attempting to erect precautionary regulatory barriers for purely speculative concerns is not only unproductive, but it can discourage future beneficial applications of the Internet of Things," they say. See Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2014, *http://www.datainnovation.org/2014/12/10-policy-principles-for-unlocking-the-potential-of-the-internet-of-things.*

be difficult to apply traditional Fair Information Practice Principles[12] in a rigid regulatory fashion for every conceivable use of these technologies.[13]

Specifically, it will be challenging to achieve perfect "notice and choice" in a world where so many devices are capturing volumes of data in real time. Moreover, while "data minimization" remains a worthy goal, if it is mandated in a one-size-fits-all fashion, it could limit many life-enriching innovations.

Law will still play a role, but we're going to need new approaches.

- Policymakers can encourage *privacy and security "by design"* for Internet of Things developers, but those best practices should not be mandated as top-down controls. Flexibility is essential.[14]
- More *privacy-enhancing tools*—especially robust encryption technologies—will also help, and government officials would be wise to promote these tools instead of restricting them.
- *Increased education* is also essential, and governments can help get the word out about inappropriate uses of these technologies.
- Existing *privacy torts and existing targeted rules* (such as "Peeping Tom" laws) will also likely evolve to address serious harms as they develop.
- Finally, the Federal Trade Commission will continue to play an important backstop role, using its Section 5 authority to *police "unfair and deceptive" practices.* The commission has already been remarkably active in encouraging companies to live up to the privacy and security promises they make to their consumers, and that will continue.

Conclusion: We Can Adapt

In closing, we should also never forget that, no matter how disruptive these new technologies may be in the short term, we humans have an extraordinary ability to adapt to technological change and bounce back from adversity.[15] That same resilience will be true for the Internet of Things.

We should remain patient and continue to embrace permissionless innovation to ensure that the Internet of Things thrives and American consumers and companies continue to be global leaders in the digital economy.

Appendices to Testimony of Adam Thierer

1. Selected Readings from Adam Thierer on the Internet of Things
2. What Is the Internet of Things?
3. Projected Use and Economic Impact of the Internet of Things
4. A Nonpartisan Policy Vision for the Internet of Things
5. Some Initial Thoughts on the FTC Internet of Things Report
6. Why "Permissionless Innovation" Matters
7. How We Adapt to Technological Change

---

[12] The Fair Information Practice Principles (FIPPs) traditionally include (1) notice, (2) choice, (3) purpose specification, (4) use limitation, and (5) data minimization.

[13] Adam Thierer, "Some Initial Thoughts on the FTC Internet of Things Report," *Technology Liberation Front,* January 28, 2015, *http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report.*

[14] Adam Thierer, "Striking a Sensible Balance on the Internet of Things and Privacy," *Technology Liberation Front,* January 16, 2015, *http://techliberation.com/2015/01/16/striking-a-sensible-balance-on-the-internet-of-things-and-privacy.* See also Adam Thierer, "Muddling Through: How We Learn to Cope with Technological Change," *Medium,* June 30, 2014, *https://medium.com/tech-liberation/muddling-through-how-we-learn-to-cope-with-technological-change-6282d0d342a6.*

[15] Adam Thierer, "Muddling Through: How We Learn to Cope with Technological Change," *Medium,* June 30, 2014, *https://medium.com/tech-liberation/muddling-through-how-we-learn-to-cope-with-technological-change-6282d0d342a6.*

APPENDIX 1: SELECTED READINGS FROM ADAM THIERER ON THE INTERNET OF THINGS

law review article: *"The Internet of Things and Wearable Technology Addressing Privacy and Security Concerns without Derailing Innovation,"* forthcoming, *Richmond Journal of Law & Technology*, Vol. 21, No. 6, (2015), *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494382.*

essay: "*A Nonpartisan Policy Vision for the Internet of Things," Technology Liberation Front,* December 11, 2014, *http://techliberation.com/2014/12/11/a-nonpartisan-policy-vision-for-the-internet-of-things.*

essay: "*Some Initial Thoughts on the FTC Internet of Things Report," Technology Liberation Front,* January 28, 2015, *http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report.*

essay: "*Striking a Sensible Balance on the Internet of Things and Privacy," Technology Liberation Front,* January 16, 2015, *http://techliberation.com/2015/01/16/striking-a-sensible-balance-on-the-internet-of-things-and-privacy.*

slide presentation: *"Policy Issues Surrounding the Internet of Things & Wearable Technology,"* September 12, 2014, *http://techliberation.com/2014/09/12/slide-presentation-policy-issues-surrounding-the-internet-of-things-wearable-technology.*

essay: "*CES 2014 Report: The Internet of Things Arrives, but Will Washington Welcome It?" Technology Liberation Front,* January 8, 2014, *http://techliberation.com/2014/01/08/ces-2014-report-the-internet-of-things-arrives-but-will-washington-welcome-it.*

essay: "*The Growing Conflict of Visions over the Internet of Things & Privacy," Technology Liberation Front,* January 14, 2014, *http://techliberation.com/2014/01/14/the-growing-conflict-of-visions-over-the-internet-of-things-privacy.*

op-ed: "*Can We Adapt to the Internet of Things?" IAPP Privacy Perspectives,* June 19, 2013, *https://privacyassociation.org/news/a/can-we-adapt-to-the-internet-of-things.*

agency filing: *My Filing to the FTC in its 'Internet of Things' Proceeding,* May 31, 2013, *http://techliberation.com/2013/05/31/my-filing-to-the-ftc-in-its-internet-of-things-proceeding.*

book: *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2014), *http://mercatus.org/permissionless/permissionlessinnovation.html.*

essay: "*What's at Stake with the FTC's Internet of Things Workshop," Technology Liberation Front,* November 18, 2013, *http://techliberation.com/2013/11/18/whats-at-stake-with-the-ftcs-internet-of-things-workshop.*

law review article: *"Removing Roadblocks to Intelligent Vehicles and Driverless Cars,"* forthcoming, *Wake Forest Journal of Law & Policy* (2015), *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496929.*

APPENDIX 2: WHAT IS THE INTERNET OF THINGS?[16]

Many of the underlying drivers of the Internet and Information Age revolution—massive increases in processing power, exploding storage capacity, steady miniaturization of computing and cameras, ubiquitous wireless communications and networking capabilities, digitization of all data, and massive datasets (or "big data")—are beginning to have a profound influence beyond the confines of cyberspace. It is cheaper than ever, for example, to integrate a microchip, a sensor, a camera, and even an accelerometer into devices today. "Thanks to advances in circuits and software," observe Neil Gershenfeld and J. P. Vasseur, "it is now possible to make a Web server that fits on (or in) a fingertip for $1." As costs continue to fall and these technologies are increasingly embedded into almost all devices that consumers own and come into contact with, a truly "seamless web" of connectivity and "pervasive computing" will exist.

As a result of these factors, mundane appliances and other machines and devices that consumers have long taken for granted—cars, refrigerators, cooking devices, lights, weight scales, watches, jewelry, eyeglasses, and even their clothing—will all

[16] This section adapted from Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the *Richmond Journal of Law and Technology* 21, no. 6 (2015), *http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.*

soon be networked, sensing, automated, and communicating. In other words, consumers are transitioning to what Alex Hawkinson, CEO and founder of SmartThings, calls a "programmable world" where "things will become intuitive [and] connectivity will extend even further, to the items we hold most dear, to those things that service the everyday needs of the members of the household, and beyond."[17]

This so-called Internet of Things—or "machine-to-machine" connectivity and communications—promises to usher in "a third computing revolution"[18] and bring about profound changes that will rival the first wave of Internet innovation. The first use of the term Internet of Things is attributed to Kevin Ashton, who used it in the title of a 1999 presentation.[19] A decade later, he reflected on the term and its meaning:

> If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best.
>
> We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory. RFID [radio-frequency identification] and sensor technology enable computers to observe, identify, and understand the world—without the limitations of human-entered data.[20]

More recently, analysts with Morrison & Foerster have defined IoT as "the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings."[21] These low-power devices typically rely on sensor technologies as well as existing wireless networking systems and protocols (Wi-Fi, Bluetooth, near field communication, and GPS) to facilitate those objectives. In turn, this reliance will fuel the creation of even more "big data." Many of these technologies and capabilities will eventually operate in the background of consumers' lives and be almost invisible to them.

IoT is sometimes understood as being synonymous with "smart" systems: smart homes, smart buildings, smart appliances, smart health, smart mobility, smart cities, and so on. Smart car technology is also expanding rapidly.[22] The promise of IoT, as described by *New York Times* reporter Steve Lohr, is that "billions of digital devices—from smartphones to sensors in homes, cars, and machines of all kinds—will communicate with each other to automate tasks and make life better."[23] "Consumers and public officials can use the connected world to improve energy conservation, efficiency, productivity, public safety, health, education, and more," predicts CEA.[24] "The connected devices and applications that consumers choose to adopt will make their lives easier, safer, healthier, less expensive, and more productive."[25] In addition to giving consumers more control over their lives, these technologies can also help them free up time by automating routine tasks and chores.

---

[17] Alex Hawkinson, "What Happens When the World Wakes Up," *Medium* (Sept. 23, 2014), *https://medium.com/@ahawkinson/what-happens-when-the-world-wakes-up-c73a5c931c17.*

[18] Timothy B. Lee, "Everything's Connected: How Tiny Computers Could Change the Way We Live," *Vox* (Aug. 13, 2014), *http://www.vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live.*

[19] Kevin Ashton, "That "Internet of Things" Thing," *RFID Journal* (June 22, 2009), *http://www.rfidjournal.com/articles/view?4986.*

[20] *Ibid.*

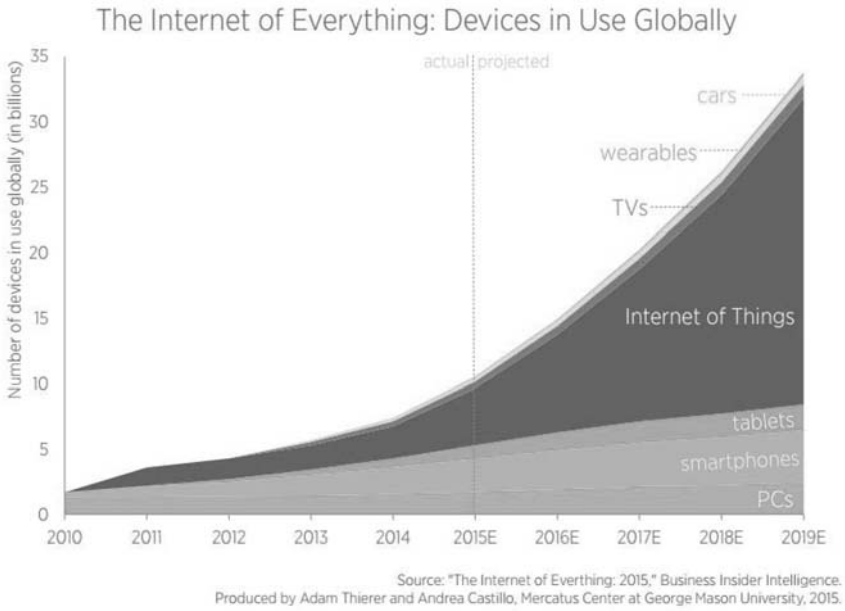
[21] Amy Collins, Adam J. Fleisher, D. Reed Freeman Jr., and Alistair Maughan, "The Internet of Things Part 1: Brave New World," *Client Alert* (Morrison Foerster), March 18, 2014, 1, *http://www.jdsupra.com/legalnews/the-internet-of-things-part-1-brave-new-23154.*

[22] See Patrick Thibodeau, "Explained: The ABCs of the Internet of Things," *Computerworld,* May 6, 2014, *http://www.computerworld.com/s/article/9248058/Explained__The__ABCs__of__the__Internet__of__Things__.*

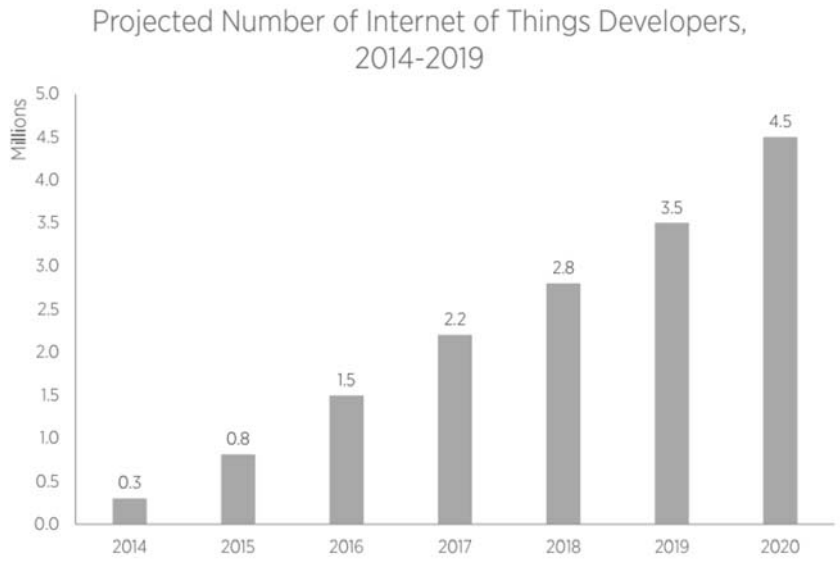
[23] Steve Lohr, "A Messenger for the Internet of Things," *N.Y. Times Bits,* April 25, 2013, *http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things.*

[24] Consumer Electronics Association, Comment to the Federal Trade Commission on Internet of Things, Project No. P135405 (June 10, 2013), 7.

[25] *Ibid.*



Source: "The Internet of Everthing: 2015," Business Insider Intelligence.
Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.



Source: "IoT: Breaking Free From Internet and Things," Vision Mobile, 2014.
Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

APPENDIX 3: PROJECTED USE AND ECONOMIC IMPACT OF THE INTERNET OF THINGS[26]

The Internet of Things is already growing at a breakneck pace and is expected to continue to accelerate rapidly. Below is a summary of recent forecasts regarding the growing device connectivity as well as potential economic benefits of the IoT.

A. Connectivity

- *Cisco* projects that 37 billion intelligent things will be connected and communicating by 2020.[27]
- *ABI Research* estimates that there are more than 10 billion wirelessly connected devices in the market today and more than 30 billion devices expected by 2020.[28]
- *IDC* (International Data Corporation) predicts far greater penetration of 212 billion devices installed globally by the end of 2020.[29]
- *Gartner* anticipates that 25 billion Internet of Things devices will be in operation by 2020.[30]
- *VisionMobile* projects that the number of IoT developers will grow from roughly 300,000 in 2014 to more than 4.5 million by 2020.[31]
- *Business Insider* estimates that will be a total of 23.4 billion Internet of Things devices connected by 2019 and that their adoption will be driven by the enterprise and manufacturing sectors.[32]
- *Harbor* projects that 21.7 billion Internet of Things devices will be connected and in use by 2019.[33]
- *Machina Research* reports that roughly 7.2 billion "machine-to-machine connected consumer electronic devices" will be in global use by 2023.[34]
- *Navigant Research* states that more than 1 billion smart meters will be installed globally by 2022, up from 313 million in 2013.[35]
- *IHS Automotive* anticipates that the number of cars connected to the Internet will grow more than six fold from 2013 to reach 152 million internationally by 2020.[36]
- *ON World* projects that roughly 100 million Internet-connected wireless lights will be in operation by 2020.[37]

---

[26] This section compiled with the assistance of Andrea Castillo, Program Manager of the Technology Policy Program at the Mercatus Center.

[27] Dave Evans, "Thanks to IoE, the Next Decade Looks Positively 'Nutty,'" *Cisco Blog,* February 12, 2013, *http://blogs.cisco.com/ioe/thanks-to-ioe-the-next-decade-looks-positively-nutty.*

[28] "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020" (Press Release, ABI Research, May 9, 2013), *https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne.*

[29] Antony Savvas, "Internet of Things Market Will Be Worth Almost $9 Trillion," *CNME,* October 6, 2013, *http://www.cnmeonline.com/news/internet-of-things-market-will-be-worth-almost-9-trillion.*

[30] "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015" (Press Release, Gartner, 2014), *http://www.gartner.com/newsroom/id/2905717.*

[31] Matt Asay, "The Internet of Things Will Need Millions of Developers by 2020," *ReadWrite,* June 27, 2014, *http://readwrite.com/2014/06/27/internet-of-things-developers-jobs-opportunity.*

[32] John Greenough, "The Enterprise Internet of Things Report: Forecasts, Industry Trends, Advantages, and Barriers for the Top IoT Sector," *Business Insider,* 2014, *https://intelligence.businessinsider.com/the-enterprise-internet-of-things-report-forecasts-industry-trends-advantages-and-barriers-for-the-top-iot-sector-2014–11.*

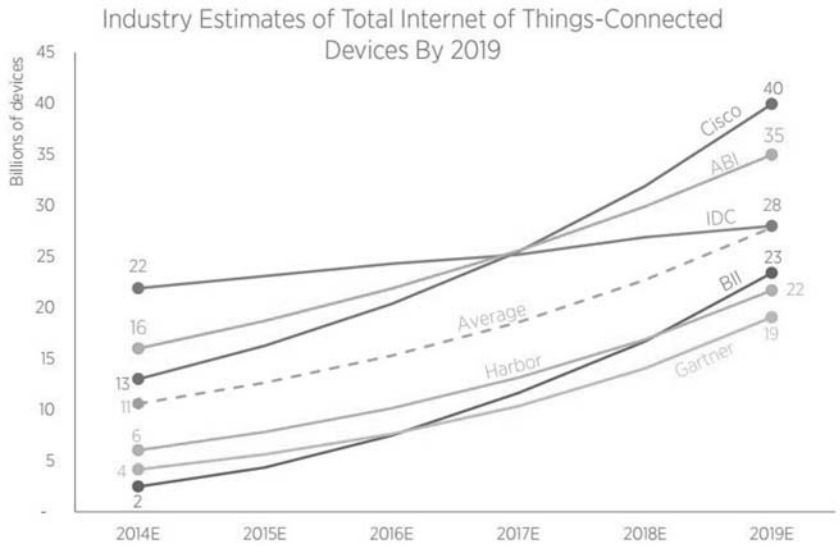
[33] Harbor Research, *Smart Systems and the Internet of Things Forecast* (2013), *http://harborresearch.com/wp-content/uploads/2013/08/Harbor-Research__2013-Forecast-Report__Prospectus.pdf.*

[34] "The Connected Life" (Press Release, Machina Research, 2014), *https://machinaresearch.com/static/media/uploads/machina__research__press__release__-__ce__report__-__2014__07__28.pdf.*

[35] Smart Electric Meters, "Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts," Navigant Research, *November 2013, http://www.navigantresearch.com/research/smart-meters.*

[36] "Emerging Technologies: Big Data in the Connected Car" (Press Release, IHS Automotive, November 2013), *http://press.ihs.com/press-release/country-industry-forecasting/big-data-drivers-seat-connected-car-technological-advance.*

[37] Mareca Hatler, Darryl Gurganious, and Charlie Chi, "Smart Wireless Lighting," *ON World,* 2013, *http://onworld.com/smartlighting.*



Source: "The Internet of Things Is Rising: How the IOT Market Will Grow Across Sectors," *BI Intelligence*, 2014.
Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

B. Economic Impact

- *McKinsey Global Institute* researchers estimate the potential economic impact of IoT technologies to be from $2.7 to $6.2 trillion per year by 2025.[38]
- *IDC* estimated in 2013 that this market would grow at a compound annual growth rate of 7.9 percent to reach $8.9 trillion by 2020.[39]
- *Cisco* analysts estimate that IoT will create $14.4 trillion in value between 2013 and 2022.[40]
- *Business Insider* estimates that IoT will add approximately $5.6 trillion in value to the global economy in between 2014 and 2019.[41]
- *Accenture* estimates that the industrial IoT could add $14.2 trillion to the global economy by 2030, and that the U.S. economy will gain at least $6.1 trillion in cumulative GDP by that year.[42]
- *General Electric* projects that industrial IoT technologies will add about $15 trillion to global GDP by 2030 (in constant 2005 dollars).[43]

---

[38] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," McKinsey, May 2013, *http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx.*

[39] Antony Savvas, "Internet of Things Market Will Be Worth Almost $9 Trillion," *CNME,* October 6, 2013, *http://www.cnmeonline.com/news/internet-of-things-market-will-be-worth-almost-9-trillion.*

[40] Joseph Bradley, Joel Barbier, and Doug Handler, "Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion," CISCO, 2013, *http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.*

[41] John Greenough, "The Enterprise Internet of Things Report: Forecasts, Industry Trends, Advantages, and Barriers for the Top IoT Sector," *Business Insider,* 2014, *https://intelligence.businessinsider.com/the-enterprise-internet-of-things-report-forecasts-industry-trends-advantages-and-barriers-for-the-top-iot-sector-2014-11.*

[42] "Winning with the Industrial Internet of Things" (Positioning Paper, Accenture, 2015), *http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDF.*

[43] Peter C. Evans and Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, 2012, *http://www.ge.com/docs/chapters/Industrial_Internet.pdf.*

- *Morgan Stanley* forecasts that driverless cars will save the U.S. economy $1.3 trillion per year once autonomous cars fully penetrate the market, while saving the world another $5.6 trillion a year.[44]

APPENDIX 4: A NONPARTISAN POLICY VISION FOR THE INTERNET OF THINGS[45]

What sort of public policy vision should govern the Internet of Things? I recently heard three public policymakers articulate their recommended vision for the Internet of Things (IoT), and I found their approach so inspiring that I wanted to discuss it here in the hopes that it will become the foundation for future policy in this arena.

On December 4, 2015, it was my pleasure to attend a Center for Data Innovation (CDI) event on "*How Can Policymakers Help Build the Internet of Things*?" As the title implied, the goal of the event was to discuss how to achieve the vision of a more fully connected world and, more specifically, how public policymakers can help facilitate that objective. It was a terrific event with many excellent panel discussions and keynote addresses.

Two of those keynotes were delivered by Senators Deb Fischer (R-Neb.) and Kelly Ayotte (R–N.H.). Below I offer some highlights from their remarks and then relate them to the vision set forth by Federal Trade Commission (FTC) Commissioner Maureen K. Ohlhausen in some of her recent speeches. I will conclude by discussing how the Ayotte-Fischer-Ohlhausen vision can be seen as the logical extension of the Clinton administration's excellent 1997 *"Framework for Global Electronic Commerce,"* which proposed a similar policy paradigm for the Internet more generally. This shows how crafting policy for the IoT can and should be a nonpartisan affair.

A. Sen. Deb Fischer's Remarks

In her *opening remarks* at the CDI event in December 2014, Sen. Deb Fischer explained how "the Internet of Things can be a game changer for the U.S. economy and for the American consumer." "It gives people more information and better tools to analyze data to make more informed choices," she noted.

After outlining some of the potential benefits associated with the Internet of Things, Sen. Fischer continued on to explain why it is essential we get public policy incentives right first if we hope to unlock the full potential of these new technologies. Specifically, she argued that:

> In order for Americans to receive the maximum benefits from increased connectivity, there are two things the government must avoid. First, policymakers can't bury their heads in the sand and pretend this technological revolution isn't happening, only to wake up years down the road and try to micromanage a fast-changing, dynamic industry.
>
> Second, the Federal Government must also avoid regulation just for the sake of regulation. We need thoughtful, pragmatic responses and narrow solutions to any policy issues that arise. For too long, the only "strategy" in Washington policy-making has been to react to crisis after crisis. We should dive into what this means for U.S. global competitiveness, consumer welfare, and economic opportunity before the public policy challenges overwhelm us, before legislative and executive branches of government—or foreign governments—react without all the facts.

Fischer concluded by noting, "It's entirely appropriate for the U.S. government to think about how to modernize its regulatory frameworks, consolidate, renovate, and overhaul obsolete rules. We're destined to lose to the Chinese or others if the Internet of Things is governed in the United States by rules that pre-date the VCR."

B. Sen. Kelly Ayotte's Remarks

Like Sen. Fischer, Ayotte similarly stressed the many economic opportunities associated with IoT technologies for both consumers and producers alike. Ayotte also noted that IoT is going to be a major topic for the Senate Commerce Committee. She said that the role of the Committee will be to ensure that the various agencies looking into IoT issues are not issuing "conflicting regulatory directives" and "that

---

[44] Ravi Shanker *et al.,* "Driverless Cars: Self-Driving the New Auto Industry Paradigm" (Blue Paper, Morgan Stanley, November 6, 2013), *http://www.wisburg.com/wp-content/uploads/2014/09/%ef%bc%88109-pages-2014%ef%bc%89morgan-stanley-blue-paper-autonomous-cars%ef%bc%9a-self-driving-the-new-auto-industry-paradigm.pdf.*

[45] This section is adapted from Adam Thierer, "A Nonpartisan Policy Vision for the Internet of Things," *Technology Liberation Front,* December 11, 2014, *http://techliberation.com/2014/12/11/a-nonpartisan-policy-vision-for-the-internet-of-things.*

what is being done makes sense and allows for future innovation that we can't even anticipate right now." Among the agencies she cited that are currently looking into IoT issues: FTC (privacy and security), FDA (medical device applications), FCC (wireless issues), FAA (commercial drones), NHTSA (intelligent vehicle technology), and NTIA (multi-stakeholder privacy reviews) as well as state lawmakers and regulatory agencies.

Sen. Ayotte then explained what sort of policy framework America needed to adopt to ensure that the full potential of the Internet of Things could be realized. She framed the choice lawmakers are confronted with as follows:

> We as policymakers we can either create an environment that allows that to continue to grow, or one that thwarts that. To stay on the cutting edge, we need to make sure that our regulatory environment is conducive to fostering innovation." [. . .] We're living in the Dark Ages in the ways the some of the regulations have been framed. Companies must be properly incentivized to invest in the future, and government shouldn't be a deterrent to innovation and job-creation.

Ayotte also stressed that "technology continues to evolve so rapidly there is no one-size-fits-all regulatory approach" that can work for a dynamic environment like this. "If legislation drives technology, the technology will be outdated almost instantly," and "that is why humility is so important," she concluded.

The better approach, she argued was to let technology evolve freely in a "*permissionless*" fashion and then see what problems developed and then address them accordingly. "[A] top-down, preemptive approach is never the best policy" and will only serve to stifle innovation, she argued. "If all regulators looked with some humility at how technology is used and whether we need to regulate or not to regulate, I think innovation would stand to benefit."

C. FTC Commissioner Maureen K. Ohlhausen

Fischer and Ayotte's remarks reflect a vision for the Internet of Things that FTC Commissioner Maureen K. Ohlhausen has articulated in recent months. In fact, Sen. Ayotte specifically cited Ohlhausen in her remarks.

Ohlhausen has actually delivered several excellent speeches on these issues and has become one of the leading public policy thought leaders on the Internet of Things in the United States today. One of her first major speeches on these issues was her October 2013 address entitled, "*The Internet of Things and the FTC: Does Innovation Require Intervention*?" In that speech, Ohlhausen noted that, "The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."

She also issued a wise word of caution to her fellow regulators:

> It is . . . vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.

In this and other speeches, Ohlhausen has highlighted the various other remedies that already exist when things do go wrong, including FTC enforcement of "unfair and deceptive practices," common law solutions (torts and class actions), private self-regulation and best practices, social pressure, and so on.

D. The Clinton Administration Vision

These three women have articulated what I regard as the ideal vision for fostering the growth of the Internet of Things. It should be noted, however, that their framework is really just an extension of the Clinton administration's outstanding vision for the Internet more generally.

In the 1997 "*Framework for Global Electronic Commerce,*" the Clinton administration outlined its approach toward the Internet and the emerging digital economy. As I've *noted* many times before, the framework was a succinct and bold market-oriented vision for cyberspace governance that recommended reliance upon civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve information-age problems. Specifically, it stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry." "[G]overnments should encourage industry self-regulation and

private sector leadership where possible" and "avoid undue restrictions on electronic commerce."

Sen. Ayotte specifically cited those Clinton principles in her speech and said, "I think those words, given twenty years ago at the infancy of the Internet, are today even more relevant as we look at the challenges and the issues that we continue to face as regulators and policymakers."

I completely agree. This is exactly the sort of vision that we need to keep innovation moving forward to benefit consumers and the economy, and this illustrates how IoT policy can be a bipartisan effort.

Why does this matter so much? As I noted in *this essay* from November 2014, thanks to the Clinton administration's bold vision for the Internet:

> This policy disposition resulted in an unambiguous green light for a rising generation of creative minds who were eager to explore this new frontier for commerce and communications. . . . The result of this freedom to experiment was an outpouring of innovation. America's info-tech sectors thrived thanks to permissionless innovation, and they still do today. An annual Booz & Company report on the world's most innovative companies revealed that 9 of the top 10 most innovative companies are based in the U.S. and that most of them are involved in computing, software, and digital technology.[46]

In other words, America had the policy right before and we can get the policy right again. Patience, flexibility, and forbearance are the key policy virtues that nurture an environment conducive to entrepreneurial creativity, economic progress, and greater consumer choice.

Other policymakers should endorse the vision originally sketched out by the Clinton administration and now so eloquently embraced and extended by Sen. Fischer, Sen. Ayotte, and Commissioner Ohlhausen. This is the path forward if we hope to realize the full potential of the Internet of Things.

APPENDIX 5: SOME INITIAL THOUGHTS ON THE FTC INTERNET OF THINGS REPORT[47]

On January 27, 2015, the Federal Trade Commission (FTC) released its long-awaited report on *"The Internet of Things: Privacy and Security in a Connected World."* The 55-page report is the result of a lengthy staff exploration of the issue, which kicked off with an FTC workshop on the issue that was held on November 19, 2013.

In this essay, I will offer a few general thoughts on the FTC's report and its overall approach to the Internet of Things and then discuss a few specific issues that I believe deserve further attention.

A. Big Picture, Part 1: Should Best Practices Be Voluntary or Mandatory?

Generally speaking, the FTC's report contains a variety of "best practice" recommendations to get Internet of Things innovators to take steps to ensure greater privacy and security "by design" in their products. Most of those recommended best practices are sensible as *general guidelines* for innovators, but the really sticky question here continued to be this: When, if ever, should "best practices" become binding regulatory requirements?

The FTC does a bit of a dance when answering that question. Consider how, in the executive summary of the report, the Commission answers the question regarding the need for additional privacy and security regulation: "Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature." But, just a few lines later, the agency (1) "reiterates the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral Federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach," and (2) "recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation."

Here and elsewhere, the agency repeatedly stresses that it is not seeking IoT-specific regulation, merely "broad-based" digital privacy and security legislation.

---

[46] Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," *Forbes,* February 12, 2012, *http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm.*

[47] This section is adapted from Adam Thierer, "Some Initial Thoughts on the FTC Internet of Things Report," *Technology Liberation Front,* January 28, 2015, *http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report.*

The problem is that once you understand what the IoT is all about you come to realize that this largely represents a distinction without a difference. The Internet of Things is simply the extension of the Net into everything we own or come into contact with. Thus, this idea that the agency is not seeking IoT-specific rule sounds terrific until you realize that it is actually seeking something far more sweeping—greater regulation of *all* online and digital interactions. And because "the Internet" and "the Internet of Things" will eventually (if they are not already) be consider synonymous, this notion that the agency is not proposing technology-specific regulation is really quite silly.

Now, it remains unclear whether there exists any appetite on Capitol Hill for "comprehensive" legislation of any variety, although perhaps we'll learn more about that possibility when the Senate Commerce Committee *hosts a hearing* on these issues on February 11. But at least so far, "comprehensive" or "baseline" digital privacy and security bills have been non-starters.

And that's for good reason in my opinion: Such regulatory proposals could take us down the path that Europe charted in the late 1990s with onerous "data directives" and suffocating regulatory mandates for the IT and computing sector. The results of this experiment have been unambiguous, as I documented in *congressional testimony* in 2013. I noted there how America's Internet sector came to be the envy of the world while it was hard to name any major Internet company from Europe. Whereas America embraced *"permissionless innovation"* and let creative minds develop one of the greatest success stories in modern history, the Europeans adopted a "Mother, may I?" regulatory approach for the digital economy. America's more flexible, light-touch regulatory regime leaves more room for competition and innovation compared to Europe's top-down regime. Digital innovation suffered over there while it blossomed here.

That's why we need to be careful about adopting the sort of "broad-based" regulatory regime that the FTC recommends in this and previous reports.

B. Big Picture, Part 2: Does the FTC Really Need More Authority?

Something else is going on in this report that has also been happening in all the FTC's recent activity on digital privacy and security matters: The agency has been busy laying the groundwork for its own expansion.

In this latest report, for example, the FTC argues that:

> Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections. . .. The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach.

In other words, this agency wants more authority. And we are talking about sweeping authority here that would transcend its *already sweeping* authority to police "unfair and deceptive practices" under Section 5 of the FTC Act. Let's be clear: It would be hard to craft a law that grants an agency more comprehensive and open-ended consumer protection authority than Section 5. The meaning of those terms—"unfairness" and "deception"—has always been a contentious matter, and at times the agency has abused its discretion by exploiting that ambiguity.

Nonetheless, Section 5 remains a powerful enforcement tool for the agency and one that has been wielded aggressively in recently years to police digital economy giants and small operators alike. Generally speaking, I'm alright with *most* Section 5 enforcement, especially since that sort of retrospective policing of unfair and deceptive practices is far less likely to disrupt *permissionless innovation* in the digital economy. That's because it does not subject digital innovators to the sort of "Mother, may I?" regulatory system that European entrepreneurs face. But an expansion of the FTC's authority via more "comprehensive, baseline" privacy and security regulatory policies threatens to convert America's more sensible bottom-up and responsive regulatory system into the sort of innovation-killing regime we see on the other side of the Atlantic.

Here's the other thing we can't forget when it comes to the question of what additional authority to give the FTC over privacy and security matters: The FTC is not the end of the enforcement story in America. Other enforcement mechanisms exist, including privacy torts, class action litigation, property and contract law, state enforcement agencies, and other targeted privacy statutes. I've summarized all these additional enforcement mechanisms in *my 2014 law review* article referenced above.

C. FIPPS, Part 1: Notice and Choice vs. Use-Based Restrictions

Let's drill down a bit and examine some of the specific privacy and security best practices that the agency discusses in its new IoT report.

The FTC report highlights how the IoT creates serious tensions for many traditional Fair Information Practice Principles (FIPPs). The FIPPs generally include (1) notice, (2) choice, (3) purpose specification, (4) use limitation, and (5) data minimization. But the report is mostly focused on notice and choice as well as data minimization.

When it comes to notice and choice, the agency wants to keep hope alive that it will still be applicable in an IoT world. I'm sympathetic to this effort because it is quite sensible for *all* digital innovators to do their best to provide consumers with adequate notice about data collection practices and then give them sensible choices about it. Yet, like the agency, I agree that "offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface."

The agency has a nuanced discussion of how context matters in providing notice and choice for IoT, but one can't help but think that even they must realize that the game is over, to some extent. The increasing miniaturization of IoT devices and the ease with which they suck up data means that traditional approaches to notice and choice just aren't going to work all that well going forward. It is almost impossible to envision how a rigid application of traditional notice and choice procedures would work in practice for the IoT.

Relatedly, as I *wrote in January 2015,* the Future of Privacy Forum (FPF) released a white paper entitled, "*A Practical Privacy Paradigm for Wearables,*" that notes how FIPPs "are a valuable set of high-level guidelines for promoting privacy, [but] given the nature of the technologies involved, traditional implementations of the FIPPs may not always be practical as the Internet of Things matures." That's particularly true of the notice and choice FIPPS.

But the FTC isn't quite ready to throw in the towel and make the complete move toward "use-based restrictions," as many academics have. Use-based restrictions would focus on specific uses of data that are particularly sensitive and for which there is widespread agreement they should be limited or disallowed altogether. But use-based restrictions are, ironically, controversial from both the perspective of industry and privacy advocates (albeit for different reasons, obviously).

The FTC doesn't really know where to go next with use-based restrictions. The agency says that, on one hand, "has incorporated certain elements of the use-based model into its approach" to enforcement in the past. On the other hand, the agency says it has concerns "about adopting a pure use-based model for the Internet of Things," since it may not go far enough in addressing the growth of more widespread data collection, especially of more sensitive information.

In sum, the agency appears to be keeping the door open on this front and hoping that a best-of-all-worlds solution miraculously emerges that extends *both* notice and choice and use-based limitations as the IoT expands. But the agency's new report doesn't give us any sort of blueprint for how that might work, and that's likely for good reason: because it probably won't work at that well in practice, and there will be serious costs in terms of lost innovation if they try to force unworkable solutions on this rapidly evolving marketplace.

D. FIPPS, Part 2: Data Minimization

The biggest policy fight that is likely to come out of this report involves the agency's push for data minimization. To minimize the risks associated with excessive data collection, the report recommends that:

> Companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or deidentify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data.

This is an unsurprising recommendation in light of the fact that, in *previous major speeches* on the issue, FTC Chairwoman Edith Ramirez argued that "information that is not collected in the first place can't be misused" and that:

> The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off chance that it might prove useful is not consistent with privacy best practices. And remember, not all data is created equally. Just as there is low quality iron ore and coal, there is low quality, unreliable data. And old data is of little value.

In *my forthcoming law review article,* I discussed the problem with such reasoning at length and note:

> If Chairwoman Ramirez's approach to a preemptive data use "commandment" were enshrined into a law that said, "Thou shall not collect and hold onto personal information unnecessary to an identified purpose." Such a precautionary limitation would certainly satisfy her desire to avoid hypothetical worst-case outcomes because, as she noted, "information that is not collected in the first place can't be misused," but it is equally true that information that is never collected may never lead to serendipitous data discoveries or new products and services that could offer consumers concrete benefits. "The socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection," *notes Ken Wasch,* president of the Software and Information Industry Association. If academics and lawmakers succeed in imposing such precautionary rules on the development of IoT and wearable technologies, many important innovations may never see the light of day.

FTC Commissioner Josh Wright issued a dissenting statement to the report that lambasted the staff for not conducting more robust cost-benefit analysis of the new proposed restrictions and specifically cited how problematic the agency's approach to data minimization was. "[S]taff merely acknowledges it would potentially curtail innovative uses of data . . . [w]ithout providing any sense of the magnitude of the costs to consumers of foregoing this innovation or of the benefits to consumers of data minimization," he says. Similarly, in her *separate statement,* FTC Commissioner Maureen K. Ohlhausen worried about the report's overly precautionary approach on data minimization when noting that, "without examining costs or benefits, [the staff report] encourages companies to delete valuable data—primarily to avoid hypothetical future harms. Even though the report recognizes the need for flexibility for companies weighing whether and what data to retain, the recommendation remains overly prescriptive," she concludes.

Regardless, the battle lines have been drawn by the FTC staff report as the agency has made it clear that it will be stepping up its efforts to get IoT innovators to significantly slow or scale back their data collection efforts. It will be very interesting to see how the agency enforces that vision going forward and how it impacts innovation in this space. All I know is that the agency has not conducted a serious evaluation here of the trade-offs associated with such restrictions. I penned another law review article in 2014 offering *"A Framework for Benefit-Cost Analysis in Digital Privacy Debates"* that they could use to begin that process if they wanted to get serious about it.

E. The Problem with the "Regulation Builds Trust" Argument

One of the interesting things about this and previous FTC reports on privacy and security matters is how often the agency premises the case for expanded regulation on "building trust." The argument goes something like this (as found on page 51 of the new IoT report): "Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected."

This is one of those commonly-heard claims that sounds so straight-forward and intuitive that few dare question it. But there are problems with the logic of the we-need-regulation-to-build-trust-and-boost-adoption arguments we often hear in debates over digital privacy.

First, the agency bases its argument mostly on polling data. "Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices," the report says. Well, of course surveys say that! It's only logical that consumers will say this, just as they will always say they value privacy and security more generally when asked. You might as well ask people if they love their mothers!

What consumers claim to care about and what they actually do in the real-world are often two very different things. In the real-world, people balance privacy and security alongside many other values, including choice, convenience, cost, and more. This leads to the so-called "privacy paradox," or the problem of many people saying one thing and doing quite another when it comes to privacy matters. Put simply,

people take some risks, including some privacy and security risks, to reap other rewards or benefits. (See *this essay* for more on the problem with most privacy polls.)

Second, online activity and the Internet of Things are both growing like gangbusters despite the privacy and security concerns that the FTC raises. Virtually every metric I've looked at that track IoT activity show astonishing growth and product adoption, and projections by all the major consultancies that have studied this consistently predict the continued rapid growth of IoT activity. Now, how can this be the case if, as the FTC claims, we'll only see the IoT really take off after we get more regulation aimed at bolstering consumer trust? Of course, the agency might argue that the IoT will grow *at an even faster clip* than it is right now, but there is no way to prove one way or the other. In any event, the agency cannot possible claim that the IoT isn't already growing at a very healthy clip. Indeed, a lot of the hand-wringing the staff engages in throughout the report is premised precisely on the fact that the IoT is exploding faster that our ability to keep up with it. In reality, it seems far more likely that *cost and complexity* are the bigger impediments to faster IoT adoption, just as cost and complexity have always been the factors weighing most heavily on the adoption of other digital technologies.

Third, let's say that the FTC is correct—and it is—when it says that *a certain amount* of trust is needed in terms of IoT privacy and security before consumers are willing to use more of these devices and services in their everyday lives. Does the agency imagine that IoT innovators don't know that? Are markets and consumers completely irrational?

The FTC says on page 44 of the report that, "If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust." Well, if such a mismatch does exist, then the assumption should be that consumers can and will push back or seek out new and better options. And other companies should be able to sense the market opportunity here to offer a more privacy-centric offering for those consumers who demand it to win their trust and business.

Finally, and perhaps most obviously, the problem with the argument that increased regulation will help IoT adoption is that it ignores how the regulations put in place to achieve greater "trust" might become so onerous or costly in practice that there won't be as many innovations for us to adopt to begin with! Again, regulation, even very well-intentioned regulation, has costs and trade-offs.

In any event, if the agency is going to premise the case for expanded privacy regulation on this notion, they are going to have to do far more to make their case besides simply asserting it.

F. Once Again, No Appreciation of the Potential for Societal Adaptation

Let's briefly shift to a subject that isn't discussed in the FTC's new IoT report at all.

Major reports and statements by public policymakers about rapidly-evolving emerging technologies are always initially prone to stress *panic* over patience. Rarely are public officials willing to step-back, take a deep breath, and consider how a resilient citizenry might adapt to new technologies as they gradually assimilate new tools into their lives.

That is really sad, when you think about it, since humans have again and again proven capable of responding to technological change in creative ways by adopting new personal and social norms. I won't belabor the point because I've already written volumes on this issue elsewhere. I tried to condense all my work into a single essay entitled, *"Muddling Through: How We Learn to Cope with Technological Change."* Here's the key takeaway:

> Humans have exhibited the uncanny ability to adapt to changes in their environment, bounce back from adversity, and learn to be resilient over time. A great deal of wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures while both developing new technologies and learning how to live with them. I believe it wise to continue to be open to new forms of innovation and technological change, not only because it provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve — and to learn from it. More often than not, I argue, citizens have found ways to adapt to technological change by employing a variety of coping mechanisms, new norms, or other creative fixes.

Again, you almost never hear regulators or lawmakers discuss this process of individual and social adaptation even though they must know there is something to it.

One explanation is that every generation has their own techno-boogeymen and lose faith in the ability of humanity to adapt to it.

To believe that we humans are resilient, adaptable creatures should not be read as being indifferent to the significant privacy and security challenges associated with any of the new technologies in our lives today, including IoT technologies. Overly exuberant techno-optimists are often too quick to adopt a "Just get over it!" attitude in response to the privacy and security concerns raised by others. But it is equally unreasonable for those who are worried about those same concerns to utterly ignore the reality of human adaptation to new technologies realities.

G. Why are Educational Approaches Merely an Afterthought?

One final thing that troubled me about the FTC report was the way consumer and business education is mostly an afterthought. This is one of the most important roles that the FTC can and should play in terms of explaining potential privacy and security vulnerabilities to the general public and product developers alike.

Alas, the agency devotes so much ink to the more legalistic questions about how to address these issues, that all we end up with in the report is this one paragraph on consumer and business education:

> Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

I applaud that language, and I very much hope that the agency is serious about plowing more effort and resources into developing new consumer and business education materials in this area. But I'm a bit surprised that the FTC report didn't even bother mentioning the excellent material already available on the *"On Guard Online"* website that it helped create with a dozen other Federal agencies. Worse yet, the agency failed to highlight the many other privacy education and "digital citizenship" efforts that are underway today to help on this front.

I hope that the agency spends a little more time working on the development of new consumer and business education materials in this area instead of trying to figure out how to craft a quasi-regulatory regime for the Internet of Things. As I noted in 2014 in this *Maine Law Review* article, that would be a far more productive use of the agency's expertise and resources. I argued there that "policymakers can draw important lessons from the debate over how best to protect children from objectionable online content" and apply them to debates about digital privacy. Specifically, after a decade of searching for legalistic solutions to online safety concerns—and convening a half-dozen blue ribbon task forces to study the issue—we finally saw a rough consensus emerge that no single "silver bullet" technological solutions or legal quick-fixes would work and that, ultimately, education and empowerment represented the better use of our time and resources. What was true for child safety is equally true for privacy and security for the Internet of Things.

It is a shame the FTC staff squandered the opportunity it had with this new report to highlight all the good that could be done by getting more serious about focusing first on those alternative, bottom-up, less costly, and less controversial solutions to these challenging problems. One day we'll all wake up and realize that we spent a lost decade debating legalistic solutions that were either technically unworkable or politically impossible. Just imagine if all the smart people who were spending all their time and energy on those approaches right now were instead busy devising and pushing educational and empowerment-based solutions instead!

One day we'll get there. Sadly, if the FTC report is any indication, that day is still a ways off.

APPENDIX 6: WHY "PERMISSIONLESS INNOVATION" MATTERS[48]

A. Innovation Policy: Attitudes Matter

"Why does economic growth . . . occur in some societies and not in others?" asked Joel Mokyr in his 1990 book, *Lever of Riches: Technological Creativity and Economic Progress.*[49] Debate has raged among generations of economists, historians, and business theorists over that question and the specific forces and policies that prompt long-term growth.

As varied as their answers have been, there was at least general agreement that *institutional* factors mattered most: it was really just a question of what mix of them would fuel the most growth. Those institutional factors include: government stability, the enforceability of contracts and property rights, tax and fiscal policies, trade policies, regulatory factors, labor costs, educational policies, research and development expenditures, infrastructure, demographics, and environmental factors.[50]

This leads many scholars and policymakers to speak of innovation policy as if it is simply a Goldilocks-like formula that entails tweaking various policy dials to get innovation *just right.*[51] Such thinking animates the Obama administration's "Strategy for American Innovation," which catalogs "policies to promote critical components of the American innovation ecosystem."[52] The White House claims its strategy plays a "critical role in guiding the development of new policy initiatives that can help unleash the transformative innovation that leads to long-term economic growth."[53]

Unfortunately, far less attention has been paid to the role that *values*—cultural attitudes, social norms, and political pronouncements—play in influencing opportunities for entrepreneurialism, innovation, and long-term growth.[54] Does a socio-political system respect what Deirdre McCloskey refers to as the "bourgeois virtues" that incentivize invention and propel an economy forward?[55] "A big change in the common opinion about markets and innovation," she has argued, "caused the Industrial Revolution, and then the modern world. . . . The result was modern economic growth."[56]

There are limits to how much policymakers can influence these attitudes and values, of course. Nonetheless, to the extent they hope to foster the positive factors that give rise to expanded entrepreneurial opportunities, policymakers should appreciate how growth-oriented innovation *policy* begins with the proper policy *disposition.*[57] As Mokyr notes, "technological progress requires above all tolerance toward the unfamiliar and the eccentric."[58]

For innovation and growth to blossom, entrepreneurs need a clear green light from policymakers that signals a general acceptance of risk-taking, especially risk-taking that challenges existing business models and traditional ways of doing

---

[48] This section is adapted from Adam Thierer, "Embracing a Culture of Permissionless Innovation" (Cato Policy Forum, Cato Institute, Washington, D.C., November 2014), *http://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation.*

[49] Joel Mokyr, *Lever of Riches: Technological Creativity and Economic Progress* (New York: Oxford University Press, 1990), 8–9.

[50] For a listing and discussion of these and other factors, see Robert D. Atkinson, "Understanding the U.S. National Innovation System," Information Technology and Innovation Foundation, June 2014, *http://www.itif.org/publications/understanding-us-national-innovation-system.*

[51] Michael Nelson, "Six Myths of Innovation Policy," The European Institute, Washington, D.C., July 2013, *http://www.europeaninstitute.org/EA-July-2013/perspectives-six-myths-of-innovation-policy.html.* ("On Capitol Hill and in Brussels, there seems to be a belief that if only governments adopt the right tax policies, adequately fund R&D, enforce patents and copyrights, and support manufacturing, innovative, then start-ups will pop up everywhere and supercharge economic growth. Unfortunately, that misses an underlying problem: In many parts of the U.S. and Europe, innovation is not really welcome. It is misunderstood and even feared.")

[52] White House, "Notice of Request for Information: Strategy for American Innovation," *Federal Register,* July 29, 2014, *https://www.federalregister.gov/articles/2014/07/29/2014-17761/strategy-for-american-innovation.*

[53] *Ibid.*

[54] Donald J. Boudreaux, "Deirdre McCloskey and Economists' Ideas about Ideas,'" *Online Library of Liberty,* July 2014, *http://oll.libertyfund.org/pages/mccloskey.*

[55] Deirdre N. McCloskey, *The Bourgeois Virtues: Ethics for an Age of Commerce* (Chicago: University of Chicago Press, 2006).

[56] Deirdre McCloskey, "Bourgeois Dignity: A Revolution in Rhetoric" (Cato Unbound, Cato Institute, Washington, D.C., October 4, 2010), *http://www.cato-unbound.org/2010/10/04/deirdre-mccloskey/bourgeois-dignity-revolution-rhetoric.*

[57] Randall Holcombe, "Entrepreneurship and Economic Growth," *The Quarterly Journal of Austrian Economics* 1, no. 2 (Summer 1998): 58, *http://mises.org/journals/qjae/pdf/qjae1_2_3.pdf,* ("When entrepreneurship is seen as the engine of growth, the emphasis shifts toward the creation of an environment within which opportunities for entrepreneurial activity are created, and successful entrepreneurship is rewarded.")

[58] Mokyr, *Lever of Riches,* 182.

things.[59] We can think of this disposition as "permissionless innovation." If there was one thing every policymaker could do to help advance long-term growth, it is to first commit themselves to advancing this ethic and making it the lodestar for all their future policy pronouncements and decisions.

B. Permissionless Innovation vs. the Precautionary Principle

While it would seem self-evident that pro-innovation attitudes matter and that a general embrace of risk-taking and commercial pursuits is crucial to unlocking entrepreneurial creativity and opportunities, scholars have typically failed to put a name on this disposition. "Permissionless innovation" is a phrase of recent (but uncertain) origin that nicely summarizes that vision. Permissionless innovation refers to the notion that experimentation with new technologies and business models should generally be permitted by default.[60] Unless a compelling case can be made that a new invention or business model will bring serious harm to individuals, innovation should be allowed to continue unabated, and problems, if they develop at all, can be addressed later.

Permissionless innovation is not an absolutist position that rejects any role for government. Rather, it is an aspirational goal that stresses the benefit of "innovation allowed" as the default position to begin policy debates. It switches the burden of proof to those who favor preemptive regulation and asks them to explain why ongoing trial-and-error experimentation with new technologies or business models should be disallowed.

This disposition stands in stark contrast to the sort of "precautionary principle" thinking that often governs policy toward emerging technologies. The precautionary principle refers to the belief that new innovations should be curtailed or disallowed until their developers can prove that they will not cause any harms to individuals, groups, specific entities, cultural norms, or various existing laws, norms, or traditions.[61]

When the precautionary principle's "better to be safe than sorry"[62] approach is applied through preemptive constraints, opportunities for experimentation and entrepreneurialism are stifled. While some steps to anticipate or to control for unforeseen circumstances are sensible, going overboard with precaution forecloses opportunities and experiences that offer valuable lessons for individuals and society. The result is less economic and social dynamism.

Innovation is more likely in systems that maximize breathing room for ongoing economic and social experimentation, evolution, and adaptation. Societies that appreciate those values—and allow them to influence both social norms and policy decisions—are likely to experience greater economic growth.[63] By contrast, those that deride such values and adopt a more precautionary policy approach are more likely to discourage innovation and languish economically.

Unlocking long-term growth opportunities, therefore, depends upon a rejection of precautionary principle thinking and an embrace of permissionless innovation as the default policy disposition.

C. The Secret Ingredient that Powered the Information Revolution

Consider how permissionless innovation powered the explosive growth of the Internet and America's information technology sectors (computing, software, Internet services, etc.) over the past two decades. Those sectors have ushered in a generation of innovations and innovators that are now the envy of the world.[64] This

---

[59] Mokyr, *Lever of Riches,* 12 ("Economic and social institutions have to encourage potential innovators by presenting them with the right incentive structure."); Bret Swanson, "More disruption, please," *TechPolicyDaily,* August 20, 2014, *http://www.techpolicydaily.com/technology/disruption-please/#sthash.PVUNga9N.dpuf* ("To reignite economic growth, we need a broad commitment to an open economy and robust entrepreneurship.").

[60] Thierer, *Permissionless Innovation.*

[61] Ibid., vii. See also Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science and Technology* 14 (2013): 309–86, *http://conservancy.umn.edu/handle/144225.*

[62] Indur M. Goklany, *The Precautionary Principle: A Critical Appraisal of Environmental Risk Assessment* (Washington, D.C.: Cato Institute, 2001), 3.

[63] Joshua C. Hall, John Pulito, and Benjamin J. VanMetre, "Freedom and Entrepreneurship: New Evidence from the 50 States" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, April 17, 2012), *http://mercatus.org/publication/freedom-and-entrepreneurship-new-evidence-50-states* ("There is a positive and statistically significant relationship between the level of economic freedom in a country and that country's total entrepreneurial activity.")

[64] See Bret Swanson, "The Exponential Internet," *Business Horizon Quarterly* (Spring 2014): 40–47, *http://www.uschamberfoundation.org/sites/default/files/article/foundation/BHQ-Spring12-Issue3-SwansonTheExponentialInternet.pdf.*

happened because the default position for the digital economy was permissionless innovation. No one had to ask anyone for the right to develop these new technologies and platforms.[65]

A series of decisions and statements in the mid-1990s paved the way, beginning with the Clinton administration's decision to allow commercialization of what was previously just the domain of government agencies and university researchers. Shortly thereafter, Congress passed, and President Clinton signed, the Telecommunications Act of 1996, which notably avoided regulating the Internet like earlier communications and media technologies. Later, in 1998, the Internet Tax Freedom Act was passed, which blocked governments from imposing discriminatory taxes on the Internet.

Perhaps most important, in 1997, the Clinton administration's released its "Framework for Global Electronic Commerce," outlining its approach toward the Internet and the emerging digital economy.[66] The framework was a succinct and bold market-oriented vision for cyberspace governance that recommended reliance upon civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve information age problems.[67] Specifically, it stated that "the private sector should lead [and] the Internet should develop as a market driven arena not a regulated industry."[68] "[G]overnments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce."[69]

This policy disposition resulted in an unambiguous green light for a rising generation of creative minds who were eager to explore this new frontier for commerce and communications. As Federal Trade Commission Commissioner Maureen K. Ohlhausen observes, "the success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."[70]

The result of this "freedom to experiment" was an outpouring of innovation. America's info-tech sectors thrived thanks to permissionless innovation, and they still do today. A 2013 Booz & Company report on the world's most innovative companies revealed that 9 of the top 10 most innovative companies are based in the United States and that most of them are involved in computing, software, and digital technology.

---

[65] Ibid., 46. ("The entrepreneurship and investment that has sustained such fast growth for so long is due, in substantial part, to light-touch government policies (at least compared to other industries. . . . There have been mistakes, but for the most part, scientists, entrepreneurs, and big investors have been allowed to build new things, try new products, challenge the status quo, cooperate, and compete. They have also been allowed to fail.") See also Bret Swanson, "Long Live the Risk Takers," *Business Horizon Quarterly* 8 (2013): 30, *http://www.uschamberfoundation.org/bhq/long-live-risk-takers* ("Failure is a core competency of capitalism and a key component of resilience. Wealth is about creating new ideas. New ideas can only emerge through experiments of science, technology, and enterprise, all of which must be capable of failure in order to generate newness. Failure flushes away bad ideas and points us toward good ones. The failures may at times harm individuals and waste resources—people lose jobs and investments can be lost. The larger effect, however, is to lift the economy to a higher plane of knowledge, efficiency, and resilience.")

[66] White House, "The Framework for Global Electronic Commerce," July 1997, *http://clinton4.nara.gov/WH/New/Commerce.*

[67] Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," *Forbes,* February 12, 2012, *http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm.*

[68] White House, "Framework for Global Electronic Commerce." (The document added that, "parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. . . . Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.")

[69] *Ibid.*

[70] Maureen K. Ohlhausen, "The Internet of Things and the FTC: Does Innovation Require Intervention?" Remarks before the U.S. Chamber of Commerce, Washington, D.C., October 18, 2013, *http://www.ftc.gov/speeches/ohlhausen/131008internetthingsremarks.pdf.*

2013: 10 Most Innovative Companies

2013 Rank		2012 Rank	Company	Geography	Industry	R&D Spend ($Bn)*
1	▸	1	Apple	United States	Computing & Electronics	3.4
2	▸	2	Google	United States	Software & Internet	6.8
3	▲	4	Samsung	South Korea	Computing & Electronics	10.4
4	▲	10	Amazon	United States	Software & Internet	4.6
5	▼	3	3M	United States	Industrials	1.6
6	▼	5	General Electric	United States	Industrials	4.5
7	▼	6	Microsoft	United States	Software & Internet	9.8
8	▲	9	IBM	United States	Software & Internet	6.3
9	New	-	Tesla Motors	United States	Automotive	0.3
10	New	-	Facebook	United States	Software & Internet	1.4

D. And What's Good for the Goose . . .

What's even more powerful about this story is how the information technology and "data-driven innovation" became the goose that laid the golden eggs for the broader U.S. economy.[71] Brink Linsdey has noted that "economists generally agree that information technology (IT) was behind the decade of high TFP [total factor productivity] growth that ran from the mid-1990s to the mid-2000s."[72] It also boosted overall economic growth during that period.[73]

If an embrace of permissionless innovation can unlock this sort of entrepreneurial energy within the information technology sectors, it can also provide a shot in the arm to other sectors. The rest of the economy could certainly use such a boost since "the evidence of a real decline in business dynamism keeps stacking up."[74]

---

[71] A study commissioned by the Direct Marketing Association, John Deighton of Harvard Business School and Peter Johnson of Columbia University found that data-driven marketing added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012. See also John Deighton and Peter A. Johnson, "The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy," Data-Driven Marketing Institute, New York, NY, 2013, *http://ddminstitute.thedma.org/#valueofdata.* Major reports from economic consultancies Gartner and McKinsey Global Institute have also documented significant consumer benefits from "big data" across multiple sectors. See Gartner, "Gartner Says Big Data Will Drive $28 Billion of IT Spending in 2012," October 17, 2012, *http://www.gartner.com/newsroom/id/2200815;* James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey, May 2011, 97–106, *http://www.mckinsey.com/insights/business☒technology/big_data_the_next_frontier_for_innovation.*

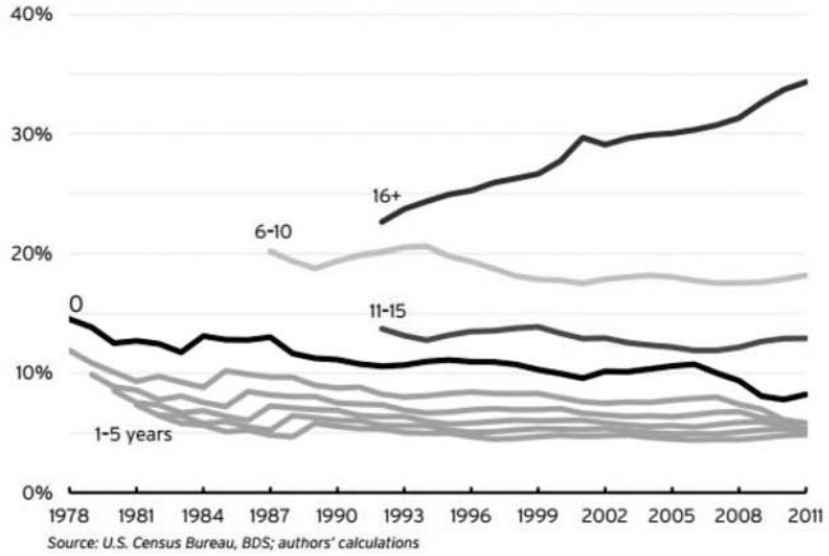
[72] Lindsey, "Why Growth Is Getting Harder," 14.

[73] Harold Furchtgott-Roth and Jeffrey Li, "The Contribution of the Information, Communications, and Technology Sector to the Growth of U.S. Economy: 1997–2007" (Research Paper, Center for the Economics of the Internet, Hudson Institute, Washington, D.C., August 2014), *http://hudson.org/content/researchattachments/attachment/1425/m0810_2.pdf* ("For the years 1997–2002, we find the sector contributed 19 percent of measurable economic gross output growth, or more than 582 billion 2013 dollars. For the period 2002–2007, we find the sector contributed 9.3 percent of gross output growth, or more than 340 billion 2013 dollars.")

[74] Richard Florida, "The Troubling Decline of American Business Dynamism," *The Atlantic City Lab,* July 31, 2014, http://www.citylab.com/work/2014/07/the-troubling-decline-of-american-business-dynamism/375353.

Figure 1.

Distribution of Total Firms by Firm Age in Years (1978-2011)



Recent studies "suggest that incentives for entrepreneurs to start new firms in the United States have diminished over time"[75] and that this is hurting job creation and productivity.[76] Two recent Brookings Institution studies by Ian Hathaway and Robert E. Litan also documented a decline in business dynamism in the American economy across a broad range of sectors—including a "precipitous drop since 2006 [that] is both noteworthy and disturbing"[77]—as well as the increased "aging" of businesses, with the share of older firms in the U.S. economy increasing by 50 percent over the past two decades.[78]

Many different institutional factors affect business dynamism, especially the regulatory environment that new startups face. "If you look over time, the number of rules has just proliferated," says Litan. "The cumulative weight of regulation—federal, state and local—is probably the most important impediment to starting a business."[79] Unfortunately, many current public policies "are rife with barriers to entrepreneurship, competition, innovation, and growth," notes Lindsey.[80]

As a result, "the regulatory environment in the United States has become less favorable to private-sector activity in recent years compared to other countries," a

[75] Ryan Decker, John Haltiwanger, Ron Jarmin, and Javier Miranda, "The Role of Entrepreneurship in U.S. Job Creation and Economic Dynamism," *Journal of Economic Perspectives* 28, no. 3 (Summer 2014): 4, *http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.28.3.3.*

[76] Robert J. Samuelson, "Where have all the entrepreneurs gone?" *Washington Post,* August 6, 2014, *http://www.washingtonpost.com/opinions/robert-samuelson-where-have-all-the-entrepreneurs-gone/2014/08/06/e01e7246-1d7c-11e4-82f9-2cd6fa8da5c4_story.html.*

[77] Ian Hathaway and Robert E. Litan, "Declining Business Dynamism in the United States: A Look at States and Metros" (Economic Studies at Brookings, Brookings Institution, Washington, D.C., May 2014), *http://www.brookings.edu/research/papers/2014/05/declining-business-dynamism-litan.*

[78] Ian Hathaway and Robert E. Litan, "The Other Aging of America: The Increasing Dominance of Older Firms" (Economic Studies at Brookings, Brookings Institution, Washington, D.C., July 2014), *http://www.brookings.edu/research/papers/2014/07/aging-america-increasing-dominance-older-firms-litan.*

[79] Quoted in Rick Newman, "What Obama Gets Wrong about Corporate America," *Yahoo Finance,* August 4, 2014, *http://finance.yahoo.com/news/what-obama-gets-wrong-about-corporate-america-200338595.html.*

[80] Lindsey, "Why Growth Is Getting Harder," 18.

Mercatus Center report concluded.[81] This is especially true for new start-ups.[82] Even if it is the case that "established firms that have the experience and resources to deal with [regulatory burdens]," Litan notes, the cumulative effect of regulations ends up hampering innovation by new, smaller firms.[83]

The reason this is important is not just because "business dynamism is inherently disruptive," as Hathaway and Litan note, "but [that] it is also critical to long-run economic growth" since "a dynamic economy constantly forces labor and capital to be put to better uses."[84] Thus, because economists widely acknowledge that "young firms are known to play a central role in job creation,"[85] it is especially important that policymakers get their signals right.

Again, an embrace of permissionless innovation is the way out of this conundrum.

E. Operationalizing the Vision

Patience, flexibility, and forbearance are the key policy virtues that nurture an environment conducive to entrepreneurial creativity. As the FTC's Ohlhausen argues, it is "vital that government officials. . .approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required."[86]

Beyond its importance as an aspirational vision, permissionless innovation can guide policy in concrete ways, especially regulatory policies. Possible reforms include regulatory streamlining[87] and flexibility requirements,[88] "sunsetting" provisions,[89] better benefit-cost analysis,[90] and a greater reliance on potential non-regulatory remedies—education, empowerment, transparency, industry self-regulation, etc.—before resorting to preemptive controls on new forms of innovation. Relying on common law solutions is also preferable to top-down administrative controls.[91]

---

[81] See also Steven Globerman and George Georgopoulos, "Regulation and the International Competiveness of the U.S. Economy" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, September 18, 2012), 4, *http://mercatus.org/publication/regulation-and-international-competitiveness-us-economy.*

[82] Jason J. Fichtner and Jakina R. Debnam, "Reducing Debt and Other Measures for Improving U.S. Competitiveness" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 13, 2012), *http://mercatus.org/publication/reducing-debt-and-other-measures-improving-us-competitiveness* ("Regulations have been historically biased toward existing technologies and increasing regulatory burdens on new entrants to a sector. This negatively impacts growth, and increases prices for consumers.")

[83] Quoted in Robert J. Samuelson, "Where Have All the Entrepreneurs Gone?" *Washington Post,* August 6, 2014, *http://www.washingtonpost.com/opinions/robert-samuelson-where-have-all-the-entrepreneurs-gone/2014/08/06/e01e7246-1d7c-11e4-82f9-2cd6fa8da5c4_story.html.*

[84] Hathaway and Litan, "Declining Business Dynamism," 1.

[85] Chiara Criscuolo, Peter N. Gal, and Carlo Menon, "DynEmp: New Cross-Country Evidence on the Role of Young Firms in Job Creation, Growth, and Innovation," *Vox,* May 26, 2014, *http://www.voxeu.org/article/dynemp-new-evidence-young-firms-role-economy.*

[86] Maureen K. Ohlhausen, "The Internet of Things and the FTC: Does Innovation Require Intervention?," Remarks before the U.S. Chamber of Commerce, Washington, D.C., October 18, 2013, *http://www.ftc.gov/speeches/ohlhausen/131008internetthingsremarks.pdf.*

[87] Sherzod Abdukadirov, "Evaluating Regulatory Reforms: Lessons for Future Reforms" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, May 29, 2014), *http://mercatus.org/publication/evaluating-regulatory-reforms-lessons-future-reforms;* Joshua C. Hall and Michael Williams, "A Process for Cleaning Up Federal Regulations" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, December 20, 2012), *http://mercatus.org/publication/process-cleaning-federal-regulations.*

[88] Richard Epstein, "Can Technological Innovation Survive Government Regulation?" *Harvard Journal of Law and Public Policy* 36, no. 1 (Winter 2013), *http://www.harvard-jlpp.com/wp-content/uploads/2013/01/36_1_087_Epstein_Tech.pdf* ("What is at stake in this area is nothing less than the question of how to preserve technical innovation in the face of wall-to-wall regulation. The prognosis is grim. Unless we reform agencies like the FDA and their procedures and operations, this country will suffer from a long-term drag on innovation that could, if the trend is not abated, lead to long-term mediocrity, as inventors and scientists flee our shores for friendlier environments. The pace of regulation is one of the central issues of our time.")

[89] Adam Thierer, "Sunsetting Technology Regulation: Applying Moore's Law to Washington," *Forbes,* March 25, 2012, *http://www.forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington;* Patrick McLaughlin, "A Solution to the Old Rules vs. New Tech Problem," *The Hill,* July 8, 2014, *http://mercatus.org/expert_commentary/solution-old-rules-vs-new-tech-problem.*

[90] See Susan E. Dudley and Jerry Brito, *Regulation: A Primer,* 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2012).

[91] See Thierer, *Permissionless Innovation,* 74–78.

F. Conclusion: Reasons for Optimism

In sum, attitudes matter as much as institutional factors in understanding what drives innovation and long-term growth, and there are reasons for optimism if policymakers embrace permissionless innovation as their default policy disposition.

Pessimists who predict permanent productivity and growth slowdown shouldn't forget that "the rate of growth of productivity at the frontiers of knowledge is especially difficult to predict; and it is unwise to underestimate human ingenuity," as Federal Reserve Vice Chairman Stanley Fischer noted in a 2014 speech.[92] While "it is difficult to know exactly in which direction technological change will move and how significant it will be," Joel Mokyr reminds us that, "something can be learned from the past, and it tells us that such pessimism is mistaken. The future of technology is likely to be bright."[93] Contrary to the belief that all the "low-hanging fruit" has already been picked, Mokyr notes that "we can also plant new trees that will grow fruits that no one today can imagine."[94]

Getting the disposition right will be more important than ever with so many exciting—but potentially highly disruptive—technologies starting to emerge, including the "sharing economy;"[95] 3D printing; the "Internet of Things" and wearable technology;[96] digital medicine; virtual reality and augmented reality technologies; commercial drone services;[97] autonomous vehicles;[98] and various robotic technologies.[99]

Permissionless innovation can help spur the next great industrial revolution by unlocking amazing opportunities in these and other arenas, boosting long-term growth in the process.

---

[92] Stanley Fischer, "The Great Recession—Moving Ahead," a Conference Sponsored by the Swedish Ministry of Finance, Stockholm, Sweden, August 11, 2014, *http://www.federalreserve.gov/newsevents/speech/fischer20140811a.htm.*

[93] Joel Mokyr, "The Next Age of Invention," *City Journal,* Winter 2014, *http://www.city-journal.org/2014/24_1_invention.html.*

[94] *Ibid.*

[95] Adam Thierer, "The Debate over the Sharing Economy: Talking Points & Recommended Reading," *Technology Liberation Front,* September 26, 2014, *http://techliberation.com/2014/09/26/the-debate-over-the-sharing-economy-talking-points-recommended-reading.*

[96] Adam Thierer, "Slide Presentation: Policy Issues Surrounding the Internet of Things & Wearable Technology," *Technology Liberation Front,* September 12, 2014, *http://techliberation.com/2014/09/12/slide-presentation-policy-issues-surrounding-the-internet-of-things-wearable-technology.*

[97] Jerry Brito, Eli Dourado, and Adam Thierer, "Federal Aviation Administration: Unmanned Aircraft System Test Site Program Docket No: FAA–2013–0061" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, April 23, 2013), *http://mercatus.org/publication/federal-aviation-administration-unmanned-aircraft-system-test-site-program;* Eli Dourado, "The Next Internet-Like Platform for Innovation? Airspace. (Think Drones)," *Wired,* April 23, 2013, *http://www.wired.com/opinion/2013/04/then-internet-now-airspace-dont-stifle-innovation-on-the-next-great-platform;* Adam Thierer, "Filing to FAA on Drones & 'Model Aircraft'," *Technology Liberation Front,* September 23, 2014, *http://techliberation.com/2014/09/23/filing-to-faa-on-drones-model-aircraft.*

[98] Adam Thierer and Ryan Hagemann, "Removing Roadblocks to Intelligent Vehicles and Driverless Cars" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, September 17, 2014), *http://mercatus.org/publication/removing-roadblocks-intelligent-vehicles-and-driverless-cars.*

[99] Adam Thierer, "Problems with Precautionary Principle-Minded Tech Regulation & a Federal Robotics Commission," *Medium,* September 22, 2014, *https://medium.com/@AdamThierer/problems-with-precautionary-principle-minded-tech-regulation-a-federal-robotics-commission-c71f6f20d8bd.*

APPENDIX 7: HOW WE ADAPT TO TECHNOLOGICAL CHANGE [100]

A. From Resistance to Resiliency

Citizen attitudes about these technologies will likely follow a cycle that has played out in countless other contexts. That cycle typically witnesses initial *resistance,* gradual *adaptation,* and then eventual *assimilation* of a new technology into society.[101] Some citizens will begin their relationship with these new technologies in a defensive crouch. In the extreme, if there is enough of a backlash, the initial resistance to these technologies might take the form of a full-blown "technopanic." [102]

Over time, however, citizens tend to learn how to adapt to new technologies or at least become more resilient in the face of new challenges posed by modern technological advances. Andrew Zolli and Ann Marie Healy, authors of *Resilience: Why Things Bounce Back,* define *resilience* as "the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances." [103] They continue:

> To improve your resilience is to enhance your ability to resist being pushed from your preferred valley, while expanding the range of alternatives that you can embrace if you need to. This is what researchers call *preserving adaptive capacity*—the ability to adapt to changed circumstances while fulfilling one's core purpose—and it's an essential skill in an age of unforeseeable disruption and volatility.[104]

Consequently, they note, "by encouraging adaptation, agility, cooperation, connectivity, and diversity, resilience-thinking can bring us to a different way of being in the world, and to a deeper engagement with it." [105]

Those who propose more precautionary solutions to challenging social problems often ignore this uncanny ability of individuals and institutions to "bounce back" from technological disruptions and become more resilient in the process. Part of the reason precautionary thinking sometimes dominates discussions about emerging technologies is that many people hold a deep-seated pessimism about future developments and a belief that, with enough preemptive planning, they can anticipate and overcome any number of hypothetical worst-case scenarios. Consequently, their innate tendency not only to be pessimistic but also to want greater certainty about the future means that "the gloom-mongers have it easy," notes author Dan Gardner.[106] "Their predictions are supported by our intuitive pessimism, so they *feel* right to us. And that conclusion is bolstered by our attraction to certainty." [107] Clive Thompson, a contributor to *Wired* and the *New York Times Magazine,* also notes that "dystopian predictions are easy to generate" and "doomsaying is emotionally self-protective: if you complain that today's technology is wrecking the culture, you can tell yourself you're a gimlet-eyed critic who isn't hoodwinked by high-tech trends and silly, popular activities like social networking. You seem like someone who has a richer, deeper appreciation for the past and who stands above the triviality of today's life." [108]

Luckily, as science reporter Joel Garreau reminds readers, "the good news is that end-of-the-world predictions have been around for a very long time, and none of them has yet borne fruit." [109] Doomsayers have a bad track record because they

---

[100] This section adapted from Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, November 2015), which will be published in the *Richmond Journal of Law and Technology* 21, no. 6 (2015), *http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.*

[101] *See* Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minn. J. L. Sci. & Tech.* 14 (2013): 309.

[102] *Ibid.,* 53–60.

[103] Andrew Zolli and Ann Marie Healy, *Resilience: Why Things Bounce Back* (New York: Simon & Schuster, 2012).

[104] *Ibid.,* 7–8.

[105] *Ibid.,* 16.

[106] Dan Gardner, *Future Babble: Why Pundits Are Hedgehogs and Foxes Know Best* (New York: Plume, 2012), 140–1.

[107] John Seely Brown and Paul Duguid, "Response to Bill Joy and the Doom-and-Gloom Technofuturists," in Albert H. Teich, Stephen D. Nelson, Celia McEnaney, and Stephen J. Lita, editors, *AAAS Science and Technology Policy Yearbook* (Washington, D.C.: American Association for the Advancement of Science, 2001), 79.

[108] Clive Thompson, *Smarter Than You Think: How Technology Is Changing Our Minds for the Better* (New York: Penguin, 2014), 283.

[109] Joel Garreau, *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies—and What It Means to Be Human* (New York: Broadway Books, 2006), 148.

typically ignore how "humans shape and adapt [technology] in entirely new directions."[110] "Just because the problems are increasing doesn't mean solutions might not also be increasing to match them," Garreau correctly notes.[111]

In their 2001 "Response to Doom-and-Gloom Technofuturists," John Seely Brown and Paul Duguid note that "technological and social systems shape each other. . . . [They] are constantly forming and reforming new dynamic equilibriums with far-reaching implications." "Social and technological systems do not develop independently," they continue. Rather, "the two evolve together in complex feedback loops, wherein each drives, restrains, and accelerates change in the other."[112]

This is how humans become more resilient and prosper, even in the face of sweeping technological change. Wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures while both developing new technologies and learning how to live with them.[113] Citizens should remain open to new forms of technological change not only because doing so provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve—and to learn from that change. More often than not, citizens find creative ways to adapt to technological change by using a variety of coping mechanisms, new norms, or other creative fixes. Although some things are lost in the process, something more is typically gained, including lessons about how to deal with subsequent disruptions.

Case Study: The Rise of Public Photography

Consider the jarring impact that the rise of the camera and public photography had on American society in the late 1800s.[114] This case study has implications for the debate over wearable technologies. Plenty of critics existed, and many average citizens were probably outraged by the spread of cameras[115] because "for the first time photographs of people could be taken without their permission—perhaps even without their knowledge," notes Lawrence M. Friedman in his 2007 book, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy.*[116]

In fact, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay "The Right to Privacy," decries the spread of public photography. The authors lament that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claim that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[117]

Despite the profound disruption caused by cameras and public photography, personal norms and cultural attitudes evolved quite rapidly as cameras became a central part of the human experience. In fact, instead of shunning cameras, most people quickly looked to buy one. At the same time, social norms and etiquette evolved to address those who would use cameras in inappropriate or privacy-invasive ways. In other words, citizens bounced back and became more resilient in the face of technological adversity.

Although some limited legal responses were needed to address the most egregious misuses of cameras, for the most part the gradual evolution of social norms, public pressure, and other coping mechanisms combined to solve the "problem" of public photography. In much the same way IoT and wearable technology will likely see a similar combination of factors at work as individuals and society slowly adjust to the new technological realities of the time. The public will likely develop coping mechanisms to deal with the new realities of a world of wearable technologies and become more resilient in the process.

That being said, resiliency should not be equated with complacency or a "Just get over it!" attitude toward privacy and security issues. With time, it may very well be the case that people "get over" *some* of the anxieties they might hold today con-

---

[110] *Ibid.,* 95.

[111] *Ibid.,* 154.

[112] Brown and Duguid, *supra* note 106, 79, 82, 83.

[113] Thierer, *Permissionless Innovation,* viii.

[114] This section was condensed from Thierer, "Technopanics."

[115] For a discussion of the anxieties caused by photography during this time, see Robert E. Mensel, *Kodakers Lying in Wait: Amateur Photography and the Right of Privacy in New York, 1885–1915, Amer. Quar.* 43 (March 1991): 24.

[116] Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy* (Palo Alto, CA: Stanford University Press, 2007), 214.

[117] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harv. L. Rev.* 4 (1890): 193, 195.

cerning these new technologies, but in the short run, IoT and wearable technologies will create serious social tensions that deserve serious responses.[118]

The CHAIRMAN. Thank you, Mr. Thierer.

Mr. Brookman?

STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY PROJECT, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. BROOKMAN. Thank you, Chairman Thune, Ranking Member Nelson, members of the Committee. I very much appreciate the opportunity to testify here today.

I am here today on behalf of the Center for Democracy & Technology. We are a digital rights advocacy group based here in D.C. where I head up our work on commercial data privacy.

So let me start by saying as a consumer advocate I am extremely optimistic about the value of what that Internet of Things devices can deliver for everyday citizens. Smart cards and infrastructure have the capacity to save lives, reduce travel times, and reduce our dependence on oil. Connected medical devices have the potential to revolutionize health care, giving patients constant real-time data about their medical conditions without tethering them to a hospital bed or medical facility. And already today smart phones, computers, TVs mean the wealth of the world's information is always at our fingertips, and on a whim, we have the ability to watch any movie, listen to any song, or read any book we want.

But some consumers are nervous about the sudden proliferation of Internet of Things devices and worry about too much exposure of their personal information. If the Internet of Things is going to be fully realized, there are a few policy challenges we are going to need to confront: first, poor data security practices; second, unexpected or unwanted data collection; third, a loss of control over our own devices; and fourth, potential government abuse of these technologies. I am going to go through each of these concerns.

An overarching theme is that Internet of Things products need to be designed with privacy and security and user empowerment in mind. Otherwise, the actions of a few careless actors may fundamentally stunt innovation of these incredibly powerful technologies.

So first let us talk about data security. Unfortunately, far too many Internet of Things devices built today are developed with security as an afterthought. Even at this early stage, we have seen all sorts of IoT devices be vulnerable to attack. Home alarm systems have been hacked. Baby monitors have been hacked. Smart refrigerators and toasters have been hacked. Medical devices, routers, thermostats—you mentioned, Senator Markey, in the *60 Minutes* report that smart vehicles may be vulnerable to attack. The list goes on and on. We absolutely need to find a better way to incentivize rigorous security practices built into products from the beginning because the status quo is not cutting it.

---

[118] Adam Thierer, "Can We Adapt to the Internet of Things?," *Privacy Perspectives,* June 19, 2013, *https://www.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things.*

Smart devices also need to be designed to make sure that data collection is consistent with consumer expectations and desires. Again, you mentioned that Samsung has been in the news this week for language in its terms of service saying it had the right to record and send to an unnamed company any conversations you have around your Smart TV in order to improve its voice recognition capabilities. Now, I suspect that Samsung's actual data collection practices are much more limited, but it is very hard for an ordinary consumer to know. And it raises a really important question. Just because a device can collect some personal data that might be useful one day, should it? A consumer might be okay with constant voice or even constant video collection going on all the time to make their device better; they might not. Ultimately, consumers should be empowered to make that choice and to control what the devices collect about them.

Connected devices also need to be configured to allow consumers to use them however they want and not to artificially constrain their choices. As one example, Keurig, the single-cup coffeemaker, configured their latest smart coffee machines to only work with Keurig-approved coffee pods, limiting consumers' ability to use their own machines to make whatever coffee they wanted. Here at least, the market seems to have noticed. Amazon reviews of these new machines are extremely critical of this feature and sales have fallen. I encourage Internet of Things designers to keep this case study in mind and make sure they are creating functionality that serves the consumers, the person who paid money for these products.

And finally, we fundamentally need to reform our government access and intelligence laws to make sure that consumers trust the Internet of Things. Forrester Research recently released a report dealing with the Snowden revelations about the PRISM program could result in a net loss of $180 billion to the U.S. IT sector by 2016. And that is just one program. Internet of Things devices are especially vulnerable to these fears. These devices have the potential to collect vast amounts of incredibly sensitive information about us, information that might be available without a warrant under the PATRIOT Act. If the Government wants access to this data about us, there need to be robust, due process requirements in place to make sure that consumers are confident that these databases will not be abused. At the end of the day, consumers need to trust the Internet of Things is working for them.

Thank you very much, and I look forward to discussing this further.

[The prepared statement of Mr. Brookman follows:]

PREPARED STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY, CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology (CDT) is pleased to submit testimony to the Senate Committee on Commerce, Science, and Transportation for today's hearing on the privacy and security implications of the Internet of Things (IoT).

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. I currently serve as the Director of CDT's Consumer Privacy Project. Our project focuses on issues surrounding consumer data, and I have previously testified before Congress on issues such as data breach notification legislation, commercial privacy, and cybersecurity.

The Internet of Things presents amazing opportunities for enriching citizens' lives. As consumer advocates, CDT is extremely enthusiastic about the potential advances to public health, the environment, education, and quality of life that will be brought about by the coming wave of IoT devices. However, in order to achieve this enormous potential for improving the lives of Americans, these sensor-and internet-enabled devices must be purposefully designed with consumer privacy and empowerment in mind. My testimony today will address four key policy areas that must be addressed for the Internet of Things to be fully realized: weak data security practices, unexpected and unwanted secondary data collection and use, diminishing user control over their own devices, and the potential for law enforcement and intelligence abuse. Companies must respond to these challenges, or user adoption of these valuable and even life-saving technologies will be dramatically stunted.

I. The transformative potential of the Internet of Things

We read about new *smart* technologies seemingly every day: keyless cars that you start with a cell phone, refrigerators that automatically order eggs when you've run out, dog collars equipped with GPS trackers, and even baby booties that monitor a child's heart rate and oxygen levels. This is a remarkable time for innovation and growth. According to recent reports, 26 to 30 *billion* devices will be connected to wireless Internet by 2020. This means in just five years, the number of connected gadgets could grow to over 30 times its size in 2009.[1]

In addition to their *cool factor,* smart devices enhance healthcare, education, finance, agriculture, and a number of other fields. Connected cities are also starting to leverage these technologies regularly: Philadelphia has saved over $1 million by placing smart garbage cans around the city that alert sanitation workers when pick-up is necessary; New York City plans to convert outdated public pay phones into free open WiFi hotspots.[2]

In many ways, consumers have already embraced many smart Internet of Things devices. Over 70 percent of Americans now own a smartphone, giving each of us access to the wealth of the world's information at our fingertips as we go about everyday life.[3] Many of us have smart TVs or smart DVD players, meaning we have access not just to what's on TV or in our video library, but we can connect to Netflix, Amazon, or YouTube to watch virtually anything, or use Skype or Hangouts to call a loved one. In the near future, smart car technologies have the potential to dramatically reduce accidents, improve traffic flows, and reduce greenhouse gas emissions.

Without question, IoT has real revolutionary potential. However efforts to make all of our things smarter raise unique consumer protection concerns. Reports of major electronics companies planning to connect *all* of its consumer devices to the Internet in the next five years[4] suggests the question: do consumers want *everything* to be smart? Is there a meaningful use case for a *smart toaster*? Even if there are incremental advantages to some connected devices, might the downsides in some cases outweigh the benefits? Unfortunately, some poor design decisions today are compromising the revolutionary potential of the Internet of Things, with the potential result that many if not most consumers will reject many of these innovations.

Smart technologies often involve the mass collection, storing and sharing individuals' data. While much of this is necessary and unobjectionable—the very nature of some devices (such as health wearables) is to track a user's data for that user's benefit—certain data practices seriously threaten individuals' security and right to privacy.

Internet of Things devices collect extremely sensitive personal information about us. This is especially true about IoT devices *in our homes.* In his majority opinion for *Florida* v. *Jardines,*[5] Justice Scalia articulated the high level of privacy an individual is entitled to in his or her home, writing "when it comes to the Fourth Amendment the home is first among equals. . .At the Fourth Amendment's 'very

---

[1] Press Release, Gartner, Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 (Dec. 12, 2013), *http://www.gartner.com/newsroom/id/2636073.*

[2] Sarah Ashley O'Brien, *The Tech Behind Smart Cities,* CNN MONEY (Nov. 11, 2014), *http://money.cnn.com/gallery/technology/2014/11/11/innovative-city-tech/index.html.*

[3] *Asymco: Smartphone penetration reaches 70 percent in the U.S.,* GSMARENA (Jul. 9, 2014), *http://www.gsmarena.com/asymco__pricing__doesnt__affect__smartphone__adoption__in__the__us-news-8982.php.*

[4] Rachel Metz, *CES 2015: The Internet of Just About Everything,* MIT TECHNOLOGY REVIEW (Jan. 6, 2015), *http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/.*

[5] *Florida* v. *Jardines,* 133 S. Ct. 1409 (2013).

core' stands 'the right of a man to retreat into his own home and there be free from unreason-able governmental intrusion'"[6]

The Supreme Court has repeatedly held that people have heightened privacy interests in what happens within their home—even over information[7] that is technologically observable[8] by others. We have "peeping tom" laws to protect against private observation in the home for the same reason—just because someone has the means to watch what you're doing in your home doesn't mean they should. Our homes are our most personal, private spaces and we maintain this expectation even if we bring smart devices into our home.

Internet of Things devices not tied to the home also have the potential to collect sensitive information. Certainly geolocation information—generated by several IoT devices—is extremely sensitive and revealing: unwanted disclosure can endanger one's personal safety by letting an attacker track your physical location. Otherwise, geolocation can reveal other deeply personal information, such as where you worship, where you protest, and where (and with whom) you sleep at night. Other IoT technologies often collect sensitive information on an individual that is not immediately apparent when that person is in a public space—such as his physical or mental health, emotions, and preferences.

In many cases, consumers will gladly share this information with IoT service providers in order to receive a particular service. However, in other cases, consumers won't want this information collected at all. Internet of Things devices must be designed with this fact in mind, or consumers will reject these products as not worth the risks.

II. There are currently insufficient security protections in place to regulate IoT data collection

It is no exaggeration to say that academics have documented the security vulnerabilities of the Internet of Things for years. Central to some of these concerns is that IoT devices use *embedded* operation systems, where computing is implanted into the device itself. The computer chips that power these systems are often cheaply produced, rarely updated or patched, and highly susceptible to hacks. Users do not have the expertise to regularly patch the system or install system updates manually, nor are they typically alerted of security updates. As prominent technologist Bruce Schneier succinctly puts it, "hundreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years. . . . We have an incipient disaster in front of us. It's just a matter of when."[9]

While some large, complex, smart IoT systems may have WiFi connections, software updates, and multiple types of functionality and interfaces, many of the more widely deployed IoT systems will be more modest, without such capabilities. These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal. Such incentives have failed certain elements of the smart phone market, resulting in millions of vulnerable devices that will remain so for the remainder of their shelf life.[10] Eventually, we expect to see entirely new types of market events, such as product recalls, based solely on vulnerabilities in the network and computational interface that provide IoT-like communication services. Otherwise, many of these devices and systems may never be updated in their after-market environment, and home networks and IoT-capable communication platforms will have to be designed to deal with errant and outright hostile (*e.g.,* hacked through a flaw or vulnerability) participants on the local network. Compounding this problem is the fact that home routers—the devices that link all these devices together—are also famously vulnerable to attack.[11]

Even at this early stage of IoT development, seemingly every type of connected device has already experienced these vulnerabilities: spy chips have been discovered

---

[6] *Id.*

[7] *Kyllo* v. *United States,* 533 U.S. 27 (2001).

[8] *Florida* v. *Jardines,* 133 S. Ct. 1409 (2013).

[9] Bruce Schneier, *Security Risks of Embedded Systems,* SCHNEIER ON SECURITY BLOG (Jan. 9, 2014), *https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.*

[10] Dan Goodin, *ACLU Asks Feds to Probe Wireless Carriers over Android Security Updates,* ARSTECHNICA, (April 17, 2013), *http://arstechnica.com/security/2013/04/wireless-carriers-deceptive-and-unfair/.*

[11] Dan Goodin, *12 million home and business routers vulnerable to critical hijacking hack,* ARSTECHNICA, (Dec. 18, 2014), *http://arstechnica.com/security/2014/12/12-million-home-and-business-routers-vulnerable-to-critical-hijacking-hack/;* Brian Krebs, *Lizard Stresser Runs on Hacked Home Routers,* KREBSONSECURITY, (Jan. 15, 2015), *http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.*

in tea kettles and irons[12]; hackers have stolen Smart TV login credentials in order to listen in and spy on people in their homes[13]; live streams from baby monitors have been uploaded to public websites[14]; thieves can disable home alarm systems with a tool from 250 yards away[15]; and even smart toilets, refrigerators and printers have been compromised.[16] And a report released this weekend by Senator Markey raises serious questions about whether connected cars are being designed to ensure that their systems are protected from malicious hackers seeking to take physical control over the vehicles.[17]

Currently, the United States does not have a dedicated data security law requiring companies to use reasonable protections to safeguard personal information. Since 2005, the Federal Trade Commission has used its general consumer protection authority under Section 5 of the FTC Act to bring enforcement actions against companies that do not safeguard personal data.[18] The Commission has argued that the FTC Act's prohibition on "unfair" business practices extends to companies using poor data security; two years ago, it brought its first enforcement action against the manufacturer of an Internet of Things device.[19] However, ongoing legal challenges threaten to undermine the agency's efforts in this area: some defendants have argued that they are not, in fact, legally obligated to use reasonable data security practices.[20]

Increased reports of massive data breaches (including the highly publicized Sony studios and Anthem healthcare hacks) have prompted new dialogue around the need for updated data breach notification laws to respond to such incidents. Unfortunately, many of the data breach notification legislative proposals would actually *dial back* legal incentives for companies to properly secure the data they collects from consumers. For example, only requiring agency or consumer notification when a specific "harm" has been identified would discourage companies from fully investigating a breach for fear of triggering the notification requirement. Further, data breach law that omits any affirmative requirement that companies design robust security procedures for their products will ultimately do little to expand upon existing state law protections and deter or prevent future breaches. In order to encourage better security than exists under the law today, a Federal breach notification bill would need to offer *new* protections not reflected in existing law, and still allow states to innovate on data sets not covered by a Federal standard.[21] For more information on this topic, visit *https://cdt.org/insight/cdt-issue-brief-on-federal-data-breach-notification-legislation/*.

---

[12] Erik Sherman, *Hacked from China: Is Your Kettle Spying on You?,* CBS (Nov. 1, 2013), *http://www.cbsnews.com/news/hacked-from-china-is-your-kettle-spying-on-you/*.

[13] Lorenzo Franceschi-Bicchierai, *Your Smart TV Could be Hacked to Spy on You,* MASHABLE (Aug. 2, 2013), *http://mashable.com/2013/08/02/samsung-smart-tv-hack/*.

[14] Loulla-Mae Eleftheriou-Smith, *Baby Monitors, CCTV Cameras and Webcams from UK Homes and Businesses Hacked and Uploaded onto Russian Website,* THE INDEPENDENT (Nov. 20, 2014), *http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitors-cctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto-russian-website-9871830.html.*

[15] Kim Zetter, *How Thieves can Hack and Disable Your Home Alarm System,* WIRED (Jul. 23, 2014), *http://www.wired.com/2014/07/hacking-home-alarms/*.

[16] Lily Hay Newman, Pretty Much Every Smart Home Device You Can Think of Has Been Hacked, SLATE BLOG (Dec. 20, 2014), *http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html.*

[17] Report, *Tracking and Hacking: Security & Privacy Gaps Put American Drivers at Risk,* OFFICE OF SENATOR ED MARKEY, (Feb. 2015) *http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.*

[18] Press Release, Federal Trade Commission, DSW Inc. Settles FTC Charges (Dec. 1, 2005), *http://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges.*

[19] Press Release, Federal Trade Commission, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.*

[20] *See* G.S. Hans, *CDT Files Brief in Wyndham Supporting FTC Regulation of Data Security* CENTER FOR DEMOCRACY & TECHNOLOGY BLOG (Nov. 13, 2014), *https://cdt.org/blog/cdt-files-brief-in-wyndham-supporting-ftc-regulation-of-data-security/; See also* Press Release, Federal Trade Commission, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), *http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.*

[21] *CDT Issue Brief on Federal Data Breach Notification Legislation,* CENTER FOR DEMOCRACY & TECHNOLOGY INSIGHTS, (Jan. 27 2015), *https://cdt.org/insight/cdt-issue-brief-on-federal-data-breach-notification-legislation/*.

III. Sensitive personal data may be collected contrary to consumer wishes and expectations

As noted above, IoT devices have the potential to collect a tremendous amount of detailed personal information about consumers. Some of the data collected is of course expected; if I buy a fitness tracker, for example, I shouldn't be surprised that the device tracks my steps throughout the day—indeed, that's the reason I bought it. On the other hand, I might be surprised if that device were also recording all my conversations with my friends, or transmitting my geolocation to third party data brokers.

As an example of surprising—and potentially unwanted—IoT data collection, last year, an independent researcher noticed that LG was monitoring what TV shows people watched on their smart TVs, and sending that information back to LG's corporate servers.[22] The purpose appeared to be for a future undeveloped advertising product; LG was also collecting and reporting back information about the names of files consumers accessed on computers connected to the same home network, though it's not clear why. In response to user complaints, LG initially directed people to a long, legalistic terms of service that vaguely reserved broad rights to transmit user data. The company backtracked after a host of media attention around its practice, and LG enabled an opt-out feature for users who did not want their information collected in this manner. This was a start, however, it is not clear that opt-out is sufficient to meet reasonable consumer expectations in this case. Should home appliances be monitoring consumers and reporting everything they can detect back to manufacturers *by default*? Certainly, other interconnected devices don't do this today. Your computer doesn't report back to Lenovo or HP everything that you do. Your phone doesn't report everything back to Motorola or Apple. When a consumer buys a TV, they are not typically looking for or expecting *a relationship* with LG or Samsung: they may appreciate additional smart capabilities like connecting to Skype or the web, but their TV is a platform for them to access others' content—it is not a destination in itself. A users' smart phone could have its microphone and camera transmitting 24 hours a day, seven days a week (setting aside battery and bandwidth issues)—it could collect significant amounts of interesting information in the name of "Big Data" but such data collection would go well beyond consumers' reasonable privacy expectations.

This precise scenario arose last week in fact, when it was revealed that Samsung's privacy policy appeared to reserve the right to collect any voice communications in proximity to its Smart TVs and send that information to an unnamed voice recognition service provider.[23] Samsung's actual practices are not easily discernable: perhaps Samsung is only collecting and transferring voice data for the limited times when a consumer is trying to use certain voice recognition commands. This might be consistent with reasonable consumer desires and expectations. Or perhaps Samsung wants to collect and process *all* dialogue in proximity to its televisions in order to refine its (or its partner's) voice recognition software. There certainly would be a benefit—to Samsung and the consumer—from that collection and processing, but query whether most consumers would find the benefit worth the persistent collection of all conversations in a living room or bedroom by an unknown third party. Ultimately, consumers must be empowered to make the determination about what data is collected and why.

We believe that the United States should enact a comprehensive privacy law regarding the collection and use of personal information. Companies should be required to offer consumers reasonable transparency and control over how their data is collected; today, the U.S. is one of the few developed nations not to have such consumer protections in place. The purpose of such a law wouldn't be to ban or prevent particular practices, but should require actionable information and an ability to express real preferences in order for a market to develop for personal information. Today, absent such requirements, too much data collection is opaque and unaccountable; consumers have a vague sense that their privacy is being violated, but don't have the information or tools available to make decisions about their personal information.

With or without a law, companies should set reasonable defaults for data collection and use based on consumer expectations. Some data may require clear opt-in because it's sensitive or the collection or use would be surprising to a user; other

---

[22] Justin Brookman, *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency,* IAPP BLOG (Nov. 27, 2013), *https://privacyassociation.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/.*

[23] Shane Harris, *Your Samsung SmartTV is Spying on You, Basically,* THE DAILY BEAST (Feb. 5, 2015), *http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.*

information may be collected automatically but consumers should have the ability to opt out of secondary data use, retention, or transfer; and some data consumers shouldn't have control over because it is fundamentally necessary for operation of the device. However, consumers must generally be empowered to make decisions about how their devices work (and what data is collected and shared with other entities). IoT should work *for* the consumer—the person who bought the product; the Internet of Things shouldn't be something that happens *to* a begrudging populace.

IV. Device connectivity and intelligence could diminish user autonomy over the devices they buy

Adding sensors and connectivity to IoT devices has the potential to make them much more useful for consumers. On the other hand, these features could also be abused to deprive consumers of continuing services, expected interoperability, or control over their own devices.

Objects included in the "Internet of Things" consist of two basic components: the physical object and the software that connects it to the network. Traditionally, when you buy something, it is yours and you are free to do with it whatever you'd like including altering, repairing, or re-selling it. However, objects within the Internet of Things do not fit into our traditional understanding of ownership. While you still take possession of the physical object, the software is typically licensed to you under an End-User License Agreement (EULA). The implications of this vary with how integral the software is to the functioning of the device—in some cases, like a washing machine that you can monitor/control from your phone, losing access to this feature wouldn't affect the core functionality and value of the machine very much. In other cases, the object itself is essentially useless without the software controlled by licensing agreements, or can quickly become obsolete without updates. For example, imagine a thermostat that only works if you can program the software. In this case, a lapse in software updates could render the physical object useless even if the physical mechanism were still in good repair.

Last year, Keurig—the popular single cup coffee maker—put software controls on its coffee maker to prevent users from using non-Keurig approved coffee pods in their machines. Though this functionality did not rely upon Internet connectivity, it did take advantage of increasingly cheap and sophisticated sensors to allow the Keurig machine to detect proprietary codes on approved coffee pods. As result of this technology, consumers were prevented from brewing their preferred brand of coffee in the devices they bought and paid for. In this case, Keurig's decision appears to have backfired: featured reviews for Keurig's new line of coffee makers on Amazon prominently criticize this design feature,[24] and sales fell 12 percent last quarter.[25]

In other cases, policymakers have intervened to mitigate potential monopolistic effects of proprietary software. One example is the repair codes used by automobile manufacturers. Cars include systems that provide a specific diagnostic code that explains, for example, the cause of a "check engine" light. Originally, the guide that explains these codes was withheld from consumers and the majority of auto repair shops, forcing drivers to use specific repair shops for their vehicles. However, some states now require that the explanations for the codes be widely available.[26] In another example, the Librarian of Congress, in consultation with the Copyright Office, eliminated an exemption to laws prohibiting circumvention of digital rights management for users seeking to *unlock* their mobile phones and change wireless providers. Mobile phone unlocking had been an entirely legal and common practice for years before the Librarian eliminated the exemption. More than 114,000 Americans petitioned the White House to overturn the ban and, after both the Federal Communications Commission and the White House recommended doing so, Congress ultimately enacted legislation restoring consumers' right to unlock their own phones. Unfortunately, the exemption applies only to mobile phones and is examined *de novo* every three years.

In the Internet of Things, digital rights management affects intellectual property accessed through networked devices as much as the devices themselves. For example, users do not own the content they purchase for their e-readers (Kindle, Nook, etc.). The physical tool allows readers to buy rights to access the content of their choice, but readers do not own the book. Additionally, this access is restricted in

---

[24] *Keurig 2.0 K350 Brewing System—Black,* AMAZON.COM, *http://www.amazon.com/Keurig-2-0-K350-Brewing-System/dp/B00KYWL34Q/ref=sr_1_1?ie=UTF8&qid=1423266957&sr=8-1&keywords=keurig+2.0* (last visited Feb. 9, 2015).

[25] Josh Dzeiza, *Keurig's attempt to "DRM" its coffee cups totally backfired,* THE VERGE (Feb. 5, 2015), *http://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totally-backfired.*

[26] *Mass. lawmakers approve "Right to Repair" bill,* FOXNEWS, (August 1, 2012), *http://www.foxnews.com/leisure/2012/08/01/mass-lawmakers-approve-right-to-repair-bill/.*

many users may not fully understand because the relationship is so different from the physical world. For example, there are typically restrictions on *lending* the book to a friend. In this case, if the licensing agreements for that content were revoked because of a perceived or alleged violation of the license, the object itself would be useless to the average consumer who would have no way to load content.

Additionally, connectivity can allow other entities to access and control the device in ways not possible in an un-networked world. One prominent example is lenders who use technology in connected cars to punish those who are late in making payments by disabling the vehicle. In a case reported by the *New York Times*,[27] subprime borrowers were allowed to lease vehicles provided they gave permission for the lender to remotely disable the ignition in the event of a late payment or default. Some argue this technology allows the lender to provide credit to a broader audience than would otherwise be possible; others argue that it is unethical and perilous to put people in a situation where they may have an emergency and cannot access their vehicle, as was the case for the woman in the article who needed to use her car to take an asthmatic child to the doctor. Moreover, vulnerable borrowers might be subject to egregious reconnection fees that had been disclosed only in inscrutable contracts. Regardless of what you believe, it is undeniable that this technology shifts the balance of power from the user to the company or institution that controls the software.

V. Our government access and intelligence laws must be reformed

Finally, the default of IoT devices to phone home by reporting data to a company rather than storing it locally on the device raise concerns about government surveillance as well. Many of the same concerns that apply to in-the-home monitoring devices like smart grid technologies[28] apply to objects in the Internet of Things. IoT systems will, in most cases, be sensing platforms augmenting devices and objects in the home or in businesses. Light sensors can tell how often certain rooms are occupied at night or how often the refrigerator is opened. Temperature sensors may be able to tell when one bathes, exercises, or leaves the home entirely. Microphones can easily pick up the content of conversations in the home and, with enough fidelity, can identify who is speaking. In essence, the privacy and security concerns highlighted by the revelation that law enforcement has access to data stored by private companies are elevated exponentially in a future with increased connectivity and automated collection.

Government access without robust due process protection is already arguably the most significant threat posed by the collection of personal information. As the recent NSA revelations aptly demonstrate, much of the data that governments collect about us derives not from direct observation, but from access to commercial stores of data. Even in the United States and Europe, that data is often obtained without transparent process, and without a particularized showing of suspicion—let alone probable cause as determined by an independent judge. Unfortunately, there is almost nothing that consumers can do to guard against such access or in many cases even know when it occurs.

The revelation that commercial data is tied to government surveillance has the potential to fundamentally change the conversation about IoT. For the vast majority of consumers, unwanted surveillance—quite apart from practical effects of such surveillance—is the harm they're seeking to avoid. Therefore, considerations of risks associated with IoT must address harms from government surveillance as well as private sector risks.

This loss of consumer confidence has a quantifiable impact on corporate bottom lines and hence the development of these useful new technologies. For example, according to Forrester Research the losses to U.S. technology companies from revelation of the PRISM program (detailing once facet of U.S. surveillance practices) could result in, "a net loss for the service provider space of about $180 billion by 2016 which would be roughly a 25 percent decline in the overall IT services market by

[27] Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car,* THE NEW YORK TIMES (Sept. 24, 2014), *http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/*.

[28] CTR. FOR DEMOCRACY & TECH. & ELEC. FRONTIER FOUND., "Proposed Smart Grid Privacy Policies and Procedures," before The Public Utilities Commission of the State of California (December 18, 2008), available at *https://cdt.org/files/pdfs/CDT__EFF__PoliciesandProcedures__15Oct2010__OpeningComment__1.pdf.*

that final year." These costs demonstrate the market value of business practices and government policies that respect privacy.[29]

Nor is the point in sighting this figure to single out the NSA and U.S. surveillance. As CDT has noted repeatedly, all governments are interested in data collection and have extensive legal tools to access that information. In an Internet connected future it is not only the U.S. government but also the governments around the world that may be interested in IoT and the information it reveals. For more on legal tools that governments possess to access personal information please see: *http://govaccess.cdt.info/*.

Government surveillance reform is a much broader topic than the IoT and this committee's hearing today. However, the continuing access by government to commercial information highlights the need to build systems that minimize the amount of information they share and also give consumers control over what information their devices collect.

The potential benefits of the IoT are exciting and profound. It is incumbent upon manufactures of these devices and governments to make sure that those benefits are fully realized while protecting the privacy of consumers.

Conclusion

Recognition of the threats to collected personal information is particularly important because in recent years, some have argued for a new definition of privacy where there are no limits on what information companies (and governments) can collect about us or how long they retain it. Privacy is in effect redefined to only prohibit certain harmful uses of personal information. For example, President Obama's Council of Advisors on Science and Technology last year released a report on Big Data making precisely this point: because of the potentially awesome power of personal information, we shouldn't put limitations on what information is collected; instead, we should just make sure that that data is not subsequently misused.[30]

This view, however, presumes a perfect world of unbreakable security, where consumer and company expectations are fully aligned, and where due process protections fully assure there is no potential for government abuse.[31] Obviously, these conditions are not met today, and likely will never fully be realized. As such, consumers have a rational interest in exercising control over how their data is collected and retained. Without affording consumers meaningful control over their own devices, IoT adoption is seriously threatened. Today, the highly sensitive data collected by IoT devices is exposed to a variety of threats, and designers must keep these threats in mind when developing their products for market. Consumers would benefit tremendously from a full-fledged, user-centric Internet of Things. Developers must keep personal privacy and empowerment in the front of their minds in creating these products.

The CHAIRMAN. Thank you, Mr. Brookman.

We will go 5-minute rounds. I may have to duck out of here for a little while to do a Finance Committee markup, but I hope to give everybody a chance to ask questions, and we will see where it goes.

I will start by asking you, Mr. Donny. You mentioned in your testimony the challenge of taking advantage of the Internet of Things on farms due to the lack of reliable broadband access and cellular coverage. I would like you to elaborate on the recommendation you made that we accelerate the availability of low-cost, long-range communication technology to ensure that we can move data from the field to the cloud on every farm. Would you please talk a little bit about that and then maybe elaborate on what you see as some of the policy impediments to that.

---

[29] James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," FORRESTER, August 14, 2013, *http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects*

[30] EXECUTIVE OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014). *http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf?utm_content=buffer06b57&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.*

[31] JUSTIN BROOKMAN & G.S. HANS, WHY COLLECTION MATTERS: SURVEILLANCE AS A DE FACTO PRIVACY HARM (2013), *http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.*

Mr. DONNY. Thank you, Senator Thune, for the question.

So let me actually elaborate on the challenge as well. The challenge in agriculture specifically for connecting devices is that the farm—both the topography of the farm, the rolling hills, as well as the trees and plants and corn stalks themselves are a lousy place for our cellular and RF signals. The plants and so forth consume a lot of that energy that comes out of those devices. So it makes it difficult to move data from a device in the field, unless you have a really tall antenna, out to a collector device. And so the traditional technology today that has been used is satellite 2.4 gigahertz, 900 megahertz RF signals, and cellular. And the challenge is, if you are in a rural area, you oftentimes do not have good cellular coverage. We have all experienced that.

And so the opportunity that we see that in particular I am interested in is the white space in which we have unused now white space channels that were used by televisions that provide the opportunity to move data around the farm very long distances at almost no cost. So I know the FTC is looking into that and reviewing that.

There are companies globally that are developing hardware in which to take advantage of that white space. So in the case of those channels, we can now move data from a sensor in the field that is no bigger than the size of your cell phone several miles, 5, 6, 7 miles in our experience—we have tested some of these earlier models—out to a device. And so for a farmer, instead of having to spend $7 or $8 or $10 a month on a cellular data communication charge per device, we can move data for free from the device to the backhaul system to get data at a central data point.

So if you are looking at farm adoption and how do we enable communication methods to improve what farmers are doing, density of data is extremely important in that analysis. So the lower we can reduce the cost of the device in the field vis-à-vis the communication channel, vis-à-vis the device, the more data we will have, the more enabled that farmer will be to make a better decision. So specifically we are interested in how do we use what we know today, the white space and other RF signals, to enable the industry to go out and innovate, go figure out how we are going to move data around 5, 6, 7 miles at no cost and enable those companies to go out and do that today.

The CHAIRMAN. Mr. Thierer or Mr. Brookman, do you have any ideas, any thoughts on how to ensure that we have sufficient wireless capacity to power the Internet of Things?

Mr. THIERER. Well, I will make a brief comment on that. It is not the primary focus of my own research, but generally speaking, we need to get a better process in place at the Federal Communications Commission. Freeing up a lot more spectrum is something I think everybody on this committee and many policy circles agrees on. It is a question of where do we get it. Creating more and better incentives to do that is going to be essential because these devices are going to be eating up a lot of it in a short time.

Mr. BROOKMAN. And I am not remotely a spectrum expert. So I am not going to weigh in on that.

The CHAIRMAN. How about on the issue of interoperability? We have all these devices, Do we have to have standards for these de-

vices, and if there are standards, who creates them? Does anybody want to take a stab at that?

Mr. THIERER. I will just make a brief comment that we all have devices we are carrying with us here today that have numerous standards in them and have a lot of complex interoperability problems. But somehow we figured it out for this. I think we can figure it out for the Internet of Things space as well.

The CHAIRMAN. Anybody else?

Mr. DONNY. The industry and agriculture are actually trying to tackle this interoperability challenge, and it is a mixed bag. So you can try to focus on a standard, but the problem with standards are there are 16 other standards you are trying to displace to begin with and another standard necessarily does not fix that.

Modern data in general—you tend to publish how that data looks and is used, and then companies that need that data then build systems around consuming that. So lots of other devices have solved that problem without creating huge standards in the space.

Mr. ABBOTT. I think along those lines that if we go back in time to just networking that the same challenges around interoperability existed then, and over time we saw certain winners emerge. And I think at that point in time, it would make sense to have some national or even actually ideally global kind of standard around that particular protocol. So in the case of the Internet, a standard Internet protocol emerged, and I think we would anticipate something along those lines.

One interesting thing to note is that as we are in this early phase of IoT, which challenges interoperability, that as we become more homogenous from that heterogeneous world, it is likely that the security issues will actually increase because actually by having more heterogeneity is actually decreasing the security exposure today.

The CHAIRMAN. Thank you all.

Senator Nelson?

Senator NELSON. The allocation of additional spectrum, Mr. Chairman, is a subject that we need to get into. It has been raised here, and it is a very important one.

Before you and I have to go off and vote in the Finance Committee, I want to get back to this question of security, Samsung, and the Smart TV. According to its privacy policy, the television records your conversations when you activate the microphone and sends those recordings to a third party. Do you want to tell me yes or no? Should consumers be given adequate notice of such a practice? Let us start. Just go down. Yes or no.

Mr. ABBOTT. I think that actually consumers should have the ability to opt out, and it should be very clearly communicated what data is being collected by that particular device or that service.

Senator NELSON. We are going to run out of time. So opt out is your answer instead of opt in.

Mr. ABBOTT. Correct.

Senator NELSON. How about it, Mr. Davis?

Mr. DAVIS. Well, I certainly think we need to be able to balance privacy and innovation. As the developers of these products, we need to be stewards of that privacy.

Senator NELSON. Yes or no. Opt out or opt in?

Mr. DAVIS. I think consumers ought to be able to opt in.

Senator NELSON. Opt in?

Mr. DAVIS. Yes.

Senator NELSON. OK.

Mr. Donny?

Mr. DONNY. Thank you, Senator.

I think they need to affirmatively agree to that policy.

Senator NELSON. So you are saying opt in.

Mr. DONNY. Correct.

Mr. THIERER. They can opt out and they do not have to buy the TV in the first place.

Senator NELSON. So when they buy the TV, and there is the privacy policy, should they opt out or opt in?

Mr. THIERER. They should opt out.

Senator NELSON. Opt out.

Mr. THIERER. Yes.

Mr. BROOKMAN. If you are using voice recognition, it is kind of clear what is going on ephemerally. If it is collecting data all the time, there is an obligation to go out of their way to explain that to folks.

Senator NELSON. What does that mean? Opt out or opt in?

[Laughter.]

Mr. BROOKMAN. I will say opt in then.

Senator NELSON. Opt in.

OK. Three opt ins and two opt outs.

Is there a role for the Congress to play here? How do we make companies accountable, or is this something the FTC should do?

Mr. THIERER. Well, Senator, as I already stressed, the FTC is already very active on this front, and has already pursued security cases against many major Internet giants. There is something like over 50 data security consent decrees that have been out there. Major fines have been levied. Twenty-year privacy audits have been imposed. So there is a very aggressive enforcement regime already in place using the unfair and deceptive practices at the FTC. And I think that will and should continue.

Mr. BROOKMAN. Yes. I think that existing law arguably already requires reasonable security. I think it would be useful to have a statute saying that.

On privacy, I would like to see flexible requirements. Requiring some level of transparency is better today. A lot of these practices today are very opaque. So I think just giving companies an obligation to actually say what they are doing I think would create a better market for these products.

Senator NELSON. Take my refrigerator example, which is not an extreme example. A smart refrigerator tells me I need milk. What about the refrigerator telling the local grocery store that I need milk? Should that be done opt out or opt in?

Mr. ABBOTT. That is absolutely enabling the consumer to go select that service provider to share that data.

And just to expand, Senator, on my prior answer, opt out works when there is a very clear communication to the consumer, what data is being collected, why it is, and if you want to actually not have that data collected, how that consumer can actually select that.

Senator NELSON. You know why I asked that question? Because we have got a real-life example. Verizon had implanted these super cookies, codes, and then that data was transmitted to third parties selling that information in order for the consumer on that Verizon smart phone to start getting all kinds of information that was recorded because of that super cookie.

Now, AT&T tried it and pulled back because of the privacy implications, but Verizon today is still studying what they have done even though we have called this out.

And if you have been the recipient of unwanted advertisements because you happen to go to a certain place or buy from a certain store, you can start to see how the privacy is beginning to be invaded.

Thank you, Mr. Chairman.

The CHAIRMAN. And I used to like super cookies.

[Laughter.]

The CHAIRMAN. Senator Ayotte?

STATEMENT OF HON. KELLY AYOTTE,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator AYOTTE. I am just thinking about the milk the refrigerator could tell me to have with my super cookie.

[Laughter.]

Senator AYOTTE. I wanted to follow up on a couple of different things. You know, as we look at something that has been a consistent challenge for us—and that is data breaches. As we see more homogeneity in the consolidation of data, I think this becomes a bigger issue. This is something that we have had numerous discussions on legislating on.

I will give you an example. Recently the big Anthem breach. 22 percent of my state got hit by that. 80 million people in the country got hit.

So I wanted to hear—I think it is probably best to direct it to Mr. Davis and Mr. Thierer—about what your thoughts are and what we should be doing on data breach legislation. I certainly want to make sure we do not do things that hurt innovation and thwart new technologies, but this seems to be a repetitive issue that we need to address. Your thoughts.

Mr. DAVIS. Thank you for the question.

You know, certainly from an Intel perspective, we think you have to design security into these implementations from the beginning not only on the endpoint device but throughout that end-to-end implementation. There are multiple levels of security in terms of how the device powers up and behaves when it is first powered, the kinds of applications it is allowed to run when it begins to run applications, and the ability to limit the types of things that can be launched on that particular device at any point in time, and then be able to manage that data through the network such that the information they are receiving from that data is trusted information. You are getting what you would expect to be getting out of that device.

At the same time, I think we have to be a bit careful in terms of how we create legislation or policy around that in terms of enabling the industry to innovate as well. So I think certainly as we

talk to customers, as we talk to others in the industry, security is the number one concern, and we believe we can build that into the technologies that these products are being developed around.

Mr. THIERER. Well, Senator, many states already pursue data breach notification requirements, and there is a case to be made for it. But I would just remind the Committee that you already have many other legal enforcement mechanisms to deal with these things. The Federal Trade Commission has gone after many companies who have had breaches like this. You have State attorneys general who have been very active on this front.

Senator AYOTTE. So I was a State AG, and I pursued some of these cases. Now, sitting with this hat on in the U.S. Senate, what are your thoughts on a national standard in terms of notification?

Mr. THIERER. Eventually I think we are probably going to get there. I think there is probably a case to be made for some uniformity in this case because many states pursuing it or others do not have any at all.

Senator AYOTTE. I appreciate it.

I also wanted to follow up with you. You talked about the ability under the FTC to determine unfair and deceptive practices in this realm. So the FTC is pursuing those cases.

But if you look at it from the perspective of innovation and having a larger plan in terms of the Internet of Things, isn't one of the challenges we face that people do not really fully understand? There has not been a full definition under section 5 of what is an unfair and deceptive practice, and so therefore, that lack of certainty to businesses can create some ambiguity about what is acceptable and what is not. So I wanted to get everyone's thoughts on that.

Mr. THIERER. I think that is a fair point, Senator, but I would also say that this is an issue we have had for many decades. Unfair and deceptive practices go back over a century, and so we are going to continue to see the evolution of that standard. But you are right. We have to be careful that it is not overzealously enforced.

Senator AYOTTE. Do you think that the FTC needs to provide further guidance on what they believe is unfair and deceptive under section 5?

Mr. THIERER. I think that is evolving out of the body of decisions that they have been handing down on data security and privacy.

Senator AYOTTE. Mr. Davis, I was very curious. In your testimony, you talked about what other countries are doing to really look at making sure the infrastructure is there, national Internet of Things plans. So what is it you would like to see us do here in a way that would be a productive role for Congress and not one that thwarts innovation?

Mr. DAVIS. Well, certainly one of the recommendations that we are making is that we support public-private partnerships so that we go out and identify areas in, say, transportation, in manufacturing, and some of these industrial areas where we can innovate. We can spur these industries to go implement new technologies and drive the productivity services and new product benefits. So certainly public-private partnerships are a key area that we are recommending.

Senator AYOTTE. And, Mr. Abbott, from the financing end, what are your thoughts? You are the ones allowing for investment. You are looking at new companies. What is your thought on that?

Mr. ABBOTT. Well, I think there needs to be more coordination, I think, through the public and the private sector especially on these issues. We are, obviously, very, very focused on looking at how we can help these early stage companies, much smaller than Intel, not be stifled and so they can actually kind of grow and expand.

Senator AYOTTE. Thank you all.

The CHAIRMAN. Thank you, Senator Ayotte.

Senator Peters?

STATEMENT OF HON. GARY PETERS, U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman.

And, panelists, thank you for your testimony here today.

As the Senator from Michigan, you can imagine the auto industry is very important to me. And the auto industry is certainly much more than just horsepower and torque, although those are the two things that I like best about the auto industry. But it is, as you know, very complex, sophisticated, and very tech heavy with some of the best minds working to develop some new safety technologies, as well as environmental technologies using the Internet of Things. Advanced technology in vehicles today have fewer crashes. They have significantly reduced injuries and fatalities, lowered emission levels, and have increased fuel economy dramatically.

In recent years, automakers have delivered advanced safety features such as lane departure warning devices, adaptive cruise control, and crash-imminent braking, features that were made possible through the use of sensors, actuators, artificial intelligence systems, and increasingly wireless connectivity that will enable these vehicles to basically have their own situational awareness and the ability to perceive and react to the environment to avoid harm.

So what comes next I think is very significant. It will save lives as the Government and industry will deploy the vehicle-to-vehicle communications system and infrastructure communication networks. The National Highway Traffic Safety Administration estimates that V2V technology has the potential to mitigate or eliminate 80 percent of the accidents that are involved in non-impaired drivers. That is significant. 80 percent of accidents could be avoided.

But in order to implement this V2V technology and in a sense then save lives, the 5 gigahertz band of spectrum will need to be preserved for its use. And I know that some of my colleagues on this committee have actually expressed an interest in opening up this band of spectrum for WiFi use, but I would caution that this should only be done after full interference testing has been completed and it is ensured that intelligent transportation technologies operating on this band, which have the potential to save lives, as I mentioned, are fully protected.

I think it is also important that the benefits made possible by advanced technologies are delivered to consumers in a transparent way that respects consumer privacy. As auto companies continue to

develop these technologies, automakers must address data privacy and cybersecurity issues head on. And that is why, in November of last year, the auto industry agreed to set a set of privacy principles and practices that is currently working to establish an auto ISAC, information sharing and analysis center, to enable these companies to share information in real time about cyber threats. And I certainly look forward to seeing the auto industry's continued leadership in this area.

And I know the Chairman has gone, but on behalf of the Committee, I would like to ask for unanimous consent to enter into the record the consumer privacy protection principles put together by the industry.

Senator MORAN [presiding]. Without objection.

[The information referred to follows:]

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.

ASSOCIATION OF GLOBAL AUTOMAKERS, INC.

Consumer Privacy Protection Principles

Privacy Principles for Vehicle Technologies and Services—November 12, 2014

I. Introduction

The automotive industry is developing innovative technologies and services that promise to deliver substantial benefits and enhance the driving experience. These technologies and services may assist in enhancing safety, reducing the environmental impacts of vehicles, diagnosing vehicle malfunctions, calling for emergency assistance, detecting and preventing vehicle theft, reducing traffic congestion, improving vehicle efficiency and performance, delivering navigation services, providing valuable information services, and more. The Alliance of Automobile Manufacturers, the Association of Global Automakers, and their members are excited about the benefits offered by today's vehicle technologies and services and look forward to expanding the array of innovative technologies and services offered to consumers.

Many of these technologies and services are based upon information obtained from a variety of vehicle systems and involve the collection of information about a vehicle's location or a driver's use of a vehicle. Consumer trust is essential to the success of vehicle technologies and services. The Alliance, Global Automakers, and their members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy.

Privacy is important to consumers, and it is important to us. That is why the Alliance and Global Automakers have issued these Privacy Principles ("Principles"). The Principles provide an approach to customer privacy that members can choose to adopt when offering innovative vehicle technologies and services. Each member has made an independent decision about whether to adopt the Principles, and other companies may choose to adopt them as well. We provide a list of those companies that have adopted the Principles in the Appendix, and they are referred to as "Participating Members."

The Principles apply to the collection, use, and sharing of *Covered Information* in association with *Vehicle Technologies and Services* available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

The Principles are subject to change over time. When they do change, the Alliance and Global Automakers will post the updated Principles at *www.automotiveprivacy.com* and _____. The Principles are not intended to replace inconsistent or conflicting applicable laws and regulations, where they exist. So, the Principles should be interpreted as subject to and superseded by applicable laws and regulations.

Participating Members may implement the Principles in different ways, reflecting differences in technologies and other factors. And Participating Members may choose to incorporate into their privacy programs elements that are not addressed in the Principles and are free to take additional privacy steps. But regardless of how Participating Members design their privacy programs and implement the Principles, Participating Members affirm the following fundamentals, as detailed in the relevant sections that follow:

- **Transparency:** Participating Members commit to providing *Owners* and *Registered Users* with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of *Covered Information.*
- **Choice:** Participating Members commit to offering *Owners* and *Registered Users* with certain choices regarding the collection, use, and sharing of *Covered Information.*
- **Respect for Context:** Participating Members commit to using and sharing *Covered Information* in ways that are consistent with the context in which the *Covered Information* was collected, taking account of the likely impact on *Owners* and *Registered Users.*
- **Data Minimization, De-Identification & Retention:** Participating Members commit to collecting *Covered Information* only as needed for legitimate business purposes. Participating Members commit to retaining *Covered Information* no longer than they determine necessary for legitimate business purposes.
- **Data Security:** Participating Members commit to implementing reasonable measures to protect *Covered Information* against loss and unauthorized access or use.
- **Integrity & Access:** Participating Members commit to implementing reasonable measures to maintain the accuracy of *Covered Information* and commit to giving *Owners* and *Registered Users* reasonable means to review and correct *Personal Subscription Information.*
- **Accountability:** Participating Members commit to taking reasonable steps to ensure that they and other entities that receive *Covered Information* adhere to the Principles.

The application of these fundamental principles is described in more detail in the sections that follow.

II. Applicability

The Principles apply to the collection, use, and sharing of *Covered Information* in association with *Vehicle Technologies and Services* available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

Participating Members are listed in the Appendix.

Each Participating Member commits to complying with the Principles for new vehicles manufactured no later than Model Year 2017 (which may begin as early as January 2, 2016) and for *Vehicle Technologies and Services* subscriptions that are initiated or renewed on or after January 2, 2016. To the extent practicable, each Participating Member commits to implementing the Principles for *Covered Information* collected from vehicles manufactured before January 2, 2016. If compliance with the Principles involves a vehicle engineering change, each Participating Member commits to complying with the Principles as soon as practicable, but by no later than vehicle Model Year 2018.

Some Participating Members may work with *Third-party Service Providers* to provide some or all of their *Vehicle Technologies and Services.* When doing so, Participating Members commit to taking reasonable steps to ensure that *Third-party Service Providers* adhere to the Principles in providing *Vehicle Technologies and Services* that involve the collection, use, or sharing of *Covered Information.* Businesses other than *Third-party Service Providers* may provide *Owners* and *Registered Users* with apps or other offerings that involve the collection of information from vehicles. Participating Members will encourage those businesses to respect the privacy of *Owners* and *Registered Users* and will take reasonable steps to provide those businesses with an opportunity to provide *Owners* and *Registered Users* with information about the businesses' privacy practices.

However, the Principles directly apply only to Participating Members. The Principles do not apply directly to vehicle dealerships that are not owned by Participating Members.

III. Scope of the Principles and Definitions

The Principles provide a framework for Participating Members to embrace when collecting, using, and sharing *Covered Information.* The following defined terms are used in the Principles. Together, the definitions describe the scope of the Principles.

Affirmative Consent: An *Owner's* or *Registered User's* clear action performed in response to a clear, meaningful, and prominent notice disclosing the collection, use, and sharing of *Covered Information.*

Biometrics: Covered Information about an *Owner's* or *Registered User's* physical or biological characteristics that serves to identify the person.

Covered Information: (1) *Identifiable Information* that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with *Vehicle Technologies and Services;* or (2) *Personal Subscription Information* provided by individuals subscribing or registering for *Vehicle Technologies and Services.*

> ***Exclusion from Covered Information:*** If Participating Members collect *Covered Information* and then alter or combine the information so that the information can no longer reasonably be linked to the vehicle from which the information was retrieved, the *Owner* of that vehicle, or any other individual, the information is no longer *Covered Information.* If Participating Members attempt to link the information to specific, identified individuals or vehicles or share the information without prohibiting the recipients from attempting such linking, the information becomes *Covered Information.*

Driver Behavior Information: *Covered Information* about how a person drives a vehicle. Examples are vehicle speed, seat belt use, and information about braking habits. This does not include information that is used only for safety, diagnostics, warranty, maintenance, or compliance purposes.

Geolocation Information: *Covered Information* about the precise geographic location of a vehicle.

Identifiable Information: Information that is linked or reasonably linkable to (i) the vehicle from which the information was retrieved, (ii) the *Owner* of that vehicle, or (iii) the *Registered User* using *Vehicle Technologies and Services* associated with the vehicle from which the information was retrieved.

Owners: Those individuals who have legal title to a vehicle that receives or is equipped with *Vehicle Technologies and Services* that use *Covered Information;* those entitled to possession of such a vehicle, like purchasers under an agreement (for example, a vehicle loan where the vehicle is collateral); and those entitled to possession of such a vehicle as lessees pursuant to a written lease agreement that, at its inception, is for a period of more than three months. The term "Owners" does not include lienholders and lenders.

Personal Subscription Information: Information that individuals provide during the subscription or registration process that on its own or in combination with other information can identify a person, such as a name, address, credit card number, telephone number, or e-mail address.

Registered User: An individual other than an *Owner* who registers with, and provides *Personal Subscription Information* to, a Participating Member in order to receive *Vehicle Technologies and Services* that use *Covered Information.*

Third-party Service Providers: Companies unaffiliated with Participating Members that receive *Covered Information* when conducting business on behalf of a Participating Member.

Vehicle Technologies and Services: Technologies and services provided by, made available through, or offered on behalf of Participating Members that involve the collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle.

IV. Specific Principles

1. Transparency

Participating Members commit to providing ***Owners*** *and* ***Registered Users*** *with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of* ***Covered Information.***

Participating Members commit to providing notices in a manner that enables *Owners* and *Registered Users* to make informed decisions.

How Participating Members may provide notices: Participating Members may make notices available in a variety of ways. Depending on the nature of the *Vehicle Technologies and Services* and the circumstances in which they are offered, different mechanisms may be reasonable to provide *Owners* and *Registered Users* with ready access to clear, meaningful notices about the *Covered Information* that Participating Members collect, use, and share.

There is no one-size-fits-all approach. Among the various ways Participating Members may choose to provide notices are in owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays. At a minimum, Participating Members commit to making information regarding the collection, use, and sharing of *Covered Information* publicly available via online web portals.

When Participating Members may provide notices: Participating Members commit to taking reasonable steps to provide *Owners* and *Registered Users* with

ready access to clear, meaningful notices prior to initial collections of *Covered Information.* Notices need not be provided prior to every instance of collection where addressed by prior notices.

Content of notices: Participating Members commit to designing the notices so that they provide *Owners* and *Registered Users* with clear, meaningful information about the following:

- the types of *Covered Information* that will be collected;
- the purposes for which that *Covered Information* is collected;
- the types of entities with which the *Covered Information* may be shared;
- the deletion or de-identification of *Covered Information;*
- the choices *Owners* and *Registered Users* may have regarding *Covered Information;*
- whether and how *Owners* and *Registered Users* may access any *Covered Information;* and
- where *Owners* and *Registered Users* may direct questions about the collection, use, and sharing of *Covered Information.*

Notices regarding the collection of *Geolocation Information, Biometrics,* and *Driver Behavior Information:* When Participating Members collect, use, or share *Geolocation Information, Biometrics,* or *Driver Behavior Information,* Participating Members commit to providing clear, meaningful, and prominent notices about the collection of such information, the purposes for which it is collected, and the types of entities with which the information may be shared. Please see the Choice section below for information about the Principles' *Affirmative Consent* conditions if Participating Members use *Geolocation Information, Biometrics,* or *Driver Behavior Information* as a basis for marketing or share such information with unaffiliated third parties for their own purposes.

Changing notices: Participating Members commit to taking reasonable steps to alert *Owners* and *Registered Users* prior to changing the collection, use, or sharing practices associated with *Covered Information* in ways that have a material impact on *Owners* or *Registered Users.* If the new practices involve using *Covered Information* in a materially different manner than claimed when the *Covered Information* was collected, Participating Members commit to obtaining *Affirmative Consent* from *Owners* and *Registered Users* to the new practices.

2. Choice

Participating Members commit to offering ***Owners*** and ***Registered Users*** *with certain choices regarding the collection, use, and sharing of* ***Covered Information.***

Certain safety, operations, compliance, and warranty information may be collected by necessity without choice.

When Participating Members provide notices consistent with the Transparency principle, an *Owner's* or *Registered User's* acceptance and use of *Vehicle Technologies and Services* constitutes consent to the associated information practices, subject to the *Affirmative Consent* provisions below.

Participating Members understand that the sharing and use of *Geolocation Information, Biometrics,* and *Driver Behavior Information* can raise concerns in some situations, therefore Participating Members also commit to obtaining *Affirmative Consent* expeditiously for the following practices:

- using *Geolocation Information, Biometrics,* or *Driver Behavior Information* as a basis for marketing; and
- sharing *Geolocation Information, Biometrics,* or *Driver Behavior Information* with unaffiliated third parties for their own purposes, including marketing.

Affirmative Consent is not required, however, when *Geolocation Information, Biometrics,* or *Driver Behavior Information* is used or shared

- as reasonably necessary to protect the safety, property, or rights of Participating Members, *Owners, Registered Users,* drivers, passengers, or others (this includes sharing information with emergency service providers);
- only for safety, operations, compliance, or warranty purposes;
- for internal research or product development;
- as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which, in the case of requests or

demands from governmental entities for *Geolocation Information,* must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and

- to assist in the location or recovery of a vehicle reasonably identified as stolen.

Participating Members also need not obtain *Affirmative Consent* when sharing *Geolocation Information, Biometrics,* or *Driver Behavior Information* with *Third-party Service Providers* that assist in providing *Vehicle Technologies and Services* if those parties are not permitted to use that information for their independent use and the sharing is consistent with the notices that Participating Members have provided.

Participating Members may obtain *Affirmative Consent* at the time of vehicle purchase or lease, when registering for a service, or at another time.

3. Respect for Context

Participating Members commit to using and sharing ***Covered Information*** *in ways that are consistent with the context in which the* ***Covered Information*** *was collected, taking account of the likely impact on* ***Owners*** *and* ***Registered Users.***

The context of collection: Various factors will determine the context of collection, including the notices offered to *Owners* and *Registered Users,* the permissions that they have provided, their reasonable expectations, and how the use or sharing will likely impact them.

- When Participating Members present clear, meaningful notices about how *Covered Information* will be used and shared, that use and sharing is consistent with the context of collection.
- Participating Members commit to making reasonable and responsible use of *Covered Information* and may share that information as reasonable for those uses. Reasonable and responsible practices may vary over time as business practices and consumer expectations evolve.

The following examples illustrate some of the reasonable and responsible ways in which Participating Members may use or share *Covered Information* consistent with the context of collecting that information, taking into account the likely impact on *Owners* and *Registered Users* The list is not meant to be exhaustive.

- Using or sharing *Covered Information* as reasonably necessary to provide requested or subscribed services;
- Using or sharing *Covered Information* to respond to a possible emergency or other situation requiring urgent attention;
- Using or sharing *Covered Information* to conduct research or analysis for vehicles or *Vehicle Technologies and Services;*
- Using or sharing *Covered Information* to diagnose or troubleshoot vehicle systems;
- Using or sharing *Covered Information* as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- Sharing *Covered Information* for operational purposes with affiliated companies that are clearly associated with the Participating Member or with the *Vehicle Technologies and Services* from which the *Covered Information* was collected or derived;
- Using or sharing *Covered Information* to prevent fraud and criminal activity, or to safeguard *Covered Information* associated with *Owners* or their vehicles;
- Using or sharing *Covered Information* to improve products and services or develop new offerings associated with *Vehicle Technologies and Services,* vehicles, vehicle safety, security, or transportation infrastructure;
- Using *Covered Information* to provide *Owners* or *Registered Users* with information about goods and services that may be of interest to them;
- Sharing *Covered Information* as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which in the case of requests or demands from governmental entities for *Geolocation Information,* must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and
- Using or sharing *Covered Information* to protect the safety, property, or rights of *Owners,* Participating Members, or others.

4. Data Minimization, De-Identification & Retention

Participating Members commit to collecting ***Covered Information*** *only as needed for legitimate business purposes. Participating Members commit to retaining* ***Covered Information*** *no longer than they determine necessary for legitimate business purposes.*

5. Data Security

Participating Members commit to implementing reasonable measures to protect ***Covered Information*** *against loss and unauthorized access or use.*

Reasonable measures to protect *Covered Information:* Reasonable measures include standard industry practices. Those practices evolve over time and in reaction to evolving threats and identified vulnerabilities.

6. Integrity & Access

Participating Members commit to implementing reasonable measures to maintain the accuracy of ***Covered Information*** *and commit to offering* ***Owners*** *and* ***Registered Users*** *reasonable means to review and correct* ***Personal Subscription Information.***

Participating Members may provide the means to review and correct *Personal Subscription Information* in a variety of ways, including but not limited to web portals, mobile applications, or in-vehicle tools.

Participating Members commit to exploring additional means of providing *Owners* and *Registered Users* with reasonable access to *Covered Information,* taking into account potential security and privacy issues.

7. Accountability:

- *Participating Members commit to taking reasonable steps to ensure that they and other entities that receive* ***Covered Information*** *adhere to the Principles.*

Accountability mechanisms that Participating Members may implement: Participating Members commit to implementing reasonable policies, procedures, and practices to help ensure adherence to the Principles. Participating Members may implement training programs for employees and other personnel that handle *Covered Information.* Participating Members may consider creating internal privacy review boards to evaluate and approve new technologies and services involving *Covered Information.* Participating Members should make available reporting mechanisms for consumers to report concerns to Participating Members. Participating Members also commit to taking reasonable steps to ensure that *Third-party Service Providers* adhere to the Principles in providing *Vehicle Technologies and Services* that involve the collection, use, or sharing of *Covered Information.*

V. Contact Information

Alliance of Automobile Manufacturers
803 7th Street, N.W., Suite 300
Washington, DC 20001
Tel: (202) 326–5500

Global Automakers
1050 K St., NW Suite 650
Washington, DC 20001
Tel: (202) 650–5555

APPENDIX PARTICIPATING MEMBERS

BMW of North America, LLC
Chrysler Group LLC
Ford Motor Company
General Motors LLC
Mazda North American Operations
Mercedes-Benz USA, LLC
Mitsubishi Motors North America, Inc.
Porsche Cars North America
Toyota Motor Sales, USA
Volkswagen Group Of America, Inc.
Volvo Car Group

Senator PETERS. Thank you.

Having said that, Mr. Brookman, the problems of privacy and security certainly are widespread in the context and not limited to

the Internet of Things, as we have been hearing about today. But having said that, with the auto industry being very proactive with their set of principles that they just recently put together to protect consumer privacy and personal information from cyber threats, do you agree that this is a step in the right direction? What are some of your thoughts about the industry's efforts?

Mr. BROOKMAN. Yes, I think it is really great to see them being proactive on this issue, recognizing they take privacy very seriously especially with their cars. Cars are incredibly personal devices. So I think those principles are a very good first step.

I would probably want to see a little more control over whether your car company always knows your location. In those principles, that is not an element. I know that the CEO of Ford was embarrassed last year at one point when he said, "well, we always know where you are." There was kind of an uproar around that because I am out driving on the road. I want to be alone. I do not necessarily want Ford to know every place I go. And he had to kind of dial back those remarks. So I think we have smart car technologies that can be deployed in ways that are very privacy-preserving. Vehicle-to-vehicle, vehicle infrastructure communications do not need to have a lot of personal information in there. As a car company, I do not need to know that it is Adam's black SUV. I just need to know that it is a big, 6,000-pound vehicle. So they can be deployed in really privacy-preserving ways.

I want to make sure that whatever principle is going to be adopted, the fundamental idea of user autonomy is really important, that I am in control of my car. I paid $30,000 for this thing. It should work for me. And, you know, maybe I am totally happy having Ford give me turn-by-turn instructions, but it should be a question of user choice.

Senator PETERS. Great. Thank you.

And, Mr. Davis, in your testimony you mentioned the integration of Intel into the Internet of Things with sensors, and you talked about heating and air conditioning which allows the operator to identify opportunities in real time to reduce power usage.

I am sure you are doing a number of things in the manufacturing sector, which of course has major ramifications. You mentioned it briefly in some of your answers. Could you tell us a little bit more about what Intel is doing in manufacturing and how that is going to transform that industry?

Mr. DAVIS. Certainly from an Intel manufacturing perspective, I think we are one of the most sophisticated manufacturers in the world. We certainly create the most complex devices on the planet. And our factories today are really already kind of models of the Internet of Things. And what we are learning, as we go further along in the implementation of these kinds of technologies, we are learning even more as we can gain more access to data inside our factories. And it is allowing us to have better insights into how our products perform.

We can improve the overall output of the factory. We can also make the operations much more efficient by using technologies like predictive analytics to be able to identify equipment that is nearing a point of failure and being able to take it offline in a proactive manner, in a scheduled kind of downtime, saves us a tremendous

amount in terms of factory interruption and improves the overall productivity.

And these are the kinds of technologies that we are putting into our own factories. We are learning as we do these and then offering those kinds of technologies and learnings to other industries as well. Things like motors and pumps and compressors, any kind of piece of equipment like that can benefit from the basic physics of understanding how that device operates, being able to apply data analytics and predict when it might fail, and avoid that failure in a manner that we can anticipate and even get to a point of machines being able to acknowledge with each other that something is going awry.

Senator PETERS. We have a question to go down the panel in the remaining minute here. We are seeing self-driving cars. We are seeing crockpots that are enabled by Internet technology as well, the full gamut of things. So some industries are embracing this. Others not so much.

What would be your view of what industries are really on the cutting edge right now? Maybe we can just start with Mr. Abbott, if you were to pick one industry that is just really leading the way.

Mr. ABBOTT. I think particularly in the enterprise phase, like manufacturing and logistics.

Mr. DAVIS. We would say that retail is one of the industries really most poised to take advantage. Manufacturing would be close behind that.

Mr. DONNY. I agree. Industrial applications of sensors are probably the driver for most of the Internet of Things.

Mr. THIERER. At the consumer level, I would just add that health and fitness for wearables is exploding, and there are probably many people in this committee room who are wearing a wearable fitness device on their wrists and used it like me to lose 30 pounds.

Mr. BROOKMAN. And I would say in the consumer space the area that I am most excited about is actually cars due to the incredible safety benefits and convenience benefits you are talking about.

Senator PETERS. Right. Thank you.

I yield back.

Senator MORAN. Senator Schatz?

STATEMENT OF HON. BRIAN SCHATZ, U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you.

Mr. Davis, you mentioned that China and Brazil are ahead of the United States in developing a plan. And I guess my question is, are they only ahead in terms of having developed a plan on paper, or are they actually ahead of us in terms of developing and taking advantage of the Internet of Things?

Mr. DAVIS. It is really both. It is having that plan that is a national plan and then aligning the implementation around it. So we are actually seeing both in the examples that we cited.

Senator SCHATZ. And I assume in the examples that you cited, that these were government-driven plans more so than any of us would be comfortable with in the American democracy system?

Mr. DAVIS. You know, the level of comfort, I guess—we will have to assess that.

But certainly I think there are opportunities to encourage innovation, to drive public-private partnerships.

Senator SCHATZ. So my question is, if we are going to develop a national Internet of Things plan that is in the context of a free market and the context of a democracy, how do we strike the right balance in terms of it being private sector-driven, which I think we all agree on, and having a light touch and not getting into regulating right away? So that is one question.

The other concern I have is simply time. In order to develop a plan in an American-style democracy, it may be a couple of years before we are able to render one. And I feel like we do not have enough time for that.

So I would like you to address both questions, the public and private balance and how do we do this efficiently enough to have a plan that is meaningful.

Mr. DAVIS. I certainly agree. I think trying to regulate it or legislate it, given the pace of technology and the pace of innovation, it will be tough to keep up.

I think there are things we can do that help lead the way, again working with different industries to understand barriers and freeing those barriers, encouraging them to innovate in very specific areas, and also driving research.

A great example would be data analytics. As we look for data scientists who can extract the information from the 44 zettabytes of data that is coming our way by the year 2020, certainly encouraging the education of the next wave of engineers and scientists to be able to support that I think is a good area.

Then the last I would cite is there are some industry consortiums that are moving fast in the U.S. There is the Industrial Internet Consortium. You know, five U.S. companies founded that. It is over 100 companies I believe today globally. It is intended to define areas of innovation that the industries need to align around, creating workgroups to actually go implement these recommendations, and then also making recommendations to standards bodies to evolve the standards as necessary. So I think there are things that we can do to use those consortiums to lead the way.

Senator SCHATZ. I have to move on to the next question. There was a mention of encryption but it was brief. And I am a little surprised that we have not kind of dug deeper into the question of encryption because it seems to me that a combination of empowering consumers, some light but not zero touch on the regulatory side, and increased and improved encryption technology is going to be what addresses a lot of the concerns expressed by my ranking member and others about the Internet of Things. And so if we could just go down the line and if you could just talk briefly, each of you, about the potential for encryption to resolve and solve some of these data security and personal privacy issues.

Mr. ABBOTT. Thank you, Senator.

So encryption will be helpful. It will not be the panacea. And I think one way to look at this is if you looked at how e-commerce emerged on the Internet. Initially there were websites that did transact—that were not necessarily over an encrypted piece, and there were attacks. And I think in the same way that over time

best practices were adopted by engineering teams, the same will actually occur with IoT and is occurring today.

Mr. DAVIS. So we think the use of encryption is important in how data traverses networks. We need to make sure that the data that we are receiving from that device is data we can trust. So trust is essential, I think, to the evolution of the Internet of Things.

But encryption alone I do not think solves the problem. Again, I think there are some best practices that we are learning and evolving and we can do so through these consortiums to implement those effectively.

Senator SCHATZ. I am almost out of time, so I am going to call an audible and not go down the line because I have a feeling you are all going to be for encryption and find the potential there.

But it does seem to me that one of the challenges is to empower consumers to know whether there can be some kind of Good Housekeeping Seal of Approval so that a consumer can know whether this is an IoT device that they ought to feel safe about, that they ought to feel comfortable with, and whether it is opt in or opt out, I think those are important policy and consumer choices to be made. But on a very basic level, consumers have to know whether someone is meeting some basic standards, and I think that is one of the challenges right now.

Thank you.

Senator MORAN. Thank you, Senator.

The Senator from Montana, Senator Daines?

STATEMENT OF HON. STEVE DAINES, U.S. SENATOR FROM MONTANA

Senator DAINES. So I get to represent the great state of Montana, and one of the things I will hear is when a bureaucrat flies into Montana from D.C. and they say they are there to help, we get really scared about that.

So I have a question regarding—and I say this in the context of someone who was part of a cloud computing startup we took public. We had an office just north of you there from Kleiner Perkins in Menlo Park. We were up in San Mateo, had 17 offices around the world, 33 languages, and our product is a cloud computing CRM map called RightNow Technologies that Oracle acquired a couple of years ago.

And I do have concerns as a consumer, as a parent about privacy and security, but I have also a great concern about the ability for technology innovation to move quickly. Somebody asked what made your company successful. Our CEO said we can run faster than anybody else, and that was our competitive differentiator.

Unlike the glacial speed of D.C., you all are living in a very different world than the Beltway here in Washington. You move at the speed of electrons and we move at the speed of glaciers here.

So a top-level question is, can the Federal Government be helpful in regulating something I do not think they even understand? Who would like to take that question?

Mr. THIERER. Well, I think they are going to have a really hard time regulating the Internet of Things. I mean, the Internet of Things, as you suggested, Senator, moves the pace of Moore's Law and is doubling every 18 months just like processors do. So that

sort of speed is going to be hard for us to set in stone any sort of rules that basically can govern that kind of innovation.

What policymakers can do, beyond establishing a clear vision for how the Internet of Things can be fostered, is to suggest efforts to educate consumers and make them aware of potential security and privacy risks and vulnerabilities. Our government has a long track record of doing an excellent job of this in other contexts. I would just commend the Federal Trade Commission and many other Federal agencies who have OnGuard Online, which is a wonderful online portal for consumers to find great information about privacy and security best practices.

Mr. BROOKMAN. Yes. I mean, to some extent, the Federal Trade Commission is already active in this area. Mr. Thierer mentioned 50-some data security cases, which I think most people recognize is probably a good idea. You should be using reasonable data security requirements.

On the privacy side, we are primarily just asking for better transparency. Right now I have a device. It is really hard to figure out what it does. At the very least, it should be written down somewhere what the company does. If you cannot explain it in a statement, maybe you do not really understand what it is doing, and that poses some privacy and security risks.

Senator DAINES. All right. Thank you.

And I think that whole opt in/opt out was an interesting discussion. I look at that—because I am running around with my devices. As someone who is a father of four children, they will say, Dad, you are so January 2015 already. You know, I mean, it is already outdated 2 weeks into February.

But I think information does become currency, and so when I opt in to one of my apps—perhaps it is my airline when it knows I arrive in a certain city—it performs at a high level. It becomes currency with that information as the consumer makes that choice ultimately.

And I guess I also have great faith in the power of crowdsourcing and what happened—the example you had in the K cups there of the reviews on Amazon. The consumers are not—I think they control the world. The horse left the barn a long time ago in terms of the consumer having the ultimate voice oftentimes in these debates in the free markets.

I do believe, though, that national infrastructure and fin services perhaps and maybe others should be held to a higher standard and more strict standards as we look at the risk management. As you think about any kind of regulatory touch, how would you differentiate perhaps the Internet of Things from fin services infrastructure and so forth? Mr. Davis?

Mr. DAVIS. I am clearly not the expert on financial services. So I will say that up front.

But as we look at this breadth of Internet of Things, given the breadth of it, yes, I believe there will be different expectations for different industries and different market sectors. What happens in the consumer space I think is certainly critical in terms of both security and privacy. In the industrial space, there are many opportunities where we can open up and look at data from different data types and different sources that will enable us to derive the value

of the Internet of Things, new services, new products. So I think we are going to see different requirements, different needs across different industries, and to your point, financial services could certainly be that example.

Senator DAINES. I am running out of time. I wanted to make sure I asked this question, though, and this is as a father of four children. With digital natives now running everywhere in America as they are growing up here, believe me, everything opens up with a swipe of the finger. Are there appropriate security measures and parental disclosures we should be thinking about to protect our children from the dangers of online security and privacy?

Mr. THIERER. Well, Senator, I have testified in front of this committee many times on online child safety issues and have written books on parental controls and online safety technologies. And I can tell you this is a never-ending battle with myself as a father of two young children who are digital natives as well, and they are sometimes ahead of us as parents in terms of their capabilities. That being said, it is a constant educational process, and there is never any end to it.

What the government can do is get more serious about media literacy and technological literacy efforts in what is called digital citizenship programs to try to make children more aware of appropriate uses and inappropriate uses of their technologies.

Senator DAINES. Yes. I am out of time. But this is a case where our kids are faster and more quickly adopting this technology oftentimes than parents are. It is a profound issue we have to deal with here I think as a country as parents around how do we protect our children in this evolution.

Senator MORAN. The Senator from Nevada, Senator Heller.

STATEMENT OF HON. DEAN HELLER, U.S. SENATOR FROM NEVADA

Senator HELLER. Chairman, thank you. Thanks for holding this hearing. It is an unusual topic, to say the least, but one I think just as important as it is odd.

I want to thank all the witnesses for being here taking time out of your day to help us better understand where we are trying to go on this.

I have a Microsoft Fit-band—now, whether it is mine or a member of my staff's sitting behind me, I am not going to tell you. But, you know there is tremendous amount of information you get out of this Fit-band. I am looking at downloading how many steps. I am downloading sleeping habits. I can tell how many hours slept, how many times you woke during the night, what the efficiency of the sleep was—and I do not even know what that means—how many calories burned while you are sleeping for those 8 hours. It is incredible the amount of information that you get out of one of these Fit-bands.

But just as this information is available to me, I guess the question we are trying to ask here on this committee is who else has this information. Where does all this information go?

There is another app on calories. It tells you what you ate, links the two programs together. It tells you how much you are exercising, how much you are eating at the end of the day. At the end

of the day, you are, I guess, figuring out whether you are making progress or not.

And I guess we are trying to decide whether you know that or does the rest of the world have access to that kind of information. Is that not in essence what we are dealing with? Is this not what we are trying to figure out?

The amount of information that is out there—I read a number. Let us see if I can find it. The amount of information that is available to us. Here it is. We are producing multiple ziggabytes each year, a number that I do not quite understand. I do know it is 21 zeros behind a 1 or a trillion a million times. That is the kind of information that is out there.

I may not be the only one that is wearing a Fit-band. There is probably multiple people here in this room that are also wearing these Fit-bands.

I guess the question is, is there a way—and, Mr. Thierer, maybe I can ask you first. Can we identify ways in which this data can be protected without doing harm?

Mr. THIERER. Yes, Senator, I think we can. I think, obviously, consumers are going to be concerned about certain types of personal information, specifically sensitive health information, being shared too broadly, and that is going to necessitate different types of approaches and policies for that sort of information. But a lot of the information that is being collected by these devices and the information, the data that we are shedding, sort of what is called our data exhaust, is going to be more easily shared and probably a lot of consumers want it to be more easily shared. The complaints that a lot of app developers get is that it is not easy enough to share some of this data with some friends and other people or maybe your doctor because of existing policies or laws.

Senator HELLER. Is that not where we are going? This information is going to be linked to your personal physician?

Mr. THIERER. I think so, but of course we have to deal with things like HIPAA and other types of laws that make that potentially difficult. And I think there are going to remain some policies in place to deal with very sensitive forms of information like health, financial information, and so on. But I think for the most part there is a really delicate balance here because a lot of consumers are going to want to have more personalization and customization in their devices so they can learn and share even more about themselves with friends, colleagues, physicians, and others. So that is the balance we have to walk.

Senator HELLER. Mr. Brookman, how does this happen? How do we make this happen without harming innovation?

Mr. BROOKMAN. Yes. I think Fitbit is actually a really good example. You are creating a lot of really personal and interesting information, but you kind of want to have control over it. You do not necessarily want the world to know what your heart rate is. And people might be able to do really interesting research on it, but you do not want to necessarily be everyone's guinea pig.

I think Fitbit actually understands that. They actually have a really good rule in their privacy policy. You are creating really a lot of information, but it is yours. You are in control over it. We

are not going to sell it to data brokers. And I think that should probably be the default especially for really sensitive stuff like this.

If you want to sell it to somebody or make it available to researchers, just get my permission for it. If you want to sell it to data brokers and, say, we will give you $5 off your Fitbit, that is fine. Make a value proposition for it. And so I think for things that would be surprising or confusing to a consumer, I think there should be a little more obligation to say, OK, here is what you are going to do. It is your device. You paid for it. You make the decision about what you want to do.

Senator HELLER. Yes. Thank you very much for your comments.

Again, I want to thank the panel for being here.

Chairman, I support where Chairman Thune is coming from on this particular issue, trying not to do harm without harming innovation as we wrestle with the very issues that the panel and I discussed today.

Thank you.

Senator MORAN. Thank you, Senator Heller.

The Senator from New Jersey, Senator Booker.

STATEMENT OF HON. CORY BOOKER,
U.S. SENATOR FROM NEW JERSEY

Senator BOOKER. Thank you very much, Mr. Acting Chairman.

You know, I just want to pick up on it. This is a phenomenal opportunity for a bipartisan, profoundly patriotic approach to an issue that can explode our economy. I think there are trillions of dollars, creating countless jobs, improving quality of life, democratizing our society in ways that gives advantages to people who are being marginalized on the edges, breaking down barriers of race and class. We cannot even imagine the future that this portends of, and we should be embracing that. America right now is the net exporter of technology innovation in the globe, and we cannot lose that advantage. It to me is something that we should continue to be: the global innovators on these areas.

And so a lot of my concerns are really what my Republican colleagues also echoed, which is we should be doing everything possible to encourage this and do nothing to restrict it. And there are a lot of legitimate fears, but in the same way of every technological era, there must have been incredible fears starting with the airline industry, just human beings taking flight, had tremendous fears. But for us to do anything to inhibit that leap in humanity to me seems unfortunate.

And so from copyright issues, security issues, privacy issues, all of these things are worthy of us wrestling and grappling with, but to me we cannot stop human innovation and we cannot give advantages in human innovation to other nations that we do not have. America should continue to lead.

And I also believe that this has got to be a public-private partnership, that we all have a role. The very Internet itself is the result of a public-private partnership, investments made by the public space, by the civic space that innovators and entrepreneurs have made, again, beyond the imagination people had just 20–30 years ago.

So I want to jump in on two things, and I imagine there might be another round, but the first issue is spectrum. I have a bias. I think government hoards too much spectrum, and I think that there is a need for more spectrum out there. Everything we are talking about—and I think the word was used, an "obesity" of usage and needs going out there—is going to necessitate more spectrum. And so for me, yesterday Senator Rubio and I, again in a bipartisan way, reintroduced the WiFi Innovation Act which aims to address this need by encouraging more spectrum sharing and freeing up more spectrum.

And so I just want to highlight the importance of these sharing agreements and increased spectrum availability is going to be in this just for the record. And let us just do it really quick. Anybody who wants to jump in on that.

Mr. DONNY. I will lean in and weigh my support. In agriculture we have very unique challenges in moving data. You do not have a building, your home in which your Fitbit when you walk in the door, syncs up with the WiFi that you have got available. On the farm, you do not have broadband. You do not have WiFi available to you. So if we want to lead the world, continue to lead the world in agriculture—and it will be through technology—we have to solve—this is a fundamental problem that I think a public-private partnership is perfect for.

Senator BOOKER. Right. And so do not get me started about states that are banning broadband innovation by municipalities. Do not get me started on that. But you agree that we have to solve these problems. We have to create more spectrum availability. And the fact that countries like South Korea and others have more broadband penetration than the United States of America is absurd, and we need to solve these problems.

But I want to stick with you being that you are the courageous one. And another thing that is an issue for me, where this issue of fear and legitimate concerns undermine American leadership, is the issue of drones. It is one of those issues that strikes fear in Americans' concerns. But the potential and possibility for drone technology to alleviate burdens of our infrastructure, to empower commerce, innovation, jobs, to really open up unlimited opportunities in this country is pretty incredible to me. And in your area of agriculture, as I watch our government go slow in promulgating rules, holding back American innovation, what has happened as a result of that is innovation has spread in other countries that do not have these rules, have put in sensible regulations, but now we are seeing innovation and technology export from America and going other places.

In the agricultural context, as my time runs out, could you just give us a picture? Because I see mine surveys, agricultural uses abroad that are not being done here. Could you just comment on that real quick?

Mr. DONNY. Thank you, Senator. It is a great topic. Agriculture is a wonderful use case for drones. There are wide open areas, lots of land to survey and crop scout. We can use drones to improve productivity. So instead of sending someone out to look at the field to go look for disease and pests, you can send a drone out that identifies those unique challenges, and then when you identify that

space, you can be more effective with pesticide applications, with use of resources. And it is a wonderful use case. We should be leading this. And the industry is spending hundreds of millions of dollars in drones, and agriculture is waiting for this to happen.

Mr. ABBOTT. I can comment, Senator, from the investment side. This is an area that in particular we have been focused in and have made investments and plan to continue additional investments in because we do see that we are at a very early stage of a massive disruption in a lot of these commercial opportunities.

Senator BOOKER. My friends at Kleiner have told me basically a lot of the innovations now are not happening in the United States. A lot of the research and investments are happening overseas because of Government policy that is restricting that here. Is that correct?

Mr. ABBOTT. It is correct that there are countries outside the U.S. that are further along on the regulatory side that we should try to learn from.

Mr. THIERER. Senator, I would just add that we need to be thinking of the drone opportunity as creating airspaces of platform for innovation the same way the Internet created a platform for new innovation. And the way we counter the fear that you correctly identified that is out there is to counter it by talking about the life-enriching and lifesaving opportunities of these and other Internet of Things devices.

Senator BOOKER. I am now really over on my time. We have people that get injured every year, and other countries like France are using drones to fix poles, not putting human beings in danger, doing it at a fraction of the cost and a fraction of the time. Forgive me.

Mr. DAVIS. Senator Booker, if I could just add on to that. I think you made two really great points around efficient use of spectrum. As we think about 50 billion devices, I think that is a really key topic.

The other is around the distinction between consumer applications. Drones are a great example. A lot of the attention is around consumer applications. But around the Internet of Things, we are going to see the economic benefit in the commercial and industrial applications. Drones are a great example. There are many others.

Senator BOOKER. Thank you.

Senator MORAN. Senator, thank you.

The Senator from Nebraska, Senator Fischer.

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Senator Moran.

I loved Senator Booker's enthusiasm on this, and we are working on the Internet of Things with Senator Ayotte and Senator Schatz and trying to move forward.

I think I am past the basic question on what is the Internet of Things. That is always a good first start here.

But there are, I believe, huge benefits out there. I would like to ask you, Mr. Abbott, what do you see as truly the benefits of the Internet of Things? And do you think, as we move forward, this space is going to be dominated by established companies or is there

going to be room for those small startups? Where are we on that? And how can we continue to be a force for innovation instead of stomping down that entrepreneurial spirit?

Mr. ABBOTT. Thank you for the question, Senator. And I will actually come back also to reiterate some of the comments I made to Senator Booker.

Senator FISCHER. Well, his time is done.

[Laughter.]

Mr. ABBOTT. We are particularly excited with the commercial applications in the drone space, whether it be mining, inspection, precision agriculture, or just pure safety. And there are a couple examples there with companies we are working with and we are really excited about.

We tend to believe, certainly, that it is going to be these small companies that disrupt the large companies in this space. And I think we are seeing this at the early days for some of these contractors on the Government side realizing that drones can be built by these small companies for much lower costs in much more innovative ways, realizing at the same time that we do need some guidance on the policy side, which I know the FAA is working on.

Senator FISCHER. And, Mr. Thierer, when you were giving your opening statement, it reminded me that 9 out of the 10 top innovative companies in the world in 2013 are American. Is that going to continue? What kind of policies are we going to need as we address the Internet of Things? I guess I am really concerned about Government getting in the way and getting in the way of that innovation, whether it is a large company or a small startup. Sure, there are concerns out there, but I do not want to see all the excitement that is with the Internet of Things move overseas. So what can we do with that?

Mr. THIERER. Well, absolutely, Senator. And I want to commend you on your recent speeches on this issue and your leadership on it because you have identified that we got policy right when it came to the Internet more broadly, and we now need to get it right for the Internet of Things.

In essence, America found the sort of secret sauce of modern innovation. We figured out how to get the right policy prerequisites in place starting with essentially a light touch vision instead of a plan. Senator Schatz pointed out earlier, do we need a plan? I think we need a vision more than we need a plan. And the vision we had, led by Congress and the Clinton administration in a nonpartisan fashion, was that sort of light touch, market-driven approach that addressed harms as they developed instead of trying to preemptively anticipate every one of those problems like some of our competitors did overseas and say we need to preemptively figure out how to solve every problem before we allow technology and innovation to go forward. Well, there is a reason that the household names in Europe on technology are American companies. Meanwhile, it is hard to name any European innovators here in the states.

Senator FISCHER. Well, I know I am working with my colleagues, Senators Booker and Schatz and Ayotte. Hopefully, we are going to present a vision as we work on a resolution that we will get before

Congress. I think that is very, very important that we have that vision and that light touch.

I would like to just touch on something that, Mr. Brookman, you and also Mr. Davis said earlier about security is an afterthought and when new products are built, that is when the security needs to be designed and put in them.

We had a hearing earlier about data security, and I have deep concerns about cybersecurity in this country. And at that hearing, we heard about businesses that may be getting pressured by foreign governments to give up their software in order to get a bigger market share in another country.

What do you feel about that? And what do you think should be a response by our government by this Congress because of the interrelationship that we see with much of the software and what we have seen with nation states creating mischief with companies?

Mr. BROOKMAN. Yes. I certainly do not want to see any mandated vulnerabilities in encryption technologies, including backdoors. Unfortunately, it is something that the U.S. Government has asked for, which I think sets a really bad precedent for the rest of the world, saying that we need to have mandated vulnerabilities into data security. So I think the best thing we can do is not doing it ourselves. Therefore, we would have some high ground to stand on to say, no, other countries should not be doing it either.

Senator FISCHER. But other countries are doing it. So what steps do we need to take, or do we need to take anything? How would you prohibit this or would you?

Mr. BROOKMAN. It is a really good question. It is one I have not put a lot of thought into. My hope is that companies doing business overseas will resist those sorts of requests. It is a tough issue for companies that are spread out all over the globe. When do you censor speech? When do you take down information in response to the right to be forgotten? Companies have a really delicate balancing act. I have never heard the best answer as far as how do you take inconsistent legal obligations when you are spread out all over the globe.

Mr. THIERER. And I would just add, Senator, that this is exactly where our Government needs to be standing side by side with companies when they have these problems internationally and defending them when they bake in better encryption and security by design instead of, as Mr. Brookman suggested, undermining them and saying, well, maybe you need to have some backdoors for us instead. That is not going to be a consistent principal message to take out globally.

Senator FISCHER. Mr. Davis?

Mr. DAVIS. Senator Fischer, I think you made a great comment in terms of the legacy devices that exist today as opposed to security being an afterthought. Really, I think part of the challenge today is about 85 percent of the billions of devices that exist today that have integrated computing are not connected to each other or the Internet. That is an opportunity. We can connect to those devices. We can start finding data that we did not have before. I gave the manufacturing example earlier. The ability to extract data that we have had access to in the past is one of the promises of the Internet of Things to drive greater efficiency. But we can do so in

a way that we can connect those securely. There are technologies that allow us to even connect those older legacy devices, be able to feed that data up into a data center or cloud to do the kinds of big data analytics that are going to be so valuable in addition to building it in from the beginning with a broad end-to-end security technology strategy in mind to begin with.

Senator FISCHER. Thank you so much.

Thank you, Mr. Chairman.

The CHAIRMAN [presiding]. Thank you, Senator Fischer.

I understand Senator Moran has done a brilliant job of presiding. So thank you.

Next up is Senator Gardner.

STATEMENT OF HON. CORY GARDNER, U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Mr. Chairman.

And thanks to the witnesses for being here today.

Where else in Congress, I guess, do you discuss super cookies, milk, and drones in the same committee hearing?

[Laughter.]

Senator GARDNER. This has been fascinating to hear, but it is exciting to talk about the future of technology and where we have been and where we are heading.

So it was 1997, I believe, when our farm equipment dealership sold our first GPS satellite system, advanced farming system. And we sold it to a gentleman who was right around 65 or 70 years old and it had the PC MCA card, the pin card that you put in to download the data. And I think at that point there were three data points that we were measuring off of the combine. It was probably some kind of a protein count, moisture count, and of course your yield. And so those were the three things that we did.

And over the past 20 years, of course, now we have seen layer after layer of data, whether it is moisture data, whether it is—you know, information that you can plug into your seed application, your seed rate, your flow rates on fertilizers and things like that. And of course, we have been using phones to turn on and off the sprinkler for decades in agriculture. And so all a part of prescription farming and how we can do a better job of providing food, fiber for the world.

The same thing we can do in the supply chain with manufacturing in industry, whether it is the vehicles or furniture. We can do the same kind of approach with the new technology.

But so much of this is tied together with how we are going to approach spectrum, getting back to Senator Booker's point, and how we are going to approach availability to innovate.

So keeping in mind the farm model, you have a combine—say you have a tractor going through the field with a cultivator. You have a sprinkler in the field that has—maybe it has got valves on it that are each individually controlled through the Internet, WiFi, perhaps from the tractor itself or the farm or your phone, wherever you are to apply a different percentage of fertilizer as your chemigation system is working. You have a drone flying over the field that is taking a picture of it to see where you may need a lit-

tle bit more or less nitrogen. All this, I am assuming, is going to be with unlicensed spectrum.

There was a situation in Congress just over the past year where—many of us do not even know it—in our offices there was an unlicensed spectrum issue that came up in our offices here on Capitol Hill. And it was an unlicensed spectrum issue where the FCC had sort of said, yes, go ahead, and then a license came in to take this spectrum.

How are we going to handle the Internet of Things? How are we going to handle and approach these issues when you have conflicts of more need for spectrum, issues of unlicensed spectrum, issues of people coming in and getting licenses for an area that may already have a campsite in it, so to speak?

Mr. Abbott, I do not know. That is a very open-ended question. Do we have policies in place, I guess, to address the balance—growing the Internet of Things, growing device application, growing utilities that we can be more productive with without a better definition of how we are going to handle unlicensed spectrum issues?

Mr. ABBOTT. Thanks for the question, Senator.

I do think that we do need to provide more licensed spectrum for innovation. I think today, while it is not a constraint we are seeing in early stage companies, it soon will be as more and more of these services and applications get deployed in the enterprise and in the consumer space.

Senator GARDNER. Mr. Davis?

Mr. DAVIS. Well, we certainly see there is an important need for licensed spectrum and unlicensed spectrum. And my comments to Senator Booker earlier—you know, what we are really looking at is how do we most efficiently use that spectrum that is available? Because as we think about connecting 50 billion devices, it is really how to most efficiently provide that to the different kinds of uses and applications.

Senator GARDNER. Mr. Donny, I do not know if you want to address that or not.

Mr. DONNY. I think I have addressed it several times. Both licensed and unlicensed, as you know, is used in agriculture and we need all we can eat really.

Senator GARDNER. Mr. Thierer?

Mr. THIERER. Yes, we all agree on this one. And I think what you and Senator Booker raise is a valid point. I think the problem is a political problem of when you have incumbent constituencies who already hold or hoard a lot of this spectrum, shaking some of that loose, you are going to have to create better incentives for them. And we are going to have to counter the narrative that only they have sort of lifesaving or life-enriching applications. We do too on this side, and we need more spectrum for it.

Senator GARDNER. And as Mr. Donny said, though, at the same time in rural America, we do have a separate challenge of making sure that we have enough mobile broadband to supply cell phone signals and everything else. So you do have this kind of a challenge particularly in rural areas where you have a conflict even within itself that needs to be addressed.

I guess I have a lot of questions. I would love to just have this conversation all day, but at this point, Mr. Chairman, I will yield back.

The CHAIRMAN. Thank you, Senator Gardner.

Senator Moran?

STATEMENT OF HON. JERRY MORAN, U.S. SENATOR FROM KANSAS

Senator MORAN. Mr. Chairman, thank you very much.

Last week, a subcommittee held a hearing on data breach security, data security. We talked about breach. We talked about the standard of what a breach is. We talked about whether there ought to be preemption. In the kind of, I think, data breaches that we have been considering, what we are worried about is a consumer's personal information is obtained by those who should not have it, financial information, Social Security number, and how that information can be used to the consumer's detriment.

And certainly here there are security issues. Part of it is related, as we have heard, to privacy. But what is different about the Internet of Things? What kind of data breach should we be worried about? So somebody learns that your milk needs to be replaced in the refrigerator, are the data breach security consequences—let me say it differently. Is the data breach, the consequences of that breach, something different than what we normally think about when we talk about data security? And if so, what should we be thinking about as we try to solve the issue of the breach and the consequences?

Mr. ABBOTT. So I do think that it is somewhat relative to the domain and the application in regards to the severity of a data breach, indeed.

Senator MORAN. What would be the spectrum within the Internet of Things?

Mr. ABBOTT. So at one end of the spectrum, you have a sensor just emitting temperature. On the other end, a sensor in the medical world that is emitting some type of physiological response that has control. Because there are sensors that are just emitting data, and there are sensors that actually can control. So we have this spectrum of, we will say, criticality, if you will. And so I do not think there is a one-size-fits-all data breach definition. And it is the same way that I do not think it would be appropriate to have a single policy for security across that spectrum.

And I think it also relates to data sharing. If you look at temperature, that might be actually a great sensor to share widely, whereas you go to the more personal data, maybe that should be shared locally, just that individual, and have a very clear ability to opt out if the user does not understand the benefit that he or she is getting by sharing that data.

Senator MORAN. Mr. Abbott, let me ask you. I will come back, Mr. Brookman. Mr. Abbott, let me ask you in particular. When you are looking for investors in companies or you, Mr. Donny, when you are finding somebody who wants to invest in a company involved in the Internet of Things, do they consider their investment risk based upon the potential of security/privacy breaches? Is that built into the investment?

Mr. ABBOTT. It typically is, and I think it is more a function of the team that is involved that is actually building the company and building that product. So if we look at a company like NEST that we are investors in, certainly that was a consideration.

Senator MORAN. Is there any private insurance that is developing to protect your companies and the investors in those companies from the consequences of a breach? Can you become insured in a private sector way?

Mr. ABBOTT. There may be but I am not aware of them.

Senator MORAN. Mr. Brookman, you wanted to respond earlier.

Mr. BROOKMAN. Yes. So I know traditionally data breach notification has been about financial information, but I think we are increasingly recognizing that you can lose other personal information as well. Think about the iCloud celebrity hack. I mean, we have a personal interest in that. If my pictures were hacked, I would want to know about it. The Sony case, for example. If my e-mails get hacked, I would want to know about it. So we are actually seeing some states pass some broader breach notification laws, saying if your online accounts get hacked, well, of course, you should tell them about it. So I think any Federal standard should consider that as well or at the very least not preempt those states from passing breach notification laws that extend to new categories of data that are not addressed by a relatively narrow financial data bill.

Senator MORAN. Mr. Chairman, thank you.

The CHAIRMAN. Thank you, Senator Moran.

Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. I think I have a worse cold than you. So this will not be one of these filibustering-by-the-Senator moments. I will let you guys answer as long as you want.

[Laughter.]

Senator KLOBUCHAR. This is a very important issue, of course, the future of connected technologies. This year at the consumer electronics show in Las Vegas, companies from around the world showed off their newest technologies, 900 of which were connected devices. So it is a pretty exciting time but also, as we know and have discussed, a time of making sure that consumers are protected as well.

Senator Hoeven and I—maybe you are aware of this—last year introduced the Data Privacy Act, and we plan on reintroducing it again.

An event data recorder, as I think many of you know, is a device that records about 5 seconds of technical safety data when a crash occurs. EDR's can be the only resource available to determine the cause of a crash by providing information about what a driver was doing in the seconds leading up to the crash.

Starting in September 2014 all new vehicles will have an EDR, and NHTSA does not have the authority to determine who owns the EDR data, which is why we introduced this Data Privacy Act bill. Our bill makes clear that the owner of the vehicle is the right-

ful owner of the data collected by that vehicle's EDR and may only be accessed under rare circumstances.

Mr. Brookman, do you agree that empowering consumers to have ownership of their data is important, similar to what we have outlined in the Data Privacy Act?

Mr. BROOKMAN. So I have not looked at that bill in some time. So forgive me for not supporting it right now.

My recollection of it is I think I very much agree with the general principles of it. This is my car. I paid a lot of money for it. I should have control in most situations of when that data is accessed. Obviously, in an accident, there will be a process for accessing that information, but fundamentally you should not be sending it off in other circumstances without my control.

So I want to look at the bill specifically, but I think that I very much agree with the general tenor of your statement.

Senator KLOBUCHAR. OK, very good. Thank you. I just want everyone to be aware of that bill.

One of the concepts that the FTC recommends for business dealing with consumer data is to design privacy and security into each product. It is oftentimes more difficult to retrofit a device with new technology to combat threats or to patch privacy controls than it is to design or install it to begin with.

Mr. Davis, if businesses and innovators keep consumer data privacy control in mind throughout the development process at the get-go, do you believe they will continue to have the flexibility needed to innovate while also protecting consumers?

Mr. DAVIS. Certainly there is a balance. Thank you for the question. Certainly there is a balance between security and privacy. Security I think we often think of as the technical implementation of the product in such a way that we can provide the level of privacy that consumers would expect. And so certainly I think as we develop the kinds of products that we are developing, with both in mind. So we have a set of requirements around both that our developers need to meet. And we have part of our organization who is looking at those implementations and making sure that our engineers and developers are adhering to those requirements.

And so I think from a higher level, being able to define what the end looks like in terms of where we need to get to as industries in the objectives that we are trying to accomplish is a way to implement these kinds of things into a national IoT plan that has long-reaching objectives without limiting the short-term innovations that are possible.

Senator KLOBUCHAR. OK, very good. Thank you.

One of the issues I have been working on since I got here has been cell phone unlocking. You mentioned it, Mr. Bookman, I think in your testimony. In fact, it was one of the first bills I introduced, The Cell Phone Bill of Rights. As you know, there have been changes, and today is the anniversary of carriers' voluntary agreement with the FCC to increase transparency for their unlocking policies.

Yesterday I sent a letter to the FCC and the CTIA for an update on that agreement.

Mr. Brookman, you mentioned in your written testimony that cell phone unlocking was an example of why policies need to be in

place in order to ensure there is competition for connected devices. Can you expand on that from your written testimony? You should also know I am the ranking on the antitrust committee in Judiciary, and so we also do a lot of work with telecom.

Mr. BROOKMAN. Yes. I think it is just normal consumer expectations where they have a device. They do not necessarily expect it to be locked down to certain carriers. If it has the technological ability to communicate with other Verizon or AT&T, of course, I should have the ability to do that. And unfortunately, it should not be incumbent upon the Library of Congress to have to pass an exception every 3 years.

You know, Samsung makes a device. It has the ability to connect to whoever it wants to. We should have that right. I mentioned the example of coffeemakers trying to lock down what coffee you can use. These products really need to be designed, you know, as a service to the consumer who is paying money for them. I own it. I bought it. It should be trying to act in a way that is consistent with my reasonable desires.

Senator KLOBUCHAR. OK.

Anyone else want to pitch in on that? OK, thank you very much.

The CHAIRMAN. Thank you, Senator Klobuchar. And I know that you and I are both hoping that the Internet of Things will lead to a cure for the head virus right now.

Senator KLOBUCHAR. It is a Midwestern problem.

[Laughter.]

The CHAIRMAN. I have in this order, Senators Manchin, Markey, and Cantwell. And I have to step out for just a minute. So Senators Manchin, Markey, and Cantwell.

STATEMENT OF HON. JOE MANCHIN,
U.S. SENATOR FROM WEST VIRGINIA

Senator MANCHIN. Thank you, Mr. Chairman.

I had to miss part of this meeting because I had another Armed Services meeting. So I am very sorry that I did not get the first of it.

Senator BOOKER. We know that because we had an Internet of Things LoJack on you.

[Laughter.]

Senator BOOKER. We are tracking your movements.

Senator MANCHIN. I do not think there is anybody who wants to stymie innovation and entrepreneurship. I do not know if 535 Members of Congress would. And we know that we are all connected because you just look out and everybody's head is down. They are working on their phones. They are working on the iPads and they do not even know we are talking.

[Laughter.]

Senator MANCHIN. So with that being said, we are moving forward.

I have a hard time believing that you are concerned that if we do a privacy bill, that you might not have access for the latest, greatest innovation in technology. If that would be the case, Facebook would have a serious problem because there are many millions and millions of people who want to share every little as-

pect of their life. So I do not think you are going to have a problem with people sharing with you.

But I think some of us have a problem if we do not want our information shared. Is there a middle ground here?

I know with the phones, when I was Governor, people would just—they wanted privacy. They said I am getting tired of all these telemarketers calling me all the time and get these unlisted phone numbers so they could block them. And they were able to block. It did not stop any innovation and creation. Nobody's business got hurt.

And I will have to be the cynic. How much money do companies make off the sharing of information right now? You all have seen it. Now come on. It is over $600 billion. So being the cynic that we might be at times, I can understand why companies do not want any type of a privacy thing because it is a big moneymaker. Correct? Anybody want to speak to that?

Mr. ABBOTT. Senator, I think one thing to keep in mind too is that by sharing that data, oftentimes it improves the consumer experience. There are many examples of products that——

Senator MANCHIN. I am saying if it improves it, do you not make it from the product itself? You are making it from selling that.

Mr. ABBOTT. And the user actually gets a reward for the sharing of that information. Let us say as an example if I am sharing data from my thermostat back to a cloud service and that collectively improves the product for the population of those users—they have already purchased the product—that is a great experience.

Senator MANCHIN. Where does this $600 billion of the economy come from? Where does it go? You are selling it and you are getting something for that, not just you are giving me more efficient service. You are selling that information to somebody else. The IoT basically is $600-plus billion growing very rapidly. So for those of us who want a little bit of privacy, we think you are doing pretty darned good.

Mr. THIERER. But, Senator, the question of where the value is going, a lot of it is going to the consumer in the form of cheap or zero prices. I mean, the fact that we do not have to spend $20 a month for Facebook or pay for every search we do on a search engine, that is value to consumers. That is an improvement in our quality of life. And if you ask most consumers how much would you pay for these services, the answer is usually very little or nothing. They like that cost. Free is a good number.

The question is what would regulation do to alter that balance and if it raised prices, would consumers appreciate it and understand why it happened. I am not so sure.

Senator MANCHIN. You are not opposed to the privacy and us being able to block. You all do it, Mr. Donny, do you not?

Mr. DONNY. We believe in the agriculture data that is owned by the farmer. That is very clear. Our objective is how do we work with the farmer to enable them to use data to make better decisions. Sometimes that is a relationship in which we are looking at data——

Senator MANCHIN. It would be a volunteer relationship.

Mr. DONNY. That is right to help that relationship.

Senator MANCHIN. So you believe in the privacy that we should have——

Mr. DONNY. I am very straightforward. I think that data privacy is important, but it is truly dependent on what data you are looking at. In ag, I think that is a very important set of information. It derives commodity prices. It could be used for regulatory purposes because there is a lot of tail end of that data use. And so we want to make sure that the grower owns their data.

Senator MANCHIN. I can understand where you all are coming from because you are afraid we might go too far. I understand. And with that being said, we have a hard time understanding that you do not believe you have enough information now because I am sure there is an awful lot of information that you do have because the financials show that. And we are just trying to find that balance I believe, and if you could help us do that—Mr. Davis, I think you want to comment on that.

Mr. DAVIS. Senator, I think your point is really important in terms of the relevance of security in everything that we are talking about with the Internet of Things. As we talk to our customers, as we talk to analysts in the industry, the number one topic—and it is foundational, the five tenets that we described—is security. And so the ability to integrate security knowing that a device that is added to my network is a device that is supposed to be on the network and the information I am getting from it is what I would expect to be getting—it is valid information—those are foundational to the Internet of Things.

In terms of privacy, you are absolutely right. We are stewards of that information in terms of balancing the value that I think has been described from having access to some of that data and the importance of protecting it and being stewards of that data in terms of the consumer. There is a balance and it is something that will continue to evolve industry by industry.

Senator MANCHIN. Thank you.

Senator Markey?

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. I am Chairman again.

[Laughter.]

Senator MARKEY. By unanimous consent, I recognize myself.

[Laughter.]

Senator MARKEY. So cars are a major part of the Internet of Things, and every year new cars are more connected than ever before. One reason that cars are such an important example of connected devices is that they are so dangerous. A small vulnerability or error in coding can lead to a catastrophic consequence for drivers, passengers, and pedestrians.

On Monday, I released a report on our connected automobiles, the Internet of Things, which describes how new cars are really no longer just internal combustion engines. They are computers on wheels.

I ask unanimous consent to submit my report for the record.

[The information referred to follows:]

TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK

A report written by the staff of Senator Edward J. Markey

Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ED MARKEY
United States Senator for Massachusetts

FEBRUARY 2015
WWW.MARKEY.SENATE.GOV

EXECUTIVE SUMMARY

New technologies in cars have enabled valuable features that have the potential to improve driver safety and vehicle performance. Along with these benefits, vehicles are becoming more connected through electronic systems like navigation, infotainment, and safety monitoring tools.

The proliferation of these technologies raises concerns about the ability of hackers to gain access and control to the essential functions and features of those cars and for others to utilize information on drivers' habits for commercial purposes without the drivers' knowledge or consent.

To ensure that these new technologies are not endangering or encroaching on the privacy of Americans on the road, Senator Edward J. Markey (D-Mass.) sent letters to the major automobile manufacturers to learn how prevalent these technologies are, what is being done to secure them against hacking attacks, and how personal driving information is managed.[1]

This report discusses the responses to this letter from 16 major automobile manufacturers: BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (with Audi), and Volvo. Letters were also sent to Aston Martin, Lamborghini, and Tesla, but those manufacturers did not respond.

The responses reveal the security and privacy practices of these companies and discuss the wide range of technology integration in new vehicles, data collection and management practices, and security measures to protect against malicious use of these technologies and data. The key findings from these responses are:

1. Nearly 100% of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.
2. Most automobile manufacturers were unaware of or unable to report on past hacking incidents.
3. Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers, and many manufacturers did not seem to understand the questions posed by Senator Markey.
4. Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.
5. Automobile manufacturers collect large amounts of data on driving history and vehicle performance.
6. A majority of automakers offer technologies that collect and wirelessly transmit driving history data to data centers, including third-party data centers, and most do not describe effective means to secure the data.
7. Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" and usually involving third parties, and retention policies – how long they store information about drivers – vary considerably among manufacturers.
8. Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.

These findings reveal that there is a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information.

In response to the privacy concerns raised by Senator Markey and others, the two major coalitions of automobile manufacturers recently issued a voluntary set of privacy principles by which their members have agreed to abide. These principles send a meaningful message that automobile manufacturers are committed to protecting consumer privacy by ensuring transparency and choice, responsible use and security of data, and accountability. However, the impact of these principles depend in part on how the manufacturers interpret them, because (1) the specific ways that transparency

[1] http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy

will be achieved are unclear and may not be noticed by the consumer, e.g., text in the user manual, (2) the provisions regarding choice for the consumer only address data sharing and do not refer to data collection in the first place, and (3) the guidelines for data use, security, and accountability largely leave these matters to the discretion of the manufacturers.

The alarmingly inconsistent and incomplete state of industry security and privacy practices, along with the voluntary principles put forward by industry, raises a need for the National Highway Traffic Safety Administration (NHTSA), in consultation with the Federal Trade Commission (FTC) on privacy issues, to promulgate new standards that will protect the data, security and privacy of drivers in the modern age of increasingly connected vehicles. Such standards should:

- Ensure that vehicles with wireless access points and data-collecting features are protected against hacking events and security breaches;
- Validate security systems using penetration testing;
- Include measures to respond real-time to hacking events;
- Require that drivers are made explicitly aware of data collection, transmission, and use;
- Ensure that drivers are given the option to opt out of data collection and transfer of driver information to off-board storage;

Require removal of personally identifiable information prior to transmission, when possible and upon consumer request.

INTRODUCTION AND METHODOLOGY

Today's cars and light trucks contain more than 50 separate electronic control units (ECUs), connected through a controller area network (CAN) or other network (such as Local Interconnect Networks or Flexray). Vehicle functionality, safety, and privacy all depend on the functions of these small computers, as well as their ability to communicate with one another. They also have the ability to record vehicle data to analyze and improve performance. On-board navigation technologies as well as the ability to integrate mobile devices with vehicle-based technologies have also fundamentally altered the manner in which drivers and the vehicles themselves can communicate during the vehicles' operation.

This new technology has also resulted in an increased ability to gather driving information. Such information-gathering abilities can be used by automobile manufacturers to provide customized service and improve customer experiences, but in the wrong hands such information could also be used maliciously. In particular, wireless technologies create vulnerabilities to hacking attacks that could be used to invade a user's privacy or modify the operation of a vehicle. Two recent developments highlight potential threats to both automobile security and to consumer privacy.

In a 2013 study that was funded by the Defense Advanced Research Projects Agency (DARPA), two researchers demonstrated their ability to connect a laptop to two different vehicles' computer systems using a cable, send commands to different ECUs through the CAN, and thereby control the engine, brakes, steering and other critical vehicle components.[2] In their initial tests with a laptop and two MY2010 vehicles from different manufacturers, they were able to cause cars to suddenly accelerate, turn, kill the brakes, activate the horn, control the headlights, and modify the speedometer and gas gauge readings.[3] More recently in 2014, those same researchers looked into the hackability of 21 different vehicle models from 10 different manufacturers, pointing out different levels of security in each vehicle with respect to wireless entry points, control points, and the types of computers than could be compromised.[4]

Before the researchers went public with their 2013 findings, they shared the results with the manufacturers in the hopes that the companies would address the identified vulnerabilities. But in response to the public release of the study, both companies reportedly noted that the researchers directly, rather than wirelessly, accessed the vehicles' computer systems, and referred to the need to prevent remote hacking from a wireless device. What the companies failed to note is that the DARPA study built on prior research that demonstrated that one could remotely and wirelessly access a vehicle's CAN bus through Bluetooth connections, OnStar systems, malware in a synced Android smartphone, or a malicious file on a CD in the stereo.[5]

A second, related area of concern relates to the increasing use of navigation or other technologies that could be used to record the location or driving history of those using them. A number of new services have emerged that permit the collection of a wide range of user data, providing valuable information not just to improve vehicle performance, but also potentially for commercial and law enforcement purposes.[6] This concern was highlighted when it was revealed that Tesla Motors recorded data during a test drive of one of its vehicles by a reporter and used data related to the driver's location, energy usage, speed, temperature and other control settings to rebut the reporter's unfavorable review of

[2] "Adventures in Automotive Networks and Control Units," Dr. Charlie Miller and Chris Valasek, http://illmatics.com/car_hacking.pdf

[3] http://www.npr.org/blogs/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves

[4] "Black Hat 2014: Hacking the Smart Car," Mark Anderson, IEEE Spectrum, http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smart-car

[5] See "Researchers Show How a Car's Electronics Can Be Taken Over Remotely," John Markoff, The New York Times, March 9, 2011, http://www.nytimes.com/2011/03/10/business/10hack.html http://www.autosec.org/pubs/cars-oakland2010.pdf and http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[6] "Dash is Turning Cars into Futurists, Data-Collecting Machines with an App and a Cheap Plastic Dongle", Alyson Shontell, Business Insider, http://www.businessinsider.com/a-tiny-piece-of-hardware-turns-your-vehicle-into-a-smart-car-that-talks-and-collect-tons-of-data-2013-8

his driving experience.[7] Car dealerships and navigation systems providers have also begun to use "remote disabling", which enable them to track and disable vehicles if drivers do not keep up with their payments[8] or if cars have been reported as stolen, which can raise safety concerns if the vehicles are disabled during an emergency or when the driver is left stranded in an unsafe location.

Furthermore, vehicle-to-vehicle (V2V) technologies are emerging as a viable tool for improving active safety through collision avoidance, and one of the main unknowns in their development is a robust communication security system.[9] As vehicles continue to become more integrated with wireless technology, there are more avenues through which a hacker could introduce malicious code, and more avenues through which a driver's basic right to privacy could be compromised. These threats demonstrate the need for robust vehicle security policies to ensure the safety and privacy of our nation's drivers.

In order to better understand the ability of automobile companies to protect the safety and privacy of drivers, letters were sent to 20 major automobile manufacturers with questions regarding technology, security precautions, and privacy policies. The questions posed were identical for each manufacturer. Responses were received from 16 manufacturers. Tesla Motors, Aston Martin, and Lamborghini, did not respond to the letters. Volkswagen and Audi responded with a single letter and are together treated in the findings as a single responding manufacturer. Some manufacturers (notably Hyundai and Toyota) provided detailed, question-by-question responses, while others (notably Mercedes-Benz and Porsche) wrote generic statements on their commitments to security and privacy that were non-responsive to the questions that were posed.

Recently, and as a result of the questions posed by Senator Markey, the automobile industry has acknowledged the deficiencies and inconsistences between manufacturers in existing practices for vehicle privacy protections by issuing its own set of voluntary privacy principles.[10] These voluntary principles were developed and supported by the Alliance of Automobile Manufacturers and the Association of Global Automakers, which combined represent 23 major automobile manufacturers, including all of the manufacturers that responded to Senator Markey with the exception of Audi. The adopted principles include (1) transparency, (2) choice, (3) respect for context, (4) data minimization, de-identification and retention, (5) data security, (6) integrity and access, and (7) accountability. The establishment of these principles, and the agreement to them by 19 manufacturers (including all of those that responded to Senator Markey's letter with the exception of Jaguar Land Rover), represent an important step forward by the automotive industry.

Through the voluntary principles, the automakers assure consumers that they will be informed when data collection occurs and given choices regarding whether their information can be used for marketing purposes, companies will not pass on any information to law enforcement without a warrant or court order, and "reasonable" security measures will be in place to protect data from falling into the wrong hands. However, the principles continue to raise a number of questions regarding how car manufacturers will effectively make their practices transparent to consumers and provide consumers with rights to prevent sensitive data collection in the first place, among other concerns.

The diversity of responses received by Senator Markey shows that each manufacturer is handling the introduction of new technology in very different ways, and for the most part these actions are insufficient to ensure security and privacy for vehicle consumers. Individual automaker responses will not be publicly released due to the proprietary and security-sensitive nature of some of the responses. The following sections summarize the major findings from the analysis of responses conducted by Senator Markey's staff.

[7] See "Elon Musk's Data Doesn't Back Up His Claims of New York Times Fakery", Rebecca Greenfield, The Atlantic Wire, http://www.theatlanticwire.com/technology/2013/02/elon-musks-data-doesnt-back-his-claims-new-york-times-fakery/62149/ and http://www.teslamotors.com/blog/most-peculiar-test-drive

[8] "Late on a Car Loan? Meet the Disabler", Jonathan Welsh, The Wall Street Journal, http://online.wsj.com/article/SB123794137545832713.html,

[9] Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist", Government Accountability Office, GAO-14-13, http://www.gao.gov/assets/660/658709.pdf

[10] "Consumer Privacy Protection Principles, Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., November 12, 2014, http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163

FINDINGS

Finding #1: Nearly 100% of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.

Wireless technologies in vehicles are becoming more prevalent as manufacturers have found ways that they can be used to improve safety, performance, and the driver experience. However, wireless technologies also require wireless entry points (WEPs), or ways that vehicle electronics can be accessed remotely. In 2011 a group of researchers showed WEPs in automobiles pose vulnerabilities, and they were able to remotely hack into a vehicle and exploit these vulnerabilities, including engaging in location tracking and eavesdropping, and controlling different features including the locks and brakes.[11]

Of the 16 manufacturers that responded to the letter, 14 provided information on the percentage of model year (MY) 2013 vehicles and the projected percentage of MY 2014 vehicles that have WEPs. Of the 14, 11 indicated that 100% of their vehicles have WEPs, and some of these manufacturers cited the federal mandate for tire pressure monitoring systems (TPMS) as a major contributor. Of the 3 who did not indicate that all vehicles have WEPs, the reported percentages of vehicles without WEPs were low, ranging from 7% to 30% and either stagnant or decreasing from 2013 to 2014.

These responses show that nearly all vehicles on the road have at least one WEP, and many vehicles have several WEPs. These include but may not be limited to TPMS, Bluetooth, keyless entry, remote start, navigation, Wi-Fi, cellular/telematics, radio, and anti-theft systems and features.

Finding #2: Most automobile manufacturers were unaware of or unable to report on past hacking incidents.

Senator Markey asked each of the manufacturers to list and describe instances in which they have been made aware of wireless or non-wireless infiltration events in their vehicles. Of the 16 manufacturers who responded to the letter, Jaguar Land Rover, Porsche, and Volkswagen did not respond to the question in any way. Of the 13 companies who did address the issue, 12 stated that they had no knowledge of any reported infiltration events, and only 1 reported such instances. This company described the following in detail:

- An application was developed by a third party and released for Android devices that could integrate with a vehicle through the Bluetooth connection. A security analysis did not indicate any ability to introduce malicious code or steal data, but the manufacturer had the app removed from the Google Play store as a precautionary measure.
- Some individuals have attempted to reprogram the onboard computers of vehicles to increase engine horsepower or torque through the use of "performance chips". Some of these devices plug into the mandated onboard diagnostic port or directly into the under-the-hood electronics system.

Finding #3: Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers, and many manufacturers did not seem to understand the questions posed by Senator Markey.

Manufacturers were asked how they assess their security against WEP infiltration, whether they use third-party testing to verify security, and how they handle software updates associated with recalls and service campaigns to ensure that these are done securely. The questions specifically asked about vulnerabilities associated with tire pressure monitoring systems, Bluetooth/wireless communications technologies, Onstar/navigation systems, smart phone/mobile device integration, web browsers, electronic control units (ECUs), and vehicle-to-vehicle communication technologies.

Of the 16 automobile manufacturers that responded to the letter, 13 of them addressed these questions in some way. Chrysler, Mercedes-Benz, and Mazda did not respond to the question at all, and five other manufacturers provided general responses that addressed the question as a whole instead of providing specific responses to the questions' sub-parts.

[11] "Researchers Show How a Car's Electronics Can Be Taken Over Remotely", John Markoff, The New York Times, March 9, 2011, http://www.nytimes.com/2011/03/10/business/10hack.html

This question seems to have been interpreted differently by different manufacturers. About half of the responses described security or encryption measures for general or specific WEPs that were more related to ensuring the WEPs were working as intended but not to ensuring that a security breach could not occur, and the other half mentioned procedures used in their development process to conduct targeted evaluations of their security measures. The responses revolving around security and encryption measures varied widely from manufacturer to manufacturer, and included the following:

1. Unique identification numbers and specific sets of radio-frequency signals;
2. Receptor to determine frequency strength of sensors to allow for proximity of legitimate communications;
3. Encrypted codes and dedicated wireless devices;
4. Encryption, masking, scanning, anomaly detection, certificates, filtering, firewalls, data loss prevention, access control, intrusion detection systems, white listing, fraud detection, zoning, network segregation and proprietary communication tools;
5. Closed systems where the implementations do not allow the ability for code to be written without authorized tools;
6. Secure Sockets Layer to encrypt the data of network connections;
7. Seed-key security to protect against unauthorized access to the ECU.

Automobile security experts consulted by Senator Markey's staff said that unique ID numbers and radio frequencies (responses 1, 2) can be identified by hackers, that closed system codes (responses 3, 5) have been proven to be re-writable, and seed-key security (response 7) is easily bypassed.

The other half of the responses named procedures utilized in the development process that manufacturers use to ensure WEP security, which was more in line with the wording and intent of the question. These responses included the following steps:

- Threat modeling;
- Penetration testing;
- Input validation and verification;
- Virtual testing;
- Component testing;
- Physical testing.

Seven of the manufacturers stated that they use third-party testing to verify their security measures, while 5 stated that they do not and 4 did not respond to this part of the question.

Automakers were also asked about the number of safety recalls and service campaigns issued by the manufacturers over the five-year period from 2009-2013 and whether those recalls or service campaigns involved software updates that could be used to introduce malware. Chrysler, Mercedes-Benz, Porsche, and Volkswagen did not respond, with the other 12 companies provided different levels of detail in their responses. The responses ranged from 27-210 combined recall or campaign events during that five-year period, with 11-44% of those including software updates of some kind, all of which were delivered using a hardwire connection (not over-the-air like some mobile phone updates are delivered) through a dealer or service center.

The manufacturers were also asked about how they secure this type of software delivery. Each manufacturer responded with descriptions of how they provide such software through authorized dealers with the appropriate tools. Automobile security experts consulted by Senator Markey's staff said that all of the responses are similar in that they presume a malicious actor could not access or acquire the technologies that mechanics have. They state that software updates for systems should be cryptographically verified by the ECU being updated in order to effectively prevent intrusions.

Finding #4: Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.

When asked about how manufacturers are capable of monitoring electronic systems in real-time in order to detect and respond to potential intrusions, most of the responses described systems that can only record information on-board the vehicle. This means that infiltrations would only come to the attention of the manufacturer if that data were manually downloaded by a dealer or service center at some subsequent date. When asked about how they would respond to an infiltration, most manufacturers did not respond or mentioned generic security systems in place. Only two manufacturers described credible real-time reactions to an intrusion event.

The manufacturers were asked whether they include technologies to monitor vehicle CAN buses

(the "controller area networks" that manage the communications among the different electronic systems in a vehicle) and to monitor WEPs. They were then asked about how they would respond to reports or detection of an unauthorized intrusion, a remote attack, or inadvertent introduction of malicious code to a WEP. Only eight of sixteen manufacturers responded to these questions, six of which claim to do CAN bus monitoring and five of which claim to be able to detect wireless intrusions. The other 2 manufacturers who responded to the question admitted that they do not monitor the CAN bus, but they are developing systems to do so. Of the other eight companies, Mercedes-Benz, Nissan, and Porsche did not respond at all, and five other manufacturers stated that such information was confidential.

The responses received varied in level of detail and in their methods of monitoring CAN buses. The six manufacturers who claim to monitor CAN buses cited the following:

1. One manufacturer claimed to have a proprietary system that cannot be disclosed;
2. Two manufacturers claimed that the electronic control unit (ECU) is equipped with; monitoring systems that can detect unusual signals, which would alert the manufacturer only if the data were later retrieved at a service center or dealership;
3. One manufacturer described a firewall and watchdog system that shields communication and recognizes inconsistencies at gateways;
4. One manufacturer listed message authentication, intrusion detection, controller hardening protection, secure diagnostics, secure gateways, and secure programming;
5. One manufacturer mentioned that seed-key security is applied to protect vehicles from unauthorized access, which generates a random security variable which must be matched in order to allow communication access.

Automobile security experts consulted by Senator Markey's staff noted that the ECU monitoring (response 2) and firewall/watchdog systems (response 3) would only check for unusual network behavior and not detect any problems with the data itself. An analogy was given to compare it to somebody receiving threatening phone calls, where the phone company is monitoring the lines to see if phone calls are getting through, but not checking the content of the conversations. They also noted that the seed-key system (response 5) could be bypassed by malicious actors.

The question of monitoring WEPs for intrusions received similar responses. Of the eight manufacturers that responded:

1. Four manufacturers mentioned that some of the features themselves are equipped with encryption and security technologies;
2. One manufacturer mentioned continuous ECU monitoring (also above);
3. One manufacturer described the firewall/watchdog system (also above);
4. One manufacturer described the seed-key security system (also above);
5. One manufacturer stated that its remote keyless entry systems can record key code authentication failures.

The encryption and security measures (response group 1) are not systems that can detect intrusion events. Automobile security experts consulted by Senator Markey's staff have noted that the ECU monitoring (response 2) described simply monitors the normal functioning of an ECU, the firewall/watchdog systems (response 3) would only protect against random outside influences like electromagnetic frequency interference and not malicious intrusions, the seed-key system (response 4) can be defeated by hackers, and the remote keyless entry systems (response 5) will only protect against people getting into the car to steal it but will do nothing to prevent or respond to remote hacking. Also, only 1 of the systems, the seed-key system, is capable of alerting the manufacturer in real-time.

Finally, on the question of how the manufacturers would respond to an intrusion in real-time, six of the manufacturers did not respond, and six more responded with vague mentions of security systems and "taking appropriate actions" such as recalls and service campaigns that could not be used to respond in real-time. The other four manufacturers provided the following responses:

1. One manufacturer claimed that it would contact the subscriber through the telematics program to alert them and resolve any problems;
2. One manufacturer said that it has the ability to disable certain connected features;
3. One manufacturer claimed that it could place a vehicle in a "fail-safe" mode that may limit vehicle operation if malfunctions that could cause damage occur;

4. One manufacturer stated that it would have the option to safely slowdown and immobilize an impacted vehicle if the vehicle is in motion at the time of detection.

The first 2 of these responses, contacting through the telematics program or disabling features, would not be an effective real-time way to deal with an ongoing attack, according to automobile security experts consulted by Senator Markey's staff. Responses 3 and 4, fail-safe mode and remote slowdown and immobilization, are the only responses that indicate an ability to immediately respond to security threats and address the situation for the drivers who subscribe to their telematics providers.

These three questions and their responses have revealed that, of the manufacturers who were willing to respond, only one of them appears to be able to detect wireless intrusions, and only one or two have described credible means of responding to such intrusions in real time.

Finding #5: Automobile manufacturers collect large amounts of data on driving history and vehicle performance.

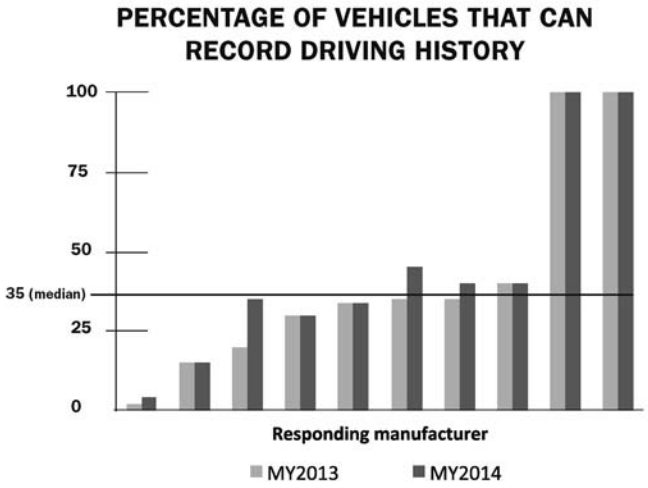
New vehicles are capable of collecting a tremendous amount of data through a variety of pre-installed technological systems. Senator Markey's letter asked manufacturers about (1) what types of navigation technology or other technologies are in their vehicles with the ability to collect driving history information, (2) what percentage of U.S. automobiles contain such technologies in MY2013 and MY2014, and (3) what types of information can be collected. Honda, Porsche, and Mercedes-Benz did not respond to these questions, and the other 13 manufacturers responded with various levels of completeness.

The responses to the first question included a range of navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems that have the ability to record driving history information. These included branded products like OnStar and SYNC as well as other unbranded technologies, collecting a diverse set of data types that included the following:

- Geographic location (7 manufacturers), such as:
- Physical location recorded at regular intervals;
- Previous destinations entered into navigation system;
- Last location parked.
- System settings for event data recorder (EDR) devices (5 manufacturers), which can include:
- Potential crash events, such as sudden changes in speed;
- Status of steering angle, brake application, seat belt use, and air bag deployment;
- Fault/error codes in electronic systems.
- Operational data (7 manufacturers), such as:
- Vehicle speed;
- Direction/heading of travel;
- Distances and times traveled;
- Average fuel economy/consumption;
- Status of power windows, doors, and locks;
- Tire pressure;
- Fuel level;
- Tachometer reading (engine RPM gauge);
- Odometer reading;
- Mileage since last oil change;
- Battery health;
- Coolant temperature;
- Engine status;
- Exterior temperature and pressure.

While three of the manufacturers who responded claimed to not record any driving history information, three others listed all three of the categories above.

The percentages of vehicles that contain such technologies varied greatly among the manufacturers, with some claiming that almost no vehicles have them while others claim that all of their vehicle models do. The percentages are shown in the chart below, with a median response of 35% of vehicles from a manufacturer containing technologies that can collect driving history information. These percentages either showed slight increases or stagnation from MY2013-MY2014.


PERCENTAGE OF VEHICLES THAT CAN RECORD DRIVING HISTORY
100
75
50
35 (median)
25
0
Responding manufacturer
MY2013
MY2014

The two coalitions of manufacturers recently adopted voluntary privacy principles—namely on "data minimization, de-identification, and retention" that attempt to address these concerns. On minimization, this principle states that manufacturers commit to collecting information "only as needed for legitimate business purposes". While this is a good step forward, limiting themselves to collection "only as needed for legitimate business purposes" still raises many questions about the extent to which companies will continue to collect sensitive information. The principles also do not ensure that consumers will have rights to prevent data collection in the first place.

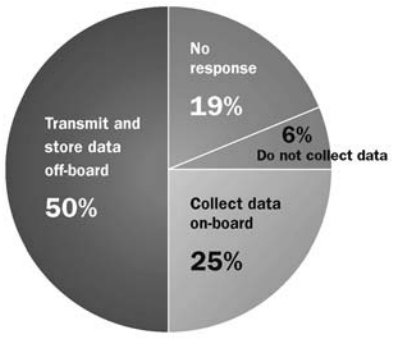
Finding #6: A majority of automakers offer technologies that collect and wirelessly transmit driving history data to data centers, including third-party data centers, and most do not describe effective means to secure the data.

Automobile manufacturers store data in a variety of different ways. Some said that it is only stored on-board the vehicle and cannot be wirelessly retrieved, and others described how they wirelessly transfer all data to a central location (known as off-board storage). Also, the large majority of the companies who responded (9 of 11) claimed that they do contract with third-party companies to provide the data-collecting features that they offer. In fact, 3 manufacturers specifically stated they license third party companies to transmit and store data associated with the features.

To the question of whether driving history information is recorded and stored in a vehicle, 12 manufacturers replied that they do store this information in some of their vehicles (depending on the features the vehicle is equipped with). Only 1 manufacturer stated that they do not collect such data, and 3 did not respond. This indicates that an overwhelming majority of vehicles collect driving history information.

Of the 12 who said they collect and store driving history data, 8 stated that they transmit and store driving history data in a server off-board the vehicle, while the other 4 stated that they do not. This reveals that a majority of vehicle manufacturers offer features that not only record but also transmit driving history wirelessly to themselves or to third parties.

PERCENTAGE OF AUTOMOBILE MANUFACTURERS THAT COLLECT AND TRANSMIT DRIVING HISTORY DATA



Finally, the security measures of these data collection systems vary widely by manufacturer, and in some cases there are none. In the case of on-board storage, no manufacturer described any security system to protect that data, and several of them noted that no security measure is needed since accessing data would require a hardwire connection. Regarding security measures to protect data that is wirelessly transmitted outside the vehicle, only 6 responses were received. Of those, 5 provided vague responses naming encryption, passwords, or general IT security practices, and only 1 specifically mentioned that they designed their systems to limit the transfer of personally identifiable information.

The automakers' voluntary privacy protection principles include commitments to "respect for context" and "data security". The "respect for context" principle addresses the ways that data are collected and shared, and it provides a list of examples to illustrate "reasonable and responsible ways" that automakers may collect and share data with both affiliated companies and non-affiliated entities. These include, among others, providing subscribed services, conducting research, responding to emergencies and faults, sharing for operational purposes, and complying with lawful government requests—describing a sweeping suite of practices and offering no specific guidelines for reducing data collection and sharing.

The "data security" principle states that the automakers commit to collecting information "only as needed for legitimate business purposes", which is another positive message toward reducing unneeded sharing of information. However, this principle offers no detail as to what may be included under "legitimate business purposes", effectively leaving it open for interpretation by the coalition members.

Finding #7: Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" and usually involving third parties, and retention policies—how long they store information about drivers—vary considerably among manufacturers.

A wide array of responses was received regarding the ways that manufacturers use vehicle history information. Of the 8 manufacturers that previously stated that they collect such information, 3 of them did not respond to this question, with the other five listing combinations of the following uses:

- Provide feature functionality;
- Maintain and improve services;
- Address vehicle safety concerns;
- Diagnose and assist with technical issues;
- Respond when the system senses the vehicle has been involved in an accident;
- Fulfill requests for service by customers;
- Research purposes (analytics and marketing).

Many of these responses are vague and not well-defined, such as providing feature functionality, maintaining and improving services, and serving research purposes. This lack of transparency in personal vehicle data usage leaves consumers with little knowledge about how the companies actually use their data.

Additionally, the letters revealed that 5 of the 8 manufacturers claimed to share this information with third parties to provide subscriber services. All of them stated that they do not sell such information, and 2 specifically mentioned that they do not share any personally identifiable information. This reveals that a majority of manufacturers who collect data share that information with third party companies.

Another question that received a wide range of responses was about how long driving history data is retained in the various systems that record and store them. To this question, four of the twelve manufacturers did not answer, with the other eight providing responses that sometimes varied by feature/technology. These ranged from responses that information is retained no longer than a year, to responses that indicate that information is retained indefinitely.

- Five manufacturers listed that information is deleted after a set period of time, ranging from one to ten years;
- Three manufacturers replied that there is no set clear date, with two of them stating that it can be deleted by users at any time;
- One manufacturer stated that navigation information is overwritten when the system runs out of memory storage space;
- One manufacturer said that on-board error information is deleted when the vehicle fault is cleared.

The new industry-led voluntary privacy principles include a commitment by automakers to only collect data "as needed for legitimate business purposes" and to retain identifiable or personal subscription

information "no longer than they determine necessary for legitimate business purposes". The intention of this principle is positive, but these limitations are subject to the interpretation of the industry and offer no explicit rules to prevent excessive collection or retention. Regarding the ways in which data are used, the coalitions put forth the "respect for context" principle, which describes a list of "reasonable and responsible ways" that members can use or share data collected from vehicles. This includes an important provision that a warrant or court order is needed if companies are to share geolocation information with law enforcement. Unfortunately, however, this broad proclamation provides little tangible assurances that consumers will not disapprove of the ways in which manufacturers use their sensitive information.

Additionally, the automakers' voluntary "choice" principle specifically requires affirmative consent from the consumer before sharing sensitive driving history data, specifically geolocation, biometric, and driver behavior information, for marketing purposes or with unaffiliated third parties. However, this commitment fails to address whether a consumer's decision to agree or disagree will affect the functionality of the vehicle or the features that are available to them. The principles also do not pertain to sharing (1) non-sensitive data for marketing purposes, and (2) sensitive data for non-marketing purposes.

Finding #8: Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.

The primary methods manufacturers use to inform customers of data collection are by mentioning it in the owners' manual or including it in the terms and conditions of the vehicle sale or specific feature activation. If a customer actually becomes aware of data collection and wishes to disable it, they often must accept a loss of feature functionality, such as GPS.

Of the twelve manufacturers who confirmed that they do record and store data, three did not respond to the question on how customers are made aware of data storage, and one stated that there is no reason to inform users of on-board storage. The other eight manufacturers listed combinations of the following methods of notice:

- Owners' manuals;
- Privacy statements;
- Terms & Conditions (which must be "accepted").

To the question of whether and how customers can disable data collection or transmission, four did not respond. Two manufacturers said that users cannot disable data collection, two said that they can disable it, and four stated that it is possible by turning off a feature or canceling a service subscription.

On the question of whether users (if they are made aware of data collection) can delete information, six manufacturers did not respond, five specifically noted that customers can delete data directly through the navigation system interface, and one mentioned that customers can request data deletion by contacting the service provider.

These responses show that customer awareness of data collection is primarily distributed within long written texts such as Terms & Agreement statements or owner manuals. In the event that customers read these and are aware of them, they do, in certain cases, have the ability to delete previously-recorded data. However, disabling the constant collection of data often requires disabling valuable vehicle features or services.

The new voluntary privacy principles from the manufacturers partially address these concerns with commitments to "transparency" and "choice". Signing members agree to provide consumers "with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing" of data. This includes a list of ways that manufacturers can provide these notices, which include "owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays". Unfortunately, these types of notices likely do not guarantee an improvement over current practices revealed in the responses to Senator Markey, as most manufacturers claimed that such notices are already provided in user manuals and terms & conditions that must be signed upon purchase.

Regarding choice, the principle states that consumers must give "affirmative consent", or opt in, when certain information such as geolocation, biometrics, or driver behavior is collected or shared for marketing or with unaffiliated third parties. The principle does not commit manufacturers to offering consumers the option to prevent data collection in the first place or giving consumers the choice to remove data that have already been collected. Additionally, consumers who choose not to consent to data collection may be denied access to valuable vehicle features. For instance, consent to sharing geolocation information for marketing purposes may be the only way for a consumer to turn on the navigation feature.

Senator MARKEY. I asked 20 automakers what they are doing to protect these computers on wheels, and what I found is that they are not doing enough. Cars today are highly connected. Every new car has some wireless technologies built into it. The problem is that there are massive holes in how car companies are securing these features against hackers. Only two of the 16 car companies who responded have developed any capability to detect and respond to a hacking attack in real time. Thieves no longer need a crowbar to break into your car. They just need a smart phone. And they can do much worse than open the doors. It is possible for wireless hackers to honk the horn, control the steering, and even cut the brakes.

Today's cars are also collecting tremendous amounts of personal driving information. Cars know where you are, where you have been, how fast or slow you drive, and even the mileage since your last oil change. This information can be used to help drivers find their destinations, get more miles per gallon, and drive more safely. But it can also jeopardize the security and privacy of drivers, of families across our country because there are currently no rules of the road to protect driver privacy and security. There are currently no rules for how to protect this data as it is being gathered, and most customers do not even know that their information is being gathered as they drive and that that information is being sent to third parties who the drivers do not even know about.

And that is why in the coming weeks, I plan to introduce legislation that directs the National Highway Traffic Safety Administration and the Federal Trade Commission to establish Federal standards to secure our cars and protect our drivers' privacy. We need the electronic equivalent of seatbelts and airbags to keep drivers and their information safe. We have stickers on cars for safety. We have stickers on cars for fuel economy standards. Well, we need a new set of minimum standards to protect driver security and privacy in new vehicles that the customer will know that the company built into that car or did not build in. If they want a zero on the sticker, they can have a zero. They can say it is too expensive. They can use the same argument the auto industry used in this committee opposing seatbelts and airbags, saying it is too expensive for the auto industry. They can make that argument, but there will be a zero on the dashboard so that people can see it.

These security performance standards should include a requirement that all wireless access points in the car are protected against hacking attacks, evaluated using penetration testing, requirements that all collected information is appropriately secured and encrypted to prevent unwanted access, and a requirement that the manufacturers or third party feature provider be able to detect, report, and respond to real-time hacking events.

And the privacy standards should include transparency requirements so drivers are made explicitly aware of data collection, transmission, and use of driving information; consumer control over that data; and a prohibition on the use of the personal driving information for advertising or marketing purposes unless you get permission from the driver.

New cars will also be evaluated by a rating system, a cyber dashboard that informs customers about how well the vehicle protects drivers beyond those minimum standards. This information will be

displayed on the label of all new vehicles just as fuel economy is today.

Mr. Brookman, do you believe that every car should be protected against hackers who can remotely access and take control of your car?

Mr. BROOKMAN. Yes.

Senator MARKEY. If a car does get hacked, Mr. Brookman, do you think it would be good for there to be a system to detect and alert the automaker or authorities that something is happening?

Mr. BROOKMAN. I do.

Senator MARKEY. Do you believe customers should be made aware of the personal information their car is collecting about them?

Mr. BROOKMAN. Absolutely.

Senator MARKEY. Do you think that drivers should be given control over their personal information and be allowed to choose whether the data is collected about them or sold to third parties?

Mr. BROOKMAN. In most cases, yes.

Senator MARKEY. Do you believe that car companies should be allowed to sell an owner-sensitive driving history to insurance companies, data brokers, or anyone else?

Mr. BROOKMAN. The consumers could obviously consent to that, as they do today, but absent user control, no.

Senator MARKEY. Thank you.

So that is the point. A software that can be built in that makes all these wonderful things possible by companies should have the same geniuses in those companies with the capability to build in a protection for security and privacy. All of a sudden, they cannot figure out how to do that? All of a sudden, they cannot figure out how to protect the consumer, their privacy, their security? No. If you can figure out an algorithm that sends information around the world in a blink of an eye, you should be able to figure out an algorithm that also provides consumers with the privacy and security which they need as they are driving their vehicles.

I thank you, and I yield back the balance of my time.

Senator CANTWELL. I am not sure there is any balance left. But thank you.

[Laughter.]

Senator MARKEY. I am talking to the ether here.

Senator KLOBUCHAR. That was a very generous offer.

[Laughter.]

Senator MARKEY. Thank you.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you.

Well, gentlemen, I want to maybe come with a little bit broader perspective. And I apologize too. We were in a Finance markup.

One, I want to hear about some of the applications that you think might actually financially benefit consumers in the future. I mean, obviously, one of the issues here is, you know, you go to the grocery store, the soup deli, and you get a little punch. You buy so many soups or so many coffees. You get a reward. So what is the

reward going to be here? What are the applications for loyalty or sharing non-personal data that might benefit consumers?

Second, we are talking about applications for privacy today on these devices just as we did for banking and health care and other applications 15–20 years ago. So are we going to continue to go by device, by sector on privacy laws, or do you think we will get to a point where we need a brighter Larry Lessig kind of privacy right issue? Do you see that happening?

And third, if you could comment on the importance of net neutrality and the open Internet for keeping the application and device economy going? Mr. Abbott?

Mr. ABBOTT. Sure. I will begin. Thank you, Senator.

So on your first topic, in terms of an example, I think one clear benefit in one scenario is around thermostats and energy conservation in the home, saving both cost to the consumer in terms of the money spent on heating his or her home. And oftentimes there are examples where the tuning of that algorithm for heating your home on and off when you are away is actually built from a population of users. So you are looking at personalization but driven off a population that is de-identified. It is really, really important.

Senator CANTWELL. I think now because so many people look at what is happening now in the identifiers or, like you were talking about, precision agriculture and the data that has been mined by the big companies, what individual consumers want to know—I am a big hiker. I want to know, OK, I will tell everybody I am a big hiker, but then I want you, if you are going to be sending me these ads, whether it is REI or someone else—I want a discount because I told you that. Because what is happening now is everybody is figuring that out by somebody else's mechanism and making benefit off of that. But I am saying I am willing to share some of that, but I want to know what my discount is going to be as part of that process and if there are applications out there that are like that.

So I get the energy thing, and it is very, very important. But I guess I am thinking a more up-front dialogue with the consumer about this data.

Mr. ABBOTT. I think, Senator, we talked a couple times before around the transparency need in this environment, and I think that is particularly important because people immediately oftentimes, when they think of data sharing, they are thinking immediately of advertising. And in those cases, at least my view is that user should be able to opt out based on a very clear communication of how that data is being used.

In the same case, that user may opt out of sharing that data around their thermostat in their home as well, but I would imagine a lot of consumers, if they understand the benefit of sharing, let us say, that data for their usage, we tend to believe that that actually will be collectively in the best interest of the consumer.

On the second question you had, in terms of sectors, we certainly see that there is going to be likely policies around privacy that vary by the use case. So certainly very different in medical with, let us say, HIPAA compliance versus, let us say, the Internet of Things of watering a lawn and actually addressing, let us say, outdoor landscape issues.

Mr. DAVIS. Thank you, Senator. I think a great set of questions.

We have seen so many examples over the past 12 to 18 months of companies delivering either significant economic value or new products and services as a result of the Internet of Things. You know, you are asking for examples that are close to consumers. You see companies that are taking smart city information, so traffic information, air quality information, and combining it with the availability of open parking spaces. And those cities then are starting to look at ways in which they can alter traffic flows during certain times of the day, making that information available to us as consumers to say I am not going to circle the block three times to find a parking space. I am going to go where I know no one is currently available. So I think there are a number of instances we are already starting to see that will see benefit in addition to productivity and greater efficiency in how the infrastructure around this operates.

I would agree with Mr. Abbott. I think from a privacy perspective, we are going to see differences by market sector. There may be some areas again around city infrastructure where we as consumers want to be able to have rich access to data, and as that innovation evolves, it will offer new products and services contrasted against health care or financial services kinds of industry.

And then on your last point, I think we have seen the cost of connectivity come down about 40X in the past 10 years, and that is even without considering some of the new technologies that are moving into the network infrastructure today that I think will dramatically transform it over the next 10 years. That availability of connectivity cost effectively is an essential tenet to the Internet of Things.

Senator CANTWELL. Thank you.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Blumenthal?

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Mr. Chairman, and thank you for having this hearing on this profoundly important topic.

I have been in and out, and I apologize. I have not heard all the testimony.

But I am very interested in the security issues, some of them raised by Senator Markey so far as automobiles are concerned, and I feel those same potential security threats exist with regard to a wide variety of devices and appliances that Americans use every day. And we have heard a lot about the coming wave of connected devices. The FTC report estimates that there will be 25 billion connected devices by the end of the year and 50 billion by the end of 2020. And each of them presents a potential attack surface for hackers and thieves. Essentially as every one of us brings a new device into our home, we create a vulnerability to those hackers and thieves to use portals that cyber criminals can attempt to access for very sensitive and confidential information.

So let me begin by asking Mr. Brookman, right now, the majority of devices have no encryption. 70 percent of these devices have no encryption on communications. The average is, I think, 60 percent

have insecure Web interfaces and 60 percent have insecure software. What is the answer?

Senator Markey very eloquently indicated that if we can do the algorithms that send messages around the world, we can have algorithms that protect us. And it is not just automobiles but every one of these devices. Is encryption the answer? What would you advise? And I will open the same question to the others.

Mr. BROOKMAN. It is a really important question. It is a hard question.

I think what Congress can do is I think they can pass an affirmative data security requirement law. Already the Federal Trade Commission thinks they can enforce reasonable security requirements on companies under section 5. That authority is being attacked in court by a few companies. I know Wyndham Hotels is challenging the FTC. FTC says the unfairness law requires you to use reasonable security. Wyndham Hotels says no. It actually does not. So having that written down in law I think would be useful.

I think having a process requirement for companies that collect this sort of information should have to think about in advance. I think institutions and people in general are really bad at considering the very small chance of a very bad thing happening. So having a process in place to think about that I think would be really good because right now security is often thought of as a cost. I am not going to get any profit from it. But when it goes bad, it goes really bad.

I also think we probably need better breach notification laws. You know, 47 states have it covering financial information. I think we should expand those laws to include online accounts like things that were compromised in the iCloud incident, in the Sony incident. This is personal information that people care a lot about. Internet of Things devices reveal really sensitive stuff about us, and if my Smart TV there has a camera and the microphone and my Samsung account gets compromised, I want to know about it. Because there are websites you can go to now where you can find thousands and thousands, like 100,000 different webcams you can find online. Just watch the live feed. Right? And I think if a company knows they get compromised, they have an obligation to tell you about it.

Senator BLUMENTHAL. And notification is kind of a basic minimum common denominator of what all of us should favor. If somebody knows about a breach, there ought to be notification to the person who is threatened by it.

Mr. BROOKMAN. Absolutely, but I think that level of notification, like if your e-mail account gets breached, is only required—I think notification is only required in two states today, Florida and California.

Senator BLUMENTHAL. And imposing the costs of a breach on the one responsible, the one who can do something about it, also seems pretty basic.

Mr. BROOKMAN. Yes, absolutely. I think that has been an incredibly important thing for credit card fraud. It is not the consumers who bear the cost of that. It is actually split between the merchants and the banks. And I think because of that, they have really strong incentives to get security right.

Senator BLUMENTHAL. Any of the other members of the panel?

Mr. THIERER. Senator, briefly on the concerns you have raised about security and those raised by Senator Markey as well. Let us keep in mind a couple of general things.

First and foremost, no consumer is going to want to buy or use a device, especially a car, that is fundamentally insecure.

Second of all, if firms do sell these sorts of devices that are fundamentally insecure to the public, class action lawsuits will fly and State AG's will be very active, as you know.

Senator BLUMENTHAL. We are going to have to have a law on which to sue.

Mr. THIERER. There are consumer protection laws already on these things, and of course, there are other general torts——

Senator BLUMENTHAL. And that goes back to Mr. Brookman's point about establishing some legal standard that provides a cause of action.

Mr. THIERER. But firms are already being sued under existing causes of action, and firms understand that they are never going to make any money if they sell devices that are fundamentally insecure and do not protect——

Senator BLUMENTHAL. If consumers know, number one, and number two, if they can make informed decisions among products that actually offer this kind of protection. The fact that protection is offered as one of the features of a device or automobile or appliance may not be decisive for a consumer who is looking at a bunch of other features and colors and attractions that may be part of the vehicle.

Any other members of the panel?

[No response.]

Senator BLUMENTHAL. Thank you.

The CHAIRMAN. Thank you, Senator Blumenthal.

I think we are ready to wrap it up. I have got a couple of letters I would like to put in the record, one from the Consumer Electronics Association, the other from the Telecommunications Industry Association and their report on this subject, the Internet of Things.

[The information referred to follows:]

CONSUMER ELECTRONICS ASSOCIATION
Arlington, VA, February 10, 2015

Chairman JOHN THUNE and Ranking Member BILL NELSON,
U.S. Senate Committee on Commerce, Science, and Transportation
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

On behalf of the Consumer Electronics Association (CEA)® please accept our views on the role of government and industry in the next shift in innovation, the Internet of a Things (IoT).

CEA is the trade association representing the $223 billion U.S. consumer technology industry. Every day, our more than 2,000 member companies are busy innovating; introducing extraordinary products and services and creating American jobs. At CEA, we work to advance government policies that encourage innovation and job and business creation.

CEA members are driving the growth of the IoT. Over 900 exhibitors displayed IoT devices at the 2015 International CES. The convergence of connected devices, cloud computing services, and powerful data analytics will help drive near to mid-term economic growth.

While businesses have been using connected devices, the IoT is new to the consumer market. Consumers are realizing its benefits, and our interactions with these devices will become so routine that they will go almost unnoticed. The IoT has profound potential to improve the lives of our citizens. Within a few years, Americans will be able to connect with their doctors remotely, share their health data and information and better manage their diseases. Home automation systems will enable consumers to manage their security systems, turn on appliances, and maximize their home's energy efficiency, all from a smart phone. Connected cars will eventually avoid collisions, but before then will notify first responders of an accident immediately, saving time and lives.

As this transition takes place, manufacturers and service providers will be focused on making good decisions about the privacy and security of information that devices collect and share. It is not only important to their customers; it is vital for them as well, because consumer adoption hinges on building trust. Devices that do not meet consumer privacy and security expectations will fail.

Along with the new capabilities that emerging technologies create also come questions about how to best protect users and promote consumer practices. CEA and others are exploring these issues and how best to ensure consumer privacy and security while enabling new technologies to develop. We believe that industry-driven solutions are the best way to promote innovation while protecting consumers.

We are just beginning to understand the benefits and challenges of the IoT. In this dynamic and rapidly changing environment, governments should exercise regulatory restraint. Overly prescriptive mandates or technologically biased standards will stymie growth and become outdated. If governments must act, such actions should be narrowly tailored to address tangible harms without creating roadblocks for future innovation.

Please recognize that the evolution of *things* comprise only part of the value of the entire IoT ecosystem. Analytics software extracts value and finds useful patterns in data collected by IoT devices. Data analytics are a vital tool in understanding consumers' needs and uses for products and allow companies to both improve current products and create new ones that meet consumers' needs and desires. The Internet runs on data. Restrictions on data collection may hurt new services which provide personal and societal benefits. We ask policymakers to tread carefully as they explore the potential and growth of the IoT.

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

Sincerely,

GARY SHAPIRO,
President and CEO.

CC: Members of the U.S. Senate Committee on Commerce, Science, and Transportation

---

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Arlington, VA, February 11, 2015

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Hon. BILL NELSON,
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

The Telecommunications Industry Association (TIA), the leading trade association for global manufacturers, vendors, and suppliers of information and communications technology (ICT), writes to communicate our support for your holding of a hearing this week to examine how devices will be made smarter and more dynamic through Internet technologies, and related policy implications. TIA and its member companies believes that this increasingly connected world—commonly referred to as an "Internet of Things" (IoT)—holds immense promise for investment and innovation that will translate to wide societal benefit and improvements in countless aspects of American consumers' everyday lives.

At its most basic, the IoT is a label for an increasingly connected future in which regular, everyday items—from household appliances to cars to medical devices—are

outfitted with sensors and connected to the Internet to share their data. Viewed more broadly, the Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. In this new world, most communications will be machine-to-machine (M2M), and there will be a continuous exchange of information between devices, sensors, computers, and networks.

While the potential for benefits in an IoT world are widely recognized, there are a number of horizontal policy issues that impact the IoT across markets and use cases, such as interoperability, privacy, security, and spectrum availability, among others. With these common threads running across IoT applications and use cases, a significant danger exists that vertical regulations imposed in one market will be inappropriate for another, which could lead to a balkanized regulatory approach, stifling innovation and delaying or degrading the economic and social potential of the IoT. To avoid this scenario, IoT policy discussions should begin with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications only as necessary.

TIA has developed *Realizing the Potential of the Internet of Things: Recommendations to Policy Makers,* a white paper offering a general framework for these IoT policy discussions, which is appended to this letter. The recommendations in this white paper are applicable across market sectors, and will help ensure that the full economic, societal, and technological potential of the Internet of Things is ultimately realized. In your February 11, 2015, hearing, we urge you and other members of the Senate Committee on Commerce, Science, and Transportation to consider the industry consensus recommendations in this white paper, which include:

- *Ensure Competitive-and Technology-Neutrality:* The IoT will be driven by the convergence of exponentially-increasing availability of connected devices in both the public and private spheres, across markets. The ICT industry is continuing to work towards realizing this continuum of connectivity, and we urge policymakers to ensure a competitive-and technology-neutral approach is taken to any activity that may impact the deployment of the IoT.
- *The Role of Global, Open, Voluntary, and Consensus-Based Standards:* We urge for recognition of the importance of the use of global voluntary, open, and consensus-based standards in the IoT which will drive interoperability. These standards are under development in a number of fora, including TIA, with adoption being mainly driven through competition. Reliance on these standardization efforts ensures that scientific expertise from implementers in the private and public sectors is reflected in approaches to the IoT. TIA further strongly encourages recognition of the global consensus that "open" standards are market-driven and allow for the inclusion of patented technologies, which are addressed through the use of fair, reasonable, and non-discriminatory patent policies.
- *A Spectrum Policy that Enables the IoT:* For the IoT to succeed, the United States must employ a spectrum policy that enables the wide range of products and services falling under this concept. Such a spectrum policy prioritizes predictability, flexibility, efficiency, and priority for superior rights from harmful interference. Reallocation and sharing efforts in the United States are crucial to the IoT's success, and will also serve as a helpful use case for regulators around the globe.
- *Utilize a Voluntary, Flexible, and Collaborative Approach to Data Security Based on International Standards:* When addressing data security and resilience, TIA urges for policymakers to ensure respect for competitive differentiation as a primary driver of enhanced security solutions, rely on international standards and best practices, fully leverage the public-private partnership model, and to prioritize end-user awareness and education.
- *Ensure Feasibility and Flexibility in Addressing Data Privacy:* The ICT industry prioritizes data privacy, and policymakers should ensure that their activities are technically feasible and do not impose barriers that would discourage the use of existing and developing voluntary solutions that typically emerge from standardization and best practice development fora, as well as public-private partnerships. Further, government should partner with the industry on efforts to ensure informed uses of products and services by consumers.

Thank you for your work to realize the potential of the IoT, and TIA looks forward to working with you moving forward. For more information, please contact Danielle Coffey at (703)-907–7734 or by e-mail at dcoffey@tiaonline.org.

Sincerely,

SCOTT BELCHER,
President,
Telecommunications Industry Association.

Attached: TIA's *Realizing the Potential of the Internet of Things: Recommendations to Policy Makers*

ATTACHMENT

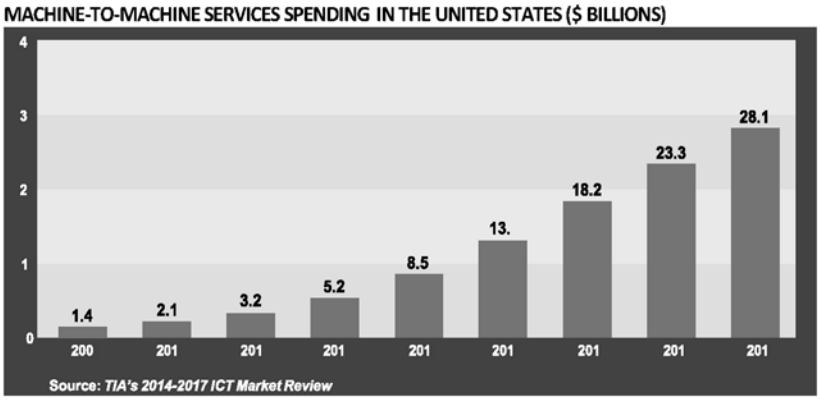
REALIZING THE POTENTIAL OF THE INTERNET OF THINGS

Recommendations to Policy Makers

The Internet of Things (IoT)—the term that has come to represent an envisioned ecosystem of interconnected objects, people, systems, and information assets working in concert with intelligent services to allow them to process information of the physical and the virtual world and react—represents an enormous market segment for information and communications technology (ICT) manufacturers, vendors, and suppliers that promises great societal benefit. Across segments impacted by the IoT, policymakers are becoming increasingly interested in the impact of the IoT as laws and regulations attempt to keep pace with innovation. Below, the Telecommunications Industry Association (TIA) provides an overview of the IoT's potential benefits and key recommendations for policymakers that the ICT industry believes will ensure the realization of the full benefits of the IoT.

The Potential for the Internet of Things

The "Internet of Things" is a broad label for the idea of an increasingly connected future where regular, everyday items will be fitted with sensors and the ability to connect to networks and transmit data. Machine-to-machine (M2M) communications is a networking term that describes the technology that enables devices to communicate with each other. M2M is the key to the IoT because it encompasses the technologies that are necessary to enable a successful IoT environment. In the new M2M-driven world, there will be a continuous exchange of information between sensors attached to connected, everyday items or infrastructure, computers, and the networks. For the future, to work as envisioned, the IoT must be designed to handle the transmission, receipt, and processing of exponential amounts of data.



The penetration of Internet adoption, faster mobile connections, and the availability of advanced computing capability in the form of cheaper, smaller devices with significant processing power has facilitated the growth of the IoT. The key element driving this market is the ability to install inexpensive sensors in machines and devices due to advances in sensor technology that have dramatically reduced the cost, and may rely on geo-location technology, RFID, and many other technologies. The increased availability of low-cost sensors will expand the potential market for M2M, as cost issues in installing sensors in devices are not expected to be significant. These sensors collect real-time data and transmit it via the Internet

or wireless networks to computers, other machines, or to people. At the receiving end, application software converts data to useful information. This ability to collect and analyze significant amounts of data is the aspect of the IoT that will be truly transformative. With low-cost sensors allowing virtually any device to become M2M-capable, this new data-centric information, consumers and businesses can make decisions that are more efficient, allowing them to maximize time and cost.

In 2012, an estimated 8.7 billion things were connected worldwide and projections show that with the new technological capabilities this could grow to 50 billion by tehe year 2020,[1] generating global revenues $8.9 trillion by 2020.[2] TIA projects the IoT will provide significant impacts across service sectors, representing an emerging market that is both unique and enormous. IoT will have a transformative impact in a host of market sectors such as healthcare, transportation, and energy, manufacturing, defense, and emergency services, such as:

Recommendation: Policymakers' Approach to the Internet of Things Should Adhere to Competitive-and Technology-Neutrality Principles

As ICT manufacturers and vendors work to meet the needs of their customers, competition will ultimately determine which products and services succeed and fail in the market thereby fueling further innovation. As businesses increasingly make investments in the IoT, an utmost concern for policymakers should be to take a competitive-and technology-neutral approach that respects the need for specific sectors to utilize creative solutions, and for innovators to address the needs of market segments. Policy makers should be wary of taking any action that locks the market to a limited set of solutions when new innovations are constantly being rolled out, some of which cannot be predicted. No industry illustrates the need for flexibility and technology neutrality more than the dynamic ICT industry.

Policymakers should also avoid any situation that would put a government actor in a position to determine the future design and development of technology. To do otherwise would set a precedent of interference with the core innovation engine of the ICT sector, negatively impacting the interoperability and standards that are needed for IoT proliferation. Should a well-developed public policy case based on the consensus of stakeholders find that regulatory action by is needed, we strongly encourage policymakers to promote the competitive dynamic by adopting regulations that are outcome-based, allowing innovation to thrive while still achieving the regulatory requirement.

Recommendation: Policymakers Should Encourage and Leverage Voluntary, Open, and Consensus-Based Standards

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards. Ongoing and future standardization efforts that enable the success of the IoT will cut across market segments, and will range from overarching guidelines to specific technical criteria, ensuring increasing interoperability as well as backwards-compatibility. Importantly, these standards are able to dynamically adapt to needed changes based on the expertise across stakeholders. These standards also reduce costs because manufacturers and software developers can produce for multiple applications and multiple end uses allowing for the benefits of economies of scale. TIA expects the development of IoT to be driven by a global—not regional—approach that is based on the development of open, voluntary, and consensus-driven standards.

Numerous existing standardization efforts, as well as future efforts, to address industry-consensus needs, will define and contribute to the development of an interoperable IoT. TIA broadly supports the "multiple paths" approach to the development of international standards whereby healthy competition amongst the different efforts will result in market-driven solutions that provide customers with the best options. TIA houses such standardization efforts, such as its Engineering Committee TR–50 M2M (Smart Device Communications).[3] Another example of such standardization activities include oneM2M, an international partnership that is working to develop technical specifications which address the need for a common M2M Service

[1] *http://share.cisco.com/internet-of-things.html.*

[2] *http://www.idc.com/getdoc.jsp?containerId=prUS24366813.*

[3] Engineering Committee TR–50 M2M (Smart Device Communications) is responsible for the development and maintenance of access agnostic interface standards for the monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications or networks. These standards development efforts pertain to but are not limited to the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.

Layer that can be readily embedded within various hardware and software, among many others.

Standardization is a form of economic self-regulation that can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways. TIA urges policymakers to defer to these standards as they are developed and come to define the IoT. By taking this approach, policymakers can use these standards as valuable sources of scientific and technical information developed with the assistance of private sector experts, allowing for agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area.

Policymakers should avoid any approaches that would redefine "open standards" in a way that equates patented technology with "free" (as in without payment) or "free to use freely" (as in without payment and without any restrictions). These kinds of redefinitions would undermine the rights of those who have invested in the development of standardized technologies that enable the functioning of countless sectors of the economy. Technological capabilities and innovations most often result from substantial investments in research and development thus, if patent holders in standards-setting activities are expected to give away or waive their patent rights there are likely to be significant adverse results, including that technology leaders will reduce or cease participation in voluntary standards-related activities; or that individuals and organizations will not invest in the development of next-generation technology in the technical areas subject to standardization, creating innovation "dead zones" in those areas.

Recommendation: Policymakers Should Employ Regulatory Approval Approaches That Are Globally Harmonized, Transparent, and Streamlined

The ICT industry is one of the most far-reaching and competitive global ICT segments of the global economy. Across jurisdictions, the varying requirements that a ICT and presents unique challenges to ensuring governments, consumers, and other stakeholders in a diverse marketplace have the ability to readily determine whether a device has been properly certified, and to obtain additional information about a device as efficiently as possible. With the drastic increase in the amount of connected things in the IoT, it will be very important for policymakers to work to ensure that regulatory approval processes are transparent and efficient. We urge policymakers to methodically examine their regulatory device approval mechanisms to ensure that these systems are as globally-harmonized, predictable, transparent, and reliable as possible. This will promote the "build once, sell anywhere" principle which drastically reduces regulatory costs, time-to-market, and cost to end users throughout the business and consumer markets.

For example, policymakers are strongly urged to consider permitting the use of Supplier Declarations of Conformity (SDoCs) for trusted classes of products as an alternative means by which an ICT manufacturer may demonstrate compliance with regulatory rules to streamline the process ICT manufacturers must go through to get products to market. The benefits of such an allowance include flexibility and objective treatment for manufacturers in where to have their products tested, high compliance levels, and lower administrative costs. The appropriate allowance of SDoCs would also lend to the mutual recognition agreements (MRAs) among trading partners and widespread recognition of another country's conformity assessments, further reducing associated costs. Based on a long-standing record of compliance, many technologies have proven to hold very low risk exists for violating the technical rules primarily because they are built to meet consensus technical standards, allowing the policymakers to be assured that they can take this step to allow for more rapid availability of products into the marketplace at reduced cost to stakeholders, including consumers.

As a further example, the use of physical markings or labels have played a key role in providing this important information, but the continuous evolution of industrial design and multiple regulatory environments has led to increased costs and difficulty in ensuring all relevant markings or labels are affixed in an efficient and convenient manner for the user of the device. An effective solution to this problem is the non-exclusive use of electronic labeling, which allows consumers and other users access to easily readable and prominently displayed information about each device. This information should include required regulatory markings and other important information including proper device care, electronic recycling programs, and warranties. Already, through close work with TIA, several key jurisdictions have allowed this approach.

Recommendation: Utilize a Spectrum Policy that Maximizes a Continuity of Connectivity

The IoT will rely significantly upon maximizing *continuity of connectivity.* With the world rapidly becoming wireless, establishing an appropriate spectrum policy is therefore essential to ensure that the IoT will be successful. In commercial communications networks, mobile data use is exploding as consumers embrace smartphones, tablets and other devices. Wireless connectivity is becoming the way in which consumers access the Internet from technologies such as LTE, Wi-Fi and satellite. Governments worldwide also have a significant dependency on spectrum for both communications and non-communications purposes.

Meanwhile, radio technologies themselves are changing, placing new demands on spectrum allocations, and raising new operational and regulatory challenges. At the moment, there are several new or emerging technologies which are competing in the marketplace to serve the Internet of Things. These include Near Field Communication ("NFC"), a standards-based short-range wireless technology widely linked with mobile payments. More recently, Bluetooth Low Energy ("Bluetooth LE" or "BLE") has been built specifically to consume small amounts of energy; it is also viewed as a good candidate for small data packets sent from wearable computing such as smart watches and fitness trackers. Traditional Wi-Fi is also expected to play a key role due to its low cost and ubiquity in the marketplace. Indeed, the future Internet of Things will likely be based on *heterogeneous networks* whereby devices can sequentially or simultaneously use different network technologies.

As a result of these dynamic changes, spectrum allocations and uses that may have sufficed during the 20th century are increasingly under stress. Unfortunately, policymakers are no longer writing spectrum policy on a blank sheet of paper, and virtually all spectrum suitable for mobile service has been allocated. For that reason, TIA believes that any spectrum policy must reflect the following principles to allow the use of radio spectrum to evolve to meet changing demand and promote innovation:

- *Predictability.* Spectrum allocations need to be predictable. Identifying demand and changes in demand, understanding the pace of radio technology development by platform, and long term planning are all essential parts of a spectrum policy that can provide predictability for both commercial and government users.
- *Flexibility.* For commercial allocations, flexible use policies consistent with baseline technical rules that are technology-neutral have proven to be the best approach. Any government allocations of spectrum should be managed to ensure better usage of scarce spectrum resources for all users.
- *Efficiency.* Policies should encourage more efficient use of spectrum where technically and economically feasible. In particular, policies should prioritize *global harmonization* and coordination or spectrum allocations;[4] protection from harmful interference for licensed uses; adjacency to similar services; and allocations of wide, contiguous blocks of spectrum. Cleared, exclusively licensed spectrum allows for the most efficient and dependable use of spectrum for commercial mobile broadband deployment.
- *Priority.* In cases where spectrum sharing is technically and economically possible, policies must advance good engineering practice to best support an environment that protects those with superior spectrum rights from harmful interference.

Furthermore, spectrum sharing represents a means for increasing the efficient use of spectrum and to help alleviate challenges in spectrum scarcity, and could eventually prove critical towards enabling the *continuity of connectivity* that is so critical for the Internet of Things. In addition to ongoing efforts underway to realize successful sharing regimes, other promising efforts include the deployment of Authorized Shared Access (ASA)/Licensed Shared Access (LSA) approaches, a "third way" spectrum management system that combines elements of traditional "command and control" spectrum management with geolocation technology, *e.g.,* by providing users with a "token" to use spectrum at certain times/places. ASA/LSA approaches show great promise as they provide a means to ensure ongoing viability of incumbent uses by creating a policy environment that enables compatible operations with new uses while also providing secondary users a means to gain access

[4] Globally harmonized spectrum is essential to ensure the economies of scale that will facilitate the large-scale deployments necessary to fully utilize the promise of new technologies. Global harmonization also facilitates roaming, which is an important part of creating the "continuity of connectivity" required for the Internet of Things.

to spectrum that is already licensed to one or more primary users, but may be under-utilized or capable of supporting multiple uses.

IEEE P2413—group recently formed, designed to aggregate technical standards from various other IEEE efforts.

IEEE 802.3 working group (Ethernet)—two efforts to look at reduced twisted pair. High data rate, includes power for applications where batteries are difficult, lower cost vs. older 4-pair technologies (*e.g.,* Cat 5 cabling). This would be useful for industrial applications, deploying lots of parking space sensors, etc.—a smarter replacement for low-voltage wiring. There are two efforts underway—one using 100MHz, one using 1GHz—over single twisted pair.

Mesh networks—Zigbee isn't just used for home standards, but also industrial applications. There are also several other mesh network protocols that could/should be mentioned in the paper.

Recommendation: Utilize a Voluntary, Flexible, and Collaborative Approach to Data Security based on International Standards

With the IoT naturally involves an ever-increasing number of "things" being connected throughout society, new and evolving security issues will emerge as challenges. Already, ICT members consider security issues throughout the design process, and this approach will continue to be employed to mitigate threats in the IoT. TIA urges policymakers to regard the IoT as an opportunity for greater security, since using a network approach that is paired with proper risk management techniques, IoT devices can be made to work together to produce comprehensive, actionable security intelligence in near real-time. These approaches and risk management techniques are by and large driven by market demands, typically manifested through industry-driven best practices and standards developed in open, voluntary, and consensus-based fora.

To support high levels of security and resilience in the IoT, TIA urges policymakers to be guided by the following principles:

Respect competitive differentiation and business continuity. As ICT manufacturers and vendors work to meet the needs of their customers, less secure products that are more vulnerable to cyber attacks will naturally be less attractive in the market. Today, this drives ICT manufacturers and vendors to strive to make their products and services less susceptible to cyber attacks, and this is expected to increase dramatically.[5] The degree to which an organization's performance goals are used to ensure their ability to provide essential services while managing cybersecurity risk will be dependent upon the specific needs of their sector and organization. However, in the ICT sector, manufacturers work with the range of organizations they supply to ensure that performance goals of those organizations are reflected in the ICT they purchase. The flexibility to innovate and the use of voluntary, consensus-based standards are both key enablers of this capability. There is no "one size fits all" solution to securing the IoT. The reach of the IoT across segments of the economy that will have varied levels of risk illustrates this.

Rely on international standards. Numerous standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners & operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels. TIA urges policymakers to ensure that their approaches to the IoT reflect the priority for the development of internationally-used standards and best practices. The global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and a global supply chain can only be secured through an industry-driven adoption of best practices and global standards. Country-specific standards should be avoided, as they would ignore the benefits of global harmonization, restricting trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system.

Utilize the successful public-private partnership model. Public-private partnerships are an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face. The voluntary, public-private model is also able toevolve in response to changes in threats and the risk environment. As both the complexity and number of attacks grow, it will be critical that policymakers leverage and augment, or create where necessary, public-private partnerships.

Increase end-user education. This is a crucial aspect to improving cybersecurity in the IoT, as many cyber vulnerabilities are already known and related attacks are relatively easily preventable. Policymakers should lend focus to efforts which inform

[5] *http://www.gartner.com/newsroom/id/2828722.*

end users across the business and consumer communities of proper steps to take to ensure that proper cyber "hygiene" is impressed.

Recommendation: Ensure Flexibility and Feasibility in Addressing Data Privacy

The ICT industry recognizes privacy as a priority in the success of the IoT, and understands the wide range of related concerns held by policymakers. Industry believes that IoT services must adopt principles similar to those that have worked successfully on the Internet to enable informed consumer choice: transparency about what data will be collected, how it will be used, and who will have access. We urge regulators not to adopt privacy regulations that would make it impossible for IoT systems to flourish, as full consumer benefits will require that data be retained and used in ways not currently contemplated, even by IoT innovators themselves. Instead, industry should be allowed to adopt best practices which can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing. Policymakers are encouraged to ensure that their activities do not impose barriers that discourage the use of the use of existing and developing voluntary efforts to address privacy concerns that are developed through standardization, best practice activities, and public-private partnerships. Internationally, policymakers should work towards interoperable privacy systems to avoid unnecessary impediments to the cross-border flow of information, which will be critical to the growth and functionality of the IoT.

Policymakers should avoid implementing privacy obligations which are ambiguous, overly burdensome, or technically infeasible. The effect of adopting such policies would be to decrease industry's incentive to invest in IoT opportunities due to resulting regulatory uncertainty and unnecessarily higher risk. Industry members exploring IoT opportunities should have certainty and the ability to determine the most appropriate method to meet any regulatory requirements. This approach would best promote the development of the IoT as it is a fluid and quickly evolving market opportunity.

In addition, policymakers may serve an important role in ensuring IoT data privacy through public awareness efforts. Through "cyber hygiene" education efforts, many breaches that would result in a loss of data privacy can be avoided. In addition, a more informed end-user is less likely to make voluntary decisions with IoT devices and services that allow data usage beyond their individual comfort.

Conclusion

The IoT represents an immense opportunity for the improvement of the lives of citizens around the globe, across use cases. By ensuring that the path taken forward is collaborative and pro-innovation consistent with the above, TIA believes that policymakers can help these benefits materialize rapidly.

ABOUT TIA

The Telecommunications Industry Association (TIA) represents manufacturers and suppliers of global communications networks through standards development, policy and advocacy, business opportunities, market intelligence, and events and networking. TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment. Visit tiaonline.org for more details.

TIA is accredited by the American National Standards Institute (ANSI) and is a proud sponsor of ANSI's Standards Boost Business campaign. Visit *www.standardsboostbusiness.org* for details.

TIA Policy Committees & Divisions

TIA conducts its policy and government affairs Innovation Agenda through membership committees. A TIA Board Member serves as TIA's Policy Chair and represents TIA's Government Affairs activities on the TIA Board of Directors.

TIA's Communications Research Division, User Premises Equipment Division, and Wireless Communications Division are also represented on the TIA Board of Directors. The Chairs and TIA Staff for each committee, working group and division can be found at *http://www.tiaonline.org/policy/tia-policy-committees-divisions.*

For more information on TIA's Government Affairs activities, please contact James Reid, Senior VP of Government Affairs, at *jreid@tiaonline.org.*

The CHAIRMAN. We will keep the hearing record open for a couple of weeks.

Senator BOOKER. Mr. Chairman?

The CHAIRMAN. Yes, sir.

Senator BOOKER. Along with Senator Rubio's staff, we would like to—and while you were out, I was talking about the spectrum availability and how that potentially could be constricting to American innovation if we do not find ways to meet the growing demands that innovation is going to bring about, not to mention the millions of people globally every month that are coming online.

So I would like to submit for the record a series of statements in support of Senator Rubio and my WiFi Innovation Act, which aims to make more spectrum available. I would love to encourage you to potentially hold a hearing just on that issue that they brought up as something to be of concern.

The CHAIRMAN. We will certainly make that a part of the record and look forward to having a hearing on the subject, which is an important one for all the reasons that have been mentioned today.

[The information referred to follows:]

For Immediate Release

CEA Praises Bipartisan, Bicameral Congressional Effort to Expand Wi-Fi

Arlington, Va., February 10, 2015—The following statement is attributed to Gary Shapiro, president and CEO of the Consumer Electronics Association (CEA)®, regarding today's introduction of the House and Senate Wi-Fi Innovation Act by Senators Marco Rubio (R–Fla.), Cory Booker (D–N.J.) and Representatives Bob Latta (R–Ohio), Anna Eshoo (D–Calif.), Darrell Issa (R–Calif.), Doris Matsui (D–Calif.) and Suzan DelBene (D–Wash.):

> "We enthusiastically applaud congressional members for taking a bipartisan and bicameral approach toward increasing speeds and easing congestion for Wi-Fi by identifying new spectrum for unlicensed uses.
>
> "Unlicensed spectrum is a catalyst for innovation, how we get online through Wi-Fi and how our wireless carriers manage the ever-growing traffic on their networks. And unlicensed spectrum is a boon to the U.S. economy, generating $62 billion a year.
>
> "A look around the show floor at the 2015 International CES® confirmed: from smart homes and unmanned systems to streaming content and wearables, many of today's consumer technology innovations are mobile-first, connected to the Web and to one another.
>
> "The Federal Communications Commission has already committed to freeing up underutilized high-frequency spectrum in the lower 5 GHz band for Wi-Fi. And the study initiated by this legislation should empower the FCC to explore putting even more of this spectrum to use for faster Wi-Fi."

Need help imagining life without unlicensed spectrum? Click here for a look at *A Day Without Unlicensed Spectrum,* an animated video produced by CEA.

About CEA: The Consumer Electronics Association (CEA) is the technology trade association representing the $223 billion U.S. consumer electronics industry. More than 2,000 companies enjoy the benefits of CEA membership, including legislative and regulatory advocacy, market research, technical training and education, industry promotion, standards development and the fostering of business and strategic relationships. CEA also owns and produces the International CES—The Global Stage for Innovation. All profits from CES are reinvested into CEA's industry services. Find CEA online at *CE.org, DeclareInnovation.com* and through social media.

CTIA-The Wireless Association® Statement on the Reintroduction of the Wi-Fi Innovation Act in the Senate

WASHINGTON, February 10, 2015—*The following statement should be attributed to CTIA-The Wireless Association® Vice President of Government Affairs Jot Carpenter:*

"CTIA appreciates Senator Rubio's and Senator Booker's leadership in pushing to make additional spectrum available for unlicensed use. Freeing additional spectrum in the 5 gigahertz band will help meet Americans' increasing demand for mobile Internet access and support the growth of the Internet of Things."

CTIA-The Wireless Association® (www.ctia.org) is an international organization representing the wireless communications industry. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products. CTIA advocates on behalf of its members at all levels of government. The association also coordinates the industry's voluntary best practices and initiatives, and sponsors the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

Twitter: @ctia—Blog: *http://ctia.it/Na6erv*—Facebook: *http://ctia.it/LCm4Nn*
LinkedIn Group: *http://ctia.it/Na6cA2*—Google+: *http://ctia.it/12PfCrO*

Press Contact: Amy Storey, astorey@ctia.org,

HIGH TECH SPECTRUM COALITION

FOR IMMEDIATE RELEASE
Contact: Jared Weaver
(202) 548–2308
jweaver@alpinegroup.com
www.hightechspectrumcoalition.org

High Tech Spectrum Coalition (HTSC) Commends Introduction of the Wi-Fi Innovation Act

Washington, D.C. February 10, 2015—The members of the High Tech Spectrum Coalition (HTSC) commend Senators Rubio and Booker and Representatives Latta, Eshoo, Issa and Matsui for reintroducing the Wi-Fi Innovation Act. This important bill will continue the expansion of unlicensed spectrum use in the 5 GHz band. We are optimistic that sharing at 5.9 GHz will be successful and lead to greater and more efficient use of the band. As the need for more spectrum is ever more evident, it is imperative that we continue to explore new spectrum bands to help satisfy consumer demand for mobile broadband. We appreciate their recognition of the need to maximize this finite resource. Spectrum is the single most critical element for the continued growth of our Nation's Internet economy. We look forward to working with Congress to find additional bands of spectrum for wireless broadband use in order for consumers to continue to see the benefits of innovation and connectivity.

BIPARTISAN WI-FI INNOVATION ACT INTRODUCED IN THE HOUSE AND SENATE

By Vince Jesaitis (ITI)

Spectrum may not be a household word, but we rely on it every day for the connected devices like smartphones and portable devices that are a central part of our lives. Spectrum is a term used to describe the radio frequencies that all wireless communications use. And, as there are only so many radio frequencies, spectrum is a limited and valuable resource. As the Internet of Things (IoT) connects everyday devices from household appliances and our cars, to industrial systems and commercial transportation fleets, more spectrum will be required and spectrum will become an even more important issue for connectivity and future innovations. ITI has long held the view that we must make efficient use of all spectrum to meet our Nation's growing demand.

The bipartisan Wi-Fi Innovation Act bills introduced today in the Senate by Sens. Cory Booker (D–NJ) and Marco Rubio (R–FL); and in the House of Representatives by Reps. Bob Latta (R–OH), Anna G. Eshoo (D–CA), Darrell Issa (R–CA), Doris Matsui (D–CA), and Suzan DelBene (D–CA); would help utilize and manage the upper 5GHz band of spectrum more efficiently to meet the growing demand for bandwidth from connected vehicles and next generation Wi-Fi.

The Wi-Fi innovation Act would direct the Federal Communications Commission (FCC) to facilitate technical and engineering analysis to determine how unlicensed Wi-Fi use can coexist with connected vehicle technology without jeopardizing safety. Moreover, with this bill, we are optimistic that if the significant technical expertise and input from many of our member companies is included to advance the technical process, successful sharing of the upper 5 GHz band is feasible.

The 5 GHz band offers tremendous opportunity to expand unlicensed Wi-Fi use and features, building on the benefits tens of millions of Americans already use to connect in their homes, at work, and in public spaces across the country. We commend these lawmakers for working together in a bipartisan fashion to introduce this proposal, and look forward to working with them to encourage their colleagues to support these bills to benefit the American public and our economy.

About ITI. The Information Technology Industry Council (ITI) is the global voice of the tech sector. As the premier advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more. Follow us on Twitter for the latest ITI news *@ITI__TechTweets.*

DUNCAN NEASHAM,
Director of Communications,
Information Technology Industry Council (ITI).

www.itic.org
Follow ITI on TWITTER: *@ITI__TechTweets*

---

http://www.pcia.com/pcia-press-releases/700-pcia-commends-senators-rubio-booker-for-introducing-wi-fi-innovation-act/

PCIA Press Releases

PCIA COMMENDS SENATORS RUBIO, BOOKER FOR INTRODUCING WI-FI INNOVATION ACT

February 10, 2015/Alexandria, Virginia, The head of PCIA—The Wireless Infrastructure Association today commended Senators Marco Rubio (R–FL) and Cory Booker (D–NJ) for introducing bipartisan legislation aimed at allocating greater spectrum use for wireless broadband and bringing leading-edge wireless service to low-income neighborhoods.

"Senators Rubio and Booker should be commended for recognizing that the U.S. faces both an unprecedented 'wireless data crunch' and a 'digital divide' that puts lower-income Americans at a disadvantage," said Jonathan Adelstein, PCIA's President and CEO. "Their Wi-Fi Innovation Act would allocate more spectrum use for the rapidly growing wireless industry while also eliminating barriers to and creating incentives for Wi-Fi deployment in low-income neighborhoods. Senators Rubio and Booker are taking a crucial bipartisan step toward the adoption of policies that will ease the wireless data crunch and help bridge the digital divide," Adelstein said.

The Rubio-Booker bill directs the FCC to conduct testing to gauge the feasibility of opening the 5850–5925 MHz band to unlicensed use. It also urges that the 5 GHz band be explored for Intelligent Transportation and other "shared" purposes. Finally, it establishes a study aimed at reducing the barriers to Wi-Fi deployment in low-income rural and urban areas and encourages the FCC to evaluate incentives and policies that could enhance wireless adoption.

"The demand for wireless mobile data is continuing to explode. Yes, we need to allocate more spectrum—but that only addresses a fraction of what we need to be doing to spur greater wireless infrastructure deployment. PCIA will continue to work hand-in-glove with Congress, the FCC, and other federal, state, and local policymakers to embrace policies that facilitate the construction and upkeep of a world-class wireless broadband network," Adelstein said.

PCIA—The Wireless Infrastructure Association is the principal organization representing the companies that build, design, own and manage telecommunications facilities throughout the world. Its over 200 members include carriers, infrastructure providers, and professional services firms.

For Immediate Release
February 10, 2015

Public Knowledge Applauds Congress for Introducing Wi-Fi Innovation Act

Today, Members of Congress introduced bipartisan, bicameral spectrum legislation that seeks to expand the availability of unlicensed spectrum. Senators Marco Rubio (R-FL) and Cory Booker (D–NJ) reintroduced the Wi-Fi Innovation Act, while Representatives Robert Latta (R–OH), Anna Eshoo (D–CA), Darrell Issa (R–CA), and Doris Matsui (D–CA) introduced companion legislation in the House.

The Wi-Fi Innovation Act directs the Federal Communications Commission to investigate ways to open the 5GHz band to unlicensed use and recognizes the need to balance the importance of developing Intelligent Transportation and incumbent licenses in the 5GHz band. The legislation also seeks to increase innovation and economic progress by establishing a study to examine Wi-Fi deployment in low-income communities.

The following can be attributed to Martyn Griffen, Government Affairs Associate of Public Knowledge:

> "The Wi-Fi Innovation Act legislation provides an excellent example of how bipartisan legislation on spectrum issues can work. Public Knowledge supported the Rubio-Booker language when it was introduced in the 113 Congress and we are pleased to see it reintroduced in the 114 Congress. This bill provides a road map for agencies that respects both the need for wireless capacity for safer smart cars and the need for more open spectrum for the Internet of Things.
>
> "Furthermore, we are pleased that this legislation addresses broadband access in underserved areas by establishing an FCC study to examine Wi-Fi deployment in low-income communities and the barriers preventing deployment of wireless networks in low-income neighborhoods. As Americans become increasingly more connected through mobile devices and the Internet of Things, our wireless spectrum demands increase.
>
> "We applaud Senator Booker, Senator Rubio, Congresswoman Eshoo and other co-sponsors for taking steps toward addressing this growing concern, while working to expand Internet access to those in underserved areas."

You may view our full release here.

Public Knowledge is a Washington D.C.-based public interest group working to defend consumer rights in the emerging digital culture. More information is available at *http://www.publicknowledge.org*

NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

FOR IMMEDIATE RELEASE
February 10, 2015

CONTACT: Brian Dietz/Joy Sims
202-222-2350

Statement of NCTA Regarding Introduction of the Wi-Fi Innovation Act

"We congratulate Senators Rubio and Booker on the introduction of Wi-Fi Innovation Act which would secure more unlicensed spectrum in the 5 Ghz band. With more and more Wi-Fi-enabled devices coming to market everyday, consumers will continue to need additional spectrum to use these tools. This bipartisan legislation provides a clear path forward for properly allocating a finite and increasingly necessary public resource and continues to establish the U.S. as a global leader in public Wi-Fi availability, speed, and scale."

NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the Nation's cable television households and more than 200 cable program networks. The cable industry is the Nation's largest broadband provider of high-speed Internet access, serving more than 54 million customers, after investing $230 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art digital telephone service to more than 28 million American consumers.

FOR IMMEDIATE RELEASE

CONTACT: Farrah Kim, *FarrahKim@Rational360.com*

TIA APPLAUDS THE RE-INTRODUCTION OF THE WI-FI INNOVATION ACT

Arlington, Va. (February 10, 2015)—The *Telecommunications Industry Association* (TIA), the leading association representing the manufacturers and suppliers of high-tech communications networks, today applauded Sens. Rubio (R–FL) and Booker (D–NJ) for re-introducing the bipartisan Wi-Fi Innovation Act.

The Wi-Fi Innovation Act would require the Federal Communications Commission (FCC) to move forward on testing for unlicensed operations in the 5.9 GHZ band. As the sponsors noted, the Wi-Fi Innovation Act aims to provide more unlicensed spectrum use in order to bolster innovation, spur economic development, and increase connectivity.

TIA CEO Scott Belcher commented, "The U.S. is in vital need of more spectrum in order to meet unprecedented and growing demand for video, data, Wi-Fi connectivity and more. The Innovation Act identifies meaningful steps to help alleviate the spectrum crunch that threatens the advancement of global communications. TIA supports efforts to work towards a workable spectrum sharing solution for the 5.9 GHz band, and agrees that sharing proposals need to be thoroughly tested, leading to the creation of a record that can be the basis for regulatory action. We thank Senators Rubio and Booker for their sponsorship of the Wi-Fi Innovation Act and look forward to working with them on this important legislation."

Follow TIA on *Facebook, LinkedIn, Twitter, YouTube, TIA NOW* and *Google+* for the latest updates.

About TIA

The Telecommunications Industry Association (TIA) represents manufacturers and suppliers of global communications networks through standards development, policy and advocacy, business opportunities, market intelligence, and events and networking. TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment. Visit *tiaonline.org* for more details.

TIA is accredited by the American National Standards Institute (ANSI), and is a proud sponsor of ANSI's Standards Boost Business campaign. Visit *www.standardsboostbusiness.org* for details.

FARRAH KIM,
Rational 360.

Wi-Fi Alliance® welcomes introduction of Wi-Fi Innovation Act

Austin, Texas, February 10, 2015—Today in the United States Congress, Senators Rubio (R–FL) and Booker (D–NJ) introduced *the Wi-Fi Innovation Act,* with a House companion measure co-sponsored by Representatives Latta (R–OH) and Eshoo (D–CA). The bill directs the U.S. Federal Communications Commission (FCC) to work with the U.S. Department of Transportation (DoT) and National Telecommunications and Information Administration (NTIA) to closely study the impact of opening the 5.9 GHz spectrum band for use by a wide array of devices.

Wi-Fi Alliance® welcomes the proposed U.S. legislation and urges lawmakers to take action swiftly to advance innovation in unlicensed spectrum.

"We applaud this group of Senators and Representatives for their recognition of the value of unlicensed spectrum in enabling innovation and economic benefits today," said Edgar Figueroa, president and CEO of Wi-Fi Alliance. "It's well understood that more unlicensed spectrum is critical to meet our society's ongoing requirements for connectivity."

Unlicensed spectrum has created significant economic opportunities in the U.S. and worldwide. Recent *studies* assess the worldwide economic value of Wi-Fi® to have been well above $200 billion in 2013, and with growth in Wi-Fi offloading, sales of Wi-Fi equipment, and other drivers of economic activity related to unlicensed spectrum usage, the economic benefit is *predicted* to exceed $500 billion in 2017.

The proposed legislation would require the FCC to develop spectrum-sharing tests to examine how devices may use the 5.9 GHz spectrum band in the U.S. without

negative impact to other users, and to open the spectrum to Wi-Fi devices, unless it identifies a compelling reason not to do so.

"Although this spectrum was allocated fifteen years ago for future use in vehicular communications, it remains underutilized today," continued Figueroa. "Wi-Fi includes a number of proven mechanisms that make it capable of sharing spectrum with other technologies, and these mechanisms can be adapted to enable shared use of the 5.9GHz band. We are eager to work closely with the FCC, DoT and NTIA to provide technical expertise and industry feedback during their examination of the issue."

Please visit *www.wi-fi.org* for more information on the various Wi-Fi Alliance technologies and certification programs available today and in development.

About Wi-Fi Alliance®
www.wi-fi.org

Wi-Fi Alliance® is a global non-profit industry association—our members are the worldwide network of companies that brings you Wi-Fi®. The members of our collaboration forum come from across the Wi-Fi ecosystem and share a common vision of connecting everyone and everything, everywhere. Since 2000, the Wi-Fi CERTIFIED™ seal of approval designates products with proven interoperability, industry-standard security protections, and the latest technology. Wi-Fi Alliance has certified more than 23,000 products, delivering the best user experience and encouraging the expanded use of Wi-Fi products and services in new and established markets. Today, billions of Wi-Fi products carry a significant portion of the world's data traffic in an ever-expanding variety of applications.

Senator BOOKER. Thank you, sir.

The CHAIRMAN. And thank you and Senator Rubio for your work on it.

All right. If there is nothing else, we will keep the record open, and witnesses are requested to submit written answers to the Committee as soon as possible to questions for the record.

I want to thank the witnesses today. It has been a great panel, a lot of good discussion and back-and-forth on a subject of just enormous importance to our economy. We want to make sure that when we approach this issue, we get it right from a public policy standpoint. So thank you for your very thoughtful suggestions in that regard.

This hearing is adjourned.

[Whereupon, at 12 p.m., the hearing was adjourned.]

A P P E N D I X

February 9, 2015

Hon. FRED UPTON,
Chair,
Committee on Energy and Commerce.

Hon. FRANK PALLONE,
Ranking Member,
Committee on Energy and Commerce.

Hon. JOHN THUNE,
Chair,
Committee on Commerce, Science, and Transportation,

Hon. BILL NELSON,
Ranking Member,
Committee on Commerce, Science, and Transportation.

We the undersigned associations, representing automobile manufacturers, motorists, state highway and transportation officials and the intelligent transportation community, write to you today to respectfully request your opposition to the Wi-Fi Innovation Act. Introduced last Congress, this bill would open up previously dedicated auto safety spectrum to unlicensed Wi-Fi users and jeopardize the implementation of a safety critical crash avoidance system that has the potential to significantly reduce traffic crashes and assist in reducing greenhouse gas emissions. While this legislation currently does not have a bill number, we anticipate its re-introduction soon.

Over the past two decades the auto industry, the U.S. Department of Transportation (USDOT), the American Association of State Highway and Transportation Officials (AASHTO), the Intelligent Transportation Society of America (ITS America) and its member companies and university research centers such as the University of Michigan Transportation Research Institute (UMTRI), have invested significant resources and over a billion dollars researching, developing and testing a vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication system collectively referred to as V2X.

The V2X communication system is comprised of seven safety channels utilizing 75 MHz of spectrum located in the upper 5.8 GHz and lower 5.9 GHz band. This system enables vehicles to communicate with each other and with the world around them (traffic signals, bicycles, pedestrians, buses, trucks and even mobile phones) providing real-time 360 degree high-speed situational safety warnings allowing drivers to respond or in some cases the vehicle to respond for them. Happening ten times per second, these communications must be free of any signal interference. One miscommunication or blocked signal could cause a crash and, possibly, serious injuries or deaths.

The Wi-Fi Innovation Act would require the Federal Communications Commission (FCC) to open up the reserved 75 MHz of spectrum to unlicensed Wi-Fi use and eliminate the proper safety mechanisms provided to the FCC to ensure the protection of the V2X communication system. The opening of this spectrum without proper interference testing would reverse decades of efforts. It would also negate the ongoing efforts of the various constituencies who are exploring whether a technical solution exists to allow sharing of the spectrum. These wide ranging constituencies include automakers, the Wi-Fi community, the FCC, the U.S. DOT and innovators from across the transportation, technology and research communities. This collaborative process should proceed without pre-emptive legislation that sets arbitrary deadlines and restrictive parameters.

Connected vehicle technology may significantly impact the future of auto safety and must be protected. In fact, the National Highway Traffic Safety Administration (NHTSA) has initiated a rulemaking to establish standards for this technology to operate in unison in all vehicles. They estimate that at full penetration, V2X technology could prevent or mitigate up to 80 percent of the annual unimpaired vehicle

crashes saving thousands of lives and reducing the $871 billion cost to our Nation's economy each year. 'Talking cars' that avoid crashes and reduce traffic congestion and pollution are being deployed today as tests continue. That is why we ask for you to oppose any legislation, such as the Wi-Fi Innovation Act, that could set the program back and risk the implementation of this life saving technology and safety system.

Thank you for your consideration of our views. Please do not hesitate to reach out to us for further information or to answer any questions.

Sincerely,

Thomas E. Kern
Interim President and CEO
Intelligent Transportation Society of America
(ITS America)

Mitch Bainwol
President and CEO
Alliance of Automobile Manufacturers

Michael P. Melaniphy
President and Chief Executive Officer
American Public Transportation Association

Jill Ingrassia
Managing Director, Government Relations
and Traffic Safety Advocacy
AAA

Roger A. Wentz, CAE
President and CEO
American Traffic Safety Services Association

Frederick "Bud" Wright
Executive Director
American Association of State Highway and Transportation Officials (AASHTO)

John Bozzella
President & CEO
Association of Global Automakers, Inc.

Greg Cohen
President & CEO
American Highway Users Alliance

Brian Pallasch
Managing Director of Government Relations
and Infrastructure Initiatives
American Society of Civil Engineers

cc: Members of the House and Senate

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO MICHAEL ABBOTT

Question 1. Mr. Abbott, as an investor, you have finite resources and need to pick and choose between great ideas. What is it about the Internet of Things that has you and your firm excited? What concerns do you see on the horizon that may temper that enthusiasm?

Answer. We are excited because of the incredible wave of innovation that we see coming in this space. Analysts today are projecting anywhere from 20 to 50 billion new sensors within the next five years. Those sensors will be deployed across consumer, industrial, and enterprise sectors. Some sensors will replace existing processes, enabling better products and services at a lower cost. Others will create entirely new capabilities, whether they are autonomous vehicles or sensor-equipped industrial machinery or delivery drones.

Beyond the developments that get headlines, there are others that are just as important. When we deploy sensors at this scale, we have new tools for quality control, moving from a timed approach to maintenance—checking the crane or the elevator or the brakes every set number of months—to knowing immediately when a product is overheating. This needs-based approach improves quality, improves durability, improves productivity, and—perhaps most important—improves workplace safety. This is just another example of how the Internet of Things will change the way we live and work. And as the best engineers in Silicon Valley focus on this area, whether in manufacturing and logistics or in other functions that make a difference for the enterprise, the possibilities will continue to increase—and the costs, for consumers, will continue to fall.

Some of the creation and deployment of these new technologies will come from existing companies. But others will come from resourceful entrepreneurs who draw on their own creativity and expertise to build meaningful standalone businesses. Our firm exists to find and back those entrepreneurs and help them build great companies.

Our main concern is not with the state of technology but with the prospect of ill-designed regulation. We know that there are legitimate concerns about how the data

collected by new sensors will be used, and we support clear transparency about what data is being collected and how it is being used. But we also know that the new sensors, if they are to unlock the power of this technology to improve the lives of consumers, require sufficient data. The technology is young—We are still learning what data is most useful and why, and we are still learning how to use data more efficiently. Our hope is that policymakers will recognize that the ability to use big data, so long as the consumer has not opted out, is essential to innovation in this space.

Question 2. Mr. Abbott, in your testimony, you urged regulators and legislators to proceed with caution when considering regulation regarding the Internet of Things. As you note in your testimony, the FTC recently released a staff level report on the Internet of Things which makes "best practice" recommendations on privacy, security, and data minimization. I understand many IoT companies are concerned about whether today's best practices may tomorrow become "reasonable" practices subject to enforcement by the FTC. This could lead to a great deal of uncertainty in the marketplace for startups. How do questions about the FTC's reach affect investors like yourself?

Answer. Starting a successful company, even in a space with as much opportunity as the Internet of Things, is never easy. If the FTC's reach began to factor more significantly into our calculations as we considered whether and how a startup would succeed, the decision to back an IoT entrepreneur would become more difficult.

This is especially true because early-stage companies, unlike large tech firms, generally do not have existing data to draw on. Their ability to innovate depends on their ability to learn from the data generated by users. If they faced restrictions in doing this, they would have a harder time getting off the ground, as so many startups fail to do. As investors, we would be more skeptical of the prospects for success when the market is constrained, and we might instead turn our attention to other markets—and perhaps look for opportunities abroad if the regulatory environment there were more favorable for entrepreneurs.

We fully support clear transparency around data collection practices and believe that the consumer should know what is being collected as a user of the product. We simply hope that the legitimate need for transparency will not turn into regulatory practices that stifle innovation in this space at such an important time.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO DOUGLAS DAVIS

Question 1. Mr. Davis, Intel is opposed to FCC reclassification of broadband service under Title II of the Communications Act, a view that I share. Do you think that reclassification could harm growth of the Internet of Things? If so, how?

Answer. As a world leader in computing and communications technologies, Intel wants net neutrality rules that foster an open, accessible Internet and affordable, high quality broadband. Therefore, we support FCC rules regarding disclosure, blocking and discrimination. We filed Reply Comments in the FCC's Open Access proceeding opposing reclassification of broadband providers as utilities under Title II, because we believe it is not necessary and could discourage expensive and risky "last mile" broadband investment. Specifically, as to IoT, Intel wants both open and high-quality connectivity for all. With a projected 50 billion connected devices by 2020, investment in ubiquitous, faster and more affordable Internet connectivity will be even more critical. In that regard, we generally believe that "light touch" regulation promotes more broadband investment while still protecting open access, and thus we encourage the FCC to implement its Title II authority in a light touch manner.

Question 2. Mr. Davis, these days, hacking and security concerns are seemingly always on the front pages. Data breaches have affected many millions of consumers and some of the largest corporations in this country. Consumers are right to be excited about the benefits of the Internet of Things to their lives, but it is reasonable to be concerned about whether IoT opens consumers up to potential harm by cyber criminals. What steps is the technology industry generally, and Intel specifically, taking to secure IoT devices?

Answer. Security must be a foundational building block for IoT in order to establish consumer trust—whether that consumer is a business, government, or an individual. Intel believes we can provide robust consumer protections, while enabling IoT investment and innovation that will improve the economy and GDP. (Of note, primary economic drivers of IoT will be commercial and industrial use cases, not consumer-facing applications.) For trusted data exchange in an IoT ecosystem, data

generated by devices and existing infrastructure must be able to be shared between the cloud, the network, and intelligent devices for analysis—enabling users to aggregate, filter, and share data from the edge to the cloud with robust protection. For this reason, security is fundamental to Intel's IoT roadmap.

As discussed in my Prepared Statement for the Record (pp. 4–6), Intel believes that it is critical to integrate security into hardware and software from the smallest devices at the edge of the network to the most advanced server in the cloud and all gateways and devices in between. These multi-level security capabilities create redundancies which prevent intrusions and enable a robust, secure, trusted end-to-end IoT solution. Intel's hardware will provide transistor-level security on the actual compute device itself at the outset (rather than layering it on top at latter point in design cycle with other, less secure external features). This means each compute device can have an irremovable identification which prevents any non-approved device from accessing the network. Intel's IoT solutions also will employ advanced hardware level capabilities—"whitelisting" (prevents harmful apps from being activated) and "blacklisting" (blocks list of known malware from entering device or network). Intel Security also integrates advanced software level security capabilities which enables the software to identify threats and proactively notify users and/or automatically quarantines devices that could be at risk. With this combination of transistor-level security, plus advanced hardware and software level security, Intel will protect IoT assets and data in ways few others can.

With respect to the technology industry generally, Intel and other technology companies collaborate with government, non-governmental organizations, and other private industry stakeholders to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction. A recent example of such collaboration is the Cybersecurity Framework led by the National Institute of Standards and Technology (NIST). Executive Order 13636 (issued in February 2013) directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. Intel and other technology companies worked collaboratively with other private industries and U.S. government partners to develop the Framework. Intel then took it a step further by creating, implementing and publishing a case study that encourages use of the Framework as a process and risk management tool.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO LANCE DONNY

Question 1. Mr. Donny, you stated the Internet of Things technology can often be cost prohibitive for farmers. One reason we've seen IoT proliferate is huge cost reductions for bandwidth, processing, and sensors. Are these trends helping to drive IoT adoption on the farm? What is needed to bring the cost of technology down for farmers?

Answer. Yes, generally these trends help farmers adopt technology in greater numbers and this is evidenced by the price of cellular data transmission falling slightly over the last several years. We expect to see this trend continue, and through better wireless technology, the ability to move greater amounts of data over fewer discrete cellular bands; further driving data transmission costs down.

Question 2. Mr. Donny, in your testimony, you talked about the drought in California and how challenging that has been. Would you please elaborate on how the Internet of Things is helping farmers deal with a lack of water?

Answer. Farmers in California have been devastated by what now is a four-year drought. Farmers have begun to deploy a greater number of soil moisture sensors to increase the understanding of the amount of available water they do have. Technology like moisture sensors provide accurate management tools that take the guess work out of irrigation. We see farmers save from 5–25 percent of their overall water though these methods.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROY BLUNT TO LANCE DONNY

Question 1. As the "Internet of Things" includes modems talking to each other, and machines talking to each other, how reliable is wireless connectivity in remote areas today?

Answer. Wireless connectivity varies based on a number of factors but are most impacted by topography, crop canopy density, and antenna height. We've seen poor connectivity outcomes where both factors are challenging, in some cases a few hundred feet of range to ranges of 10-miles where we have ideal conditions. While we don't need to see every installation achieve 10-mile range, we need reliably to cover a full section (640 acres) in most cases.

Question 2. What broadband capacity is needed and how soon will it be available for the potential of the "Internet of Things" to be realized in agriculture—particularly for precision agriculture?

Answer. The bandwidth demand in agriculture is not as significant as other demands such as online learning or telemedicine. We can reliably move most data (excluding large image files) over relatively low bandwidth speeds, less then 10mbps. More importantly is the coverage area. If large agriculture areas go uncovered, the industry will continue to rely on cellular and satellite for communication, which is costly and less then reliable.

Question 3. A number of colleagues from this committee and myself recently wrote the Federal Communications Commission to emphasize that "rural households and businesses stand to benefit" from the Mobility Fund for wireless broadband in rural areas, and the Connect America Fund for fiber broadband in rural areas.

Today's hearing underscores that need, as the "Internet of Things" is dependent on broadband connectivity—both wireline and wireless.

What is your opinion of the Federal Communications Commission's attempt so far to reform the Mobility Fund for rural wireless, and the Connect America Fund for fiber to unserved rural areas?

Answer. In all fairness, I am not fully versed on the Mobility Fund. In my opinion the changes to increase 4G services with Phase II funding must not inadvertently allow whatever level of data service, which support IoT, in rural markets to deteriorate. In addition, in order to ensure IoT data services don't diminish over time the FCC should consider grouping areas that lack 2G coverage in an auction separate and apart from those areas in which carriers are seeking to upgrade from 2G, 2.5G and 3G services to 4G services. This, in my opinion, will enable lower cost carriers a means to support the vast amount of connected devices in rural markets.

Question 4. In your testimony, you cite the American Farm Bureau's Privacy and Security Principles. These principles cover a wide range of issues including education about rights and responsibilities, ownership of data, the collection and use of data, notice, transparency, and choice for consumers.

Did the American Farm Bureau need a government agency to instruct them in developing these principles, or were they able to come up with them on their own?

If the American Farm Bureau can establish a set of principles regarding expectations of rights and responsibilities for the "Internet of Things," can other sectors of the economy do the same?

Answer. The American Farm Bureau, given it's breath of farm knowledge, 6 million members, industry relations, and capacity to engage farmers in dialog regarding their concerns and needs was able to develop these principles without government agency support.

While I'm not an expert on other sectors their make up or challenges, I firmly believe in the power of collaboration. The most efficient and realistic method of developing principles is for industry and it's customers to work together. In this way needs, fears, opportunities, and challenges can be discussed and solutions can be agreed upon that will achieve actual success once implemented.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO ADAM D. THIERER

Question 1. Mr. Thierer, in comments to the FTC, you argued that policymakers should exercise regulatory humility in the face of uncertain technological change and address harms only after conducting a cost-benefit analysis of various remedies. FTC Commissioner Wright raised similar concerns about the FTC's recent staff report on the Internet of Things. What are the dangers of not doing a cost benefit analysis before moving forward with policymaking in this space?

Answer. Although benefit-cost analysis is extremely challenging in the field of digital privacy policy, it is essential that analysts and policymakers attempt to conduct such reviews of any regulatory proposals aimed at curbing private sector data collection. While we will never be able to perfectly determine either the benefits or costs of data controls, the very act of conducting a regulatory impact analysis will help us to better understand the trade-offs associated with various regulatory proposals. In this case, benefit-cost analysis would help us determine the impact of new data regulation on technological innovation, consumer choice, entrepreneurialism, economic growth and the competitiveness of America's digital economy. And because data has powered the Information Revolution and brought consumers a cornucopia of new choices, it is essential that we carefully evaluate any new rules for their impact on the economy.

Question 2. Mr. Thierer, in a submission to the FTC you wrote that, "It is likely that citizen attitudes about IoT technologies will follow a familiar cycle we have seen play out in other contexts: initial *resistance,* gradual *adaptation,* and then eventual *assimilation* of that new technology into society." Where are we today on the spectrum of Internet of Things adoption?

Answer. We are still in the very early stages of Internet of Things adoption and, at least thus far, we've not seen as the same sort of initial resistance to IoT technologies that we witnessed with many previous technologies. While some privacy and security concerns have, perhaps, held back some consumer adoption at the margin, it appears that the public is quickly moving into the "gradual adaption" phase and embracing these technologies. It could be the case that the public's remarkably rapid assimilation of smartphone technology into their lives since 2007 has acclimated consumers to IoT technologies and made their adoption less jarring.

○

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.