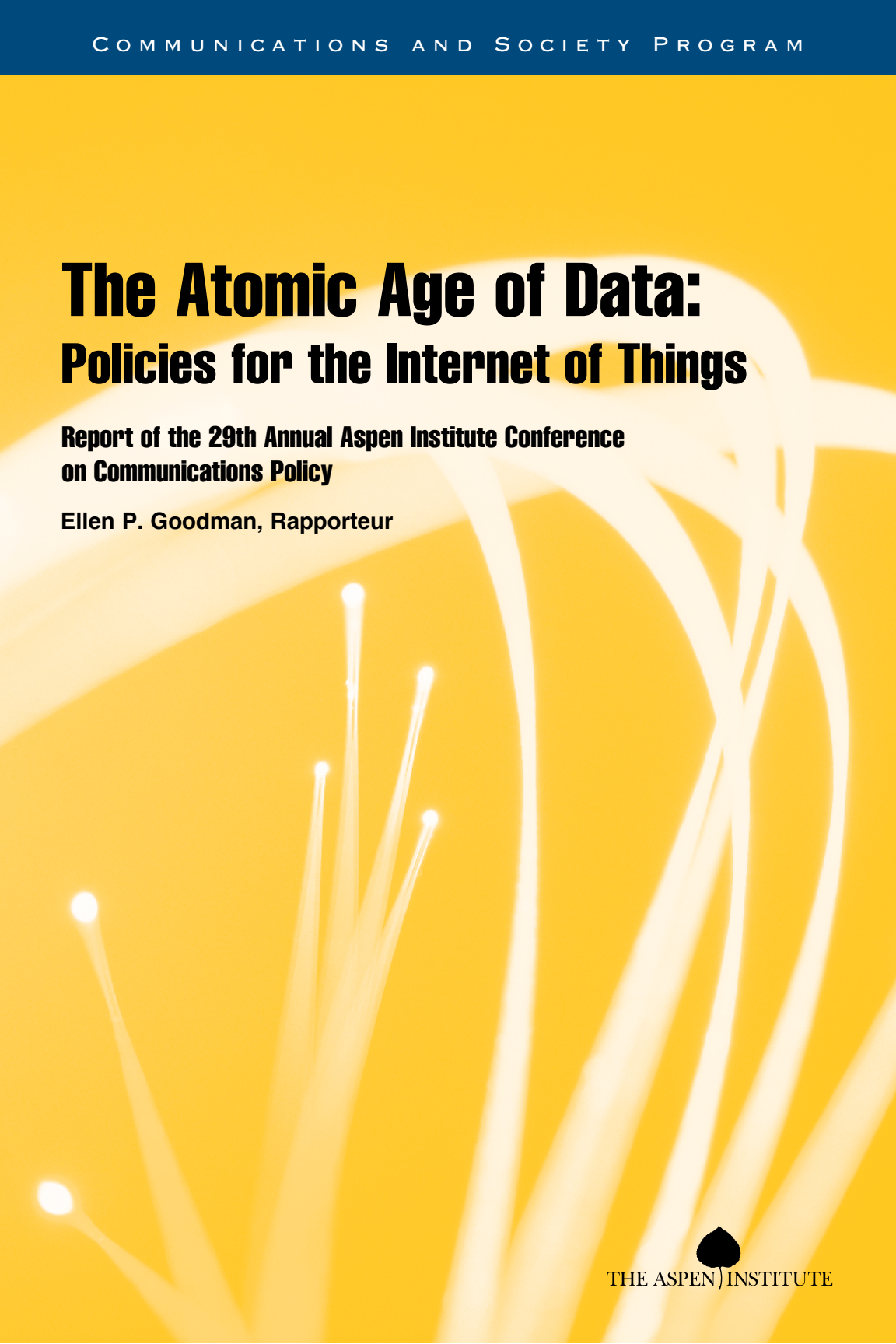
The Atomic Age of Data:
Policies for the Internet of Things

Report of the 29th Annual Aspen Institute Conference on Communications Policy

Ellen P. Goodman, Rapporteur



THE ASPEN INSTITUTE

The Atomic Age of Data
Policies for the Internet of Things

Ellen P. Goodman
Rapporteur

THE ASPEN INSTITUTE

Communications and Society Program
Charles M. Firestone
Executive Director
Washington, D.C.
2015

To purchase additional copies of this report, please contact:

The Aspen Institute
Publications Office
P.O. Box 222
2014 Carmichael Road
Queenstown, Maryland 21658
Phone: (410) 820-5326
Fax: (410) 827-9174
E-mail: publications@aspeninstitute.org

For all other inquiries, please contact:

The Aspen Institute
Communications and Society Program
One Dupont Circle, NW
Suite 700
Washington, DC 20036
Phone: (202) 736-5818
Fax: (202) 467-0790

Charles M. Firestone
Executive Director

Patricia K. Kelly
Assistant Director

The Aspen Institute
One Dupont Circle, NW
Suite 700
Washington, DC 20036

Published in the United States of America in 2015
by The Aspen Institute

Printed in the United States of America

ISBN: 0-89843-623-0

15/10

2029CSP/15-BK

Contents

This report is written from the perspective of an informed observer at the Aspen Institute Conference on Communications Policy. Unless attributed to a particular person, none of the comments or ideas contained in this report should be taken as embodying the views or carrying the endorsement of any specific participant at the Conference.

Foreword

Each summer the Aspen Institute Communications and Society Program convenes approximately 30–35 leaders and experts in the information and communications technology sectors—from business, non-profits, government and academia—to address a cutting-edge topic in U.S. domestic communications regulation. For the summer of 2014 the topic was the Internet of Things, the difference in kind created by the connection of billions of devices, sensors and people to the common communications network of the future.

Often the gathering of these experts leads to significant advances in regulatory thinking, but of an incremental kind. This conference went further. In reviewing the interplay between the vast increase in data created on the Internet of Things (IoT), and the resultant strain on the networks that carry this information, the group came to a realization. *Data needs to be thought of as "infrastructure."*

With this realization, a number of recommendations for information and communications policy ensued. While viewpoints varied widely, there was a level of consensus among the group on the following principles:

- Treat IoT data *itself* as infrastructure—an essential building block for all kinds of economic, social and civic activity.
- Design-in security controls that reduce threats to connected devices and systems, and ensure that these security controls can be kept current.
- Design-in privacy controls that minimize collection of personally identifiable information and effectuate Fair Information Practice Principles.
- Promote broad accessibility of data and data analytics, which will require interoperable standards in many parts of the IoT ecosystem.
- Government should promote adoption and diffusion of technology, including building out IoT capabilities when it invests in infrastructure (known as a "dig once" proposal).

- IoT systems should ensure accessibility for the disabled and underserved through inclusion by design.
- The IoT should act as a vehicle for citizen participation and empowerment.
- Government should promote common standards for smart cities and other applications.
- Government should use procurement powers and regulatory powers to promote privacy and security.

Data needs to be accessible, and government needs to facilitate data production in certain cases. The role of private investment is as crucial as ever, but government purchasing and deployment of data is also significant, particularly in the area of public goods such as health care, public safety, energy and transportation.

There are indeed many positive uses envisioned by the Internet of Things, and policies to foster those public and private benefits are important. But there are also a number of cautions the group grappled with. These include the values of privacy, inclusion, equity and security. These concerns ran through the deliberations and resulting recommendations, which are reported below.

Acknowledgments

The Institute wishes to acknowledge and thank the following companies and foundations for supporting the Communications and Society Program and participating in this conference: AT&T, Cablevision, Charter Communications, Cisco Systems, Comcast Corporation, Google Inc., Intel Corporation, Motorola Mobility, Netflix, New Street Research, Telefónica Internacional USA, Inc., Time Warner Cable and Verizon Communications.

We thank Ellen P. Goodman, Professor of Law at Rutgers University, for writing the conference report in a way that gives the reader context, conceptual understanding and, thankfully to the participants, a continuity to the dialogue that took place over three days in August 2014. We ask our rapporteurs to give their sense of the proceedings. So any statement made in the report, unless attributed in quotes, is not necessarily the view of each of the participants or their employers. Rather it reflects the

arguments or assertions being made at the meeting, leading to the recommendations of the group.

I also want to thank Ian Smalley, Senior Project Manager for the Aspen Institute Communications and Society Program, who was responsible for managing the meeting and report, Rachel Pohl and Liyuan Zhang for their help in selecting and editing background readings, and Tricia Kelly, our Assistant Director, who supervised the production of the report.

Charles M. Firestone
Executive Director
Communications and Society Program
The Aspen Institute
Washington, D.C.
April 2015

The Atomic Age of Data
Policies for the Internet of Things

Ellen P. Goodman

The Atomic Age of Data
Policies for the Internet of Things

Ellen P. Goodman

Introduction

The networked devices dispersed on store shelves, factory floors, city streets, home surfaces and the human body are creating an Internet of Things (IoT). The IoT outfits the physical world with digital intelligence and moves data flows to the atomic level. A sushi restaurant puts sensors on its plates to assess, in real time, what's being eaten so it can adjust its food offerings. An environmental monitoring firm analyzes sensor data from construction sites to keep a lid on noise. A city monitors traffic flows, energy use and trash can levels. A health care provider collects data on individual medication metabolism. A company sells a microcontroller for dozens of connected devices, a cloud-based system for managing them and analytics to make meaning from the data they produce. Wearables, massive sensor networks, and public and enterprise deployment of IoT technologies raise important policy questions about privacy, security, equity, innovation, governance and growth. Some are familiar—like Internet policy questions—only on a significantly larger scale. Others are new.

The Internet of Things outfits the physical world with digital intelligence and moves data flows to the atomic level.

This report explores the nascent promises and challenges of the IoT. It documents the Twenty-Ninth Annual Aspen Institute Conference on Communications Policy, entitled "Developing Policies for the Internet of Things," that convened 35 participants on August 13–16, 2014, in Aspen, Colorado. The Conference itself organized the discussion

around three general topics: data as infrastructure, adoption and digital inclusion issues, and government role. In light of the cross-cutting issues, this report organizes its policy examination and recommendations according to six principal areas of focus: Data as Infrastructure; Privacy; Equity, Inclusion and Opportunity; Civic Engagement; Telecommunications Network Architecture; and Security. It drills down on some of these policy questions in the context of the use case of the Smart City. Before reaching these issues, we start by describing what we mean by the IoT and mapping its applications and architecture.

Mapping the Internet of Things

Kevin Ashton, an MIT researcher, first used the term "Internet of Things" in 1999 to describe the use of radio frequency identification (RFID) in supply chain management.[1] There were big expectations then that RFID data would revolutionize business. That didn't happen. It may be that the time was not ripe. Others think that when just a few companies were pushing RFID—notably Walmart—there was resistance to its adoption.[2] The new IoT—small sensors + big data + actuators—looks like it's the real thing. And it is a much bigger thing than RFID deployments alone could ever have been. The IoT is the emergence of a network connecting things, all with unique identifiers, all generating data, with many subject to remote control. It is a network with huge ambitions, to connect all things. This is what Bruce Sterling calls "the Manifest Destiny of silicon."

As grand as the ambition, the implementation is made possible by some very mundane things that did not exist in the early days of RFID. The first is the continuing transition to Internet Protocol version 6 (IPv6), which creates enough Internet addresses to associate with a virtually infinite number of things. The second is cheap data storage. If there will be 50 billion connected things by 2020 (and in all likelihood, more), all the resulting data will have to be held somewhere.[3] The first task for the Conference was to map the IoT, to define its terrain. That begins with demarking the boundaries between the IoT and the Internet, while recognizing that in many ways the IoT is an extension of the Internet.

The IoT Explosion

Hype. The 2014 Gartner Hype Cycle identified the IoT as one of the 10 technology trends with the greatest potential.[4] Cisco estimates that by the year 2020 there will be over 50 billion connected devices.[5] McKinsey estimates that the IoT could have an economic impact of $6.2 trillion by 2025.[6] What are the implications of this massive expansion of connectivity? From one perspective, as much as 99 percent of the world—those things not connected to the Internet—has been sleeping; the IoT will awaken it, enabling everything to be more responsive to the needs of users. From another perspective, more connectivity will exacerbate the security and privacy concerns already pronounced in a world of big data collection and analytics. As the ACLU has said, "Your home will know your secrets, and chances are it will have loose lips."[7]

What is not in doubt is that the IoT is becoming commercially attractive, as borne out by the tech world's recent large investments in hooking up the home. Cable started the connected home movement years ago, but the pace picked up recently when Google purchased Nest, Samsung bought SmartThings and Apple launched its HomeKit strategy all in an effort to provide the platform over which people will control their home environments and feed their information into a network of connected devices. These companies are betting on transforming home appliances and systems into networked communicators that will track customer habits and better respond to inchoate customer desires. Others, like IBM and Cisco, have staked futures on doing the same in industrial and municipal contexts. They count on widely deployed sensor networks to exploit the ambient intelligence of chattering things.

These networks build on the Internet, but their features differ in some important ways from the Internet itself.

Heterogeneity. The IoT takes advantage of the Internet for long-distance communications, but there are important architectural differences between the Internet and other parts of the IoT infrastructure. Whereas the Internet was designed as a network of networks to be a general purpose utility, the IoT involves specialized technology and varied architectures. Some devices, such as traffic lights, communicate continuously, while others send information in bursts, such as a pill that tells the nurse when it's been swallowed. While some applications require big pipes for continuous video, most need fractional bits of

bandwidth. Some will have a user interface, subject to individual control, while others will contain connectivity deeply embedded in appliances. Users can opt-out of or control connectivity in some cases, but in many others, they will not know whether or how sensors are working.

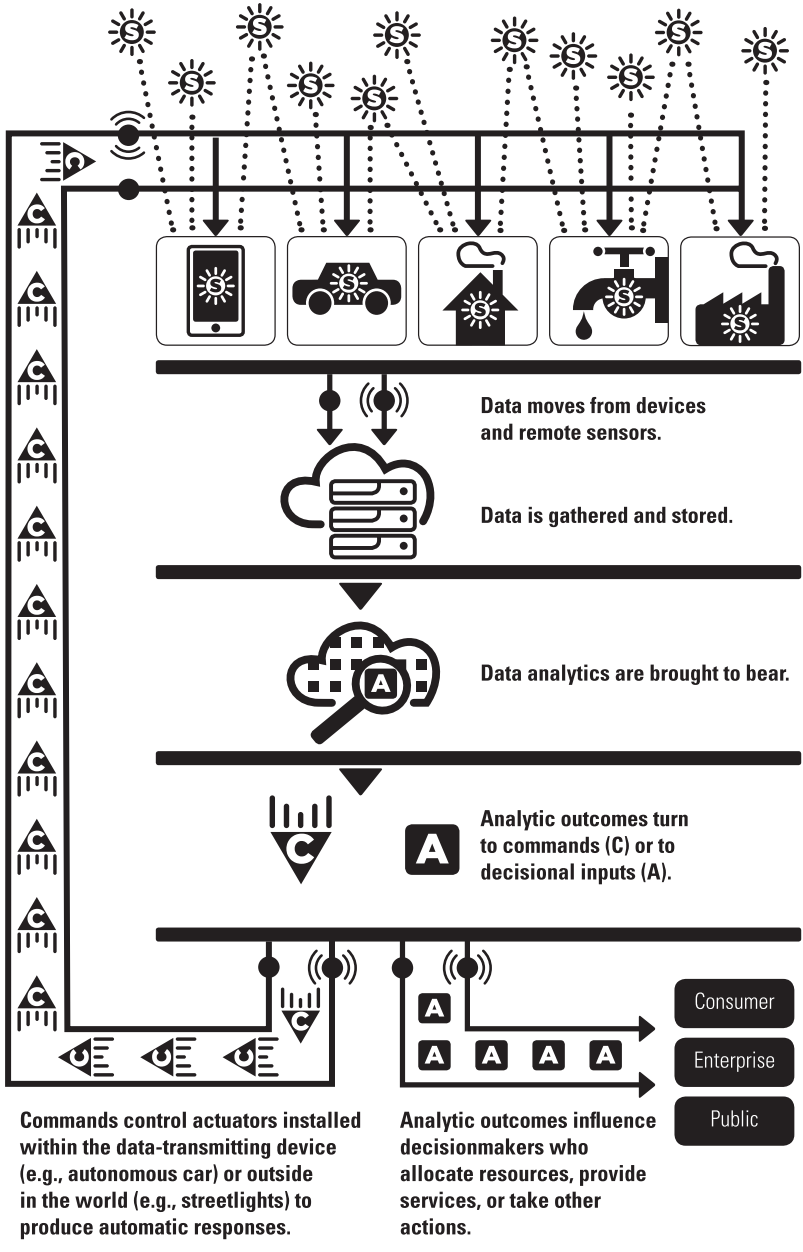
The heterogeneity of the IoT complicates policy discussions. What might be a very serious concern for some applications, such as consumer privacy, might be irrelevant for others. So too, issues of interoperability, standards and network access might play out very differently in different kinds of component IoT networks. This report will try to be sensitive to variations in IoT deployment, while at the same time positing that the IoT as a whole is a coherent subject for consideration and distinct from the Internet.

A map of the Internet of Things would include the following components:

- Low-power integrated circuits and wireless communications that enable miniature devices to sense their environments and generate data.
- Middleware that runs these sensor networks.
- Cloud and other data storage, including the "fog" of more proximate shared storage among devices.[8]
- Analytics that make sense of the data and then trigger either autonomous or human-mediated decisions.
- Schemas that uniquely identify objects and also allow for their remote control through the network.[9]
- Visualization and presentation tools that enable interaction between the user and sensor network data.[10]
- Actuators.

Of all these components, the most significant and new capabilities are: (1) vast webs of cheap and low-powered sensors gathering data from their environments and (2) actuators making autonomous decisions based on this data.[11] The sensors and actuators run on top of communications infrastructure to make key connections. The data they collect or act upon may be stored or acted upon locally, remotely in a cloud system or both.

Diagram 1. IoT Data Flows



Benefits and Risks. With the IoT, as with the Internet, its features are sometimes its bugs. IoT applications create a smarter world that is better able to align resource use with need, where cities and citizens, consumers and companies all benefit from having more data to make better consumption and resource deployment choices. At the same time, efficiencies and innovation obtained through data sharing could increase security breaches, data discrimination, digital exclusion and threats to civil liberties. These negative outcomes may be the result of either intended or unintended IoT features.

Critics of the IoT warn that integrating our things into digital networks creates a "digital feudalism" in which an ever-larger range of human activity is surveilled and monetized by platform operators.

An intended feature of the IoT world is more efficient decision making. For example, the insurance company refines its premiums based on the eating habits of individuals who are now trackable through personal monitoring systems and a smart refrigerator. What is an efficiency-gain for the company can be experienced by the individual as discrimination and an invasion of privacy. In the online world, sellers tailor prices and offerings based on consumer data. That kind of "smart selling" will migrate to the offline world. Critics of the IoT warn that integrating our things into digital networks creates a "digital feudalism" in which an ever-larger range of human activity is surveilled and monetized by platform operators.[12]

Then there are the unintended consequences. We worry about and seek to mitigate the cyber-security vulnerabilities of the online world. These risks already implicate the physical plant when it comes to critical infrastructure.[13] A diffuse IoT introduces greater vulnerabilities to a broader array of atomic things, where hacking can interfere with the operation of devices from cars to pacemakers.

To some extent, the IoT merely enlarges—vastly—the existing Internet. It dramatically increases the number of inputs into the sys-

tems of data collection and analytics that drive the digital world. In other ways, the IoT is something entirely new. It empowers our physical world to make decisions about how it interacts with us, without any direct human intervention.

The Territory of the IoT

Peak buzz on the Gartner Hype Curve does not necessarily produce peak clarity on whether the IoT is just Internet sprawl or new territory. What changes qualitatively when we increase by an order of magnitude the nodes on the Internet (or other networks)? What does it mean when information generation migrates from people to things? The Conference participants wrestled with how to talk about and define the IoT.

Scale. One of the distinguishing features of the IoT is its sheer scale. The amount of data that can be gathered from ubiquitous sensor networks dwarfs even the most aggressive mining of the Internet of People. Consumer Internet applications give people free stuff and services in exchange for data. The same dynamic will fuel consumer IoT applications, only on a much bigger scale. In exchange for data, manufacturers will offer consumers cheaper durable goods, food, deliveries, etc.

Kevin Werbach, Associate Professor of Legal Studies at the University of Pennsylvania's Wharton School, made the point that what the IoT does is turn "data at rest into data in motion." Data that was once latent in objects or residing in devices is suddenly moving, findable and usable. The sheer volume of these flows raises new questions about who controls the information; who benefits from it; and how the information changes business, civic and personal relationships.

User Control. The territory of the IoT is defined not just by differences in scale from the Internet but also differences in kind. One of the most significant differences is user control. The ability of users to meaningfully opt out of data collection has long been subject to debate. We know that it is difficult to forego data collection when the collecting apps are a virtual necessity. The mobile phone itself—a sensor that we all carry with us—must be put to sleep or clothed in a Faraday case in order to avoid tracking. The IoT further reduces, and in many cases eliminates, user control over data collection.

People also cannot control the environments into which they walk. Nicol Turner-Lee, Vice President and Chief Research & Policy Officer of the Minority Media and Telecommunications Council, said she fears that the idea of consent and autonomy in the IoT world is mere fantasy. There will be times when the mere act of entering a physical space "submits you to the Internet of Things." The same kind of involuntary submission may follow you home if you are a renter who may not know about smart-home choices. Turner-Lee questioned, "If I walk into an apartment that's fully equipped with IoT devices, do I have a right to say to my landlord that 'I'm going to disconnect'?"

Privacy and the right to disconnect are of course implicated in a big way when people and their things are connected in such an automatic and uncontrolled way. People may want rights over the resulting data, whether personally identifiable or anonymized, but it is not clear how Fair Information Practice Principles developed for the digital world apply when so many IoT applications will have no user interface or meaningful opt-out features.[14]

Actuators. Stefaan Verhulst, Co-Founder of the Governance Laboratory (GovLab) at NYU, said that what's really different about the IoT is that it allows things to act, not just to speak. This can be as banal as a refrigerator ordering milk. Or it can be as consequential as an autonomous car making decisions about where to brake. According to Verhulst, "This level of agency that you create through the IoT has hugely different policy implications" from the ordinary Internet.

Data Analytics. Robert Atkinson, Founder and President of The Information Technology and Innovation Foundation (ITIF), said that the territory of the IoT is defined by analytics. "The Internet has largely been a platform for communications and transactions," Atkinson observed. The data analytics built atop these activities have been crucial in funding the development of the Internet. Analytics will become vastly more important for the IoT. To be sure, IoT technologies will provide information (e.g., Fitbit giving you the number of calories burned) and enable controls (e.g., the Nest thermostat adjusting the temperature), but "a lot of the value will come from analytics." As part

of the evolving world of big data, the massive amounts of data that IoT sensor networks collect will become useful through big data analytics.[15]

The data analytics will drive the actuators, changing the behavior of things based on algorithmic prediction. Advertising, too, the lifeblood of the consumer Internet, will morph in response to the data analytics the vast number of IoT sensors support. The IoT creates an ambient layer of intelligence throughout the physical world and advertising will be part of this layer. According to *Advertising Age*, the IoT will require advertisers to "buy people at a moment in time—buying micro-moments to serve hyper-relevant personal ads" based on intimate data and analytics that can "promote routes in our cars" and respond to stress indicators on wearables and smartphones.[16]

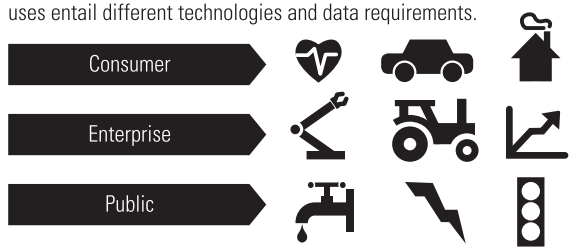
Not Made in America. Bob Pepper, Vice President, Global Technology Policy for Cisco Systems, notes that whereas the Internet was invented in the United States and moved outwards, the IoT is global from the start. Different approaches in different parts of the world mean that we may see many regulatory strategies, and we can expect power struggles over technology standards, data location and management. "The players are global. The device makers are global. Where the data is and how it's being used is global, and there are broader global questions about data transfer and data localization."

Data as Infrastructure. The insights that the Internet is principally about communications and that the IoT is principally about data analytics lead to another distinguishing feature of the IoT: It turns data into infrastructure. Like the Internet, the IoT depends on a physical infrastructure of routers, servers, IP protocols, telecommunications networks and distributed storage and processing systems associated with long-distance communication, cloud-based storage and processing for big-data analytics. Data is infrastructural as well. The collection of data and data analytics drive the behavior of actuators and the purpose of sensor networks. The data collected from these sensor networks becomes a new infrastructure, access to which may be critical for the provision of certain services.

Diagram 2. Conceptualizing IoT Applications

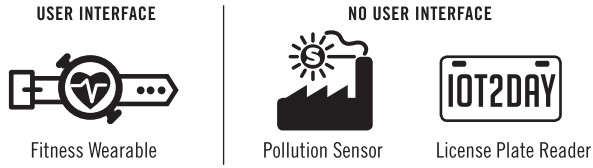
IoT World by **Application Use Case**

One way of dividing the IoT world is by use case, as different uses entail different technologies and data requirements.



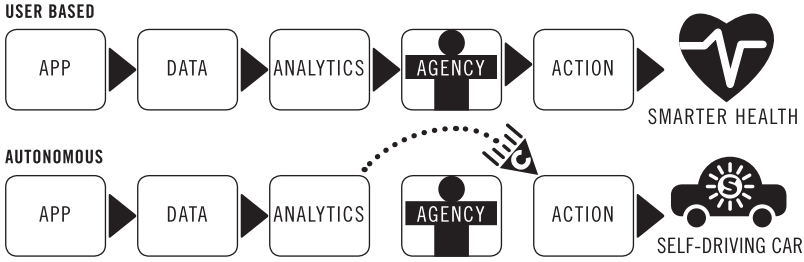
IoT World by **User Interface**

Some IoT applications have a user interface. Others have no user interface at all; users have no control except possibly to disable connectivity.



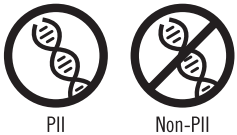
IoT World by **Data Flow**

Some IoT applications operate autonomously without human intervention between data flow and actuators. Others require or invite human agency.



IoT World by **Data Collection**

Some IoT applications will collect and analyze personally identifiable information (PII) while others will rely on non-PII.



Types of IoT

Once within the territory of the IoT, there are different ways to visualize its topography.

- One is according to **user** and associated kinds of applications.
- Personal→smart homes, health and wellness monitoring, driving.
- Enterprise (cities, industries)→industrial automation, municipal or other public resource management, agricultural productivity.
- Utilities→water monitoring, electrical grid.

Another cut is according to possibilities for **user control**. Some IoT applications have no user interface. Once the connectivity is installed in a thing, a human being plays no role at all, except possibly to disable it. Sensors woven into fabric, or dropped into paint, would be examples of this.

- User interface (e.g., Fitbit).
- No user interface (e.g., environmental sensors).

A third way to categorize the IoT is by **technology**. Some applications transmit data but require human intervention for subsequent action. Others lay actuators on top of sensor networks and data analytics so that the data can direct action autonomously, without the need for human decision making after the software is written. Examples might be found in the smart house that tailors energy supplies based on usage data. The autonomous car is another.

Policy Issues and Recommendations

It is early days for IoT policy. The European Union held a consultation on the subject in 2013 and issued a report that identifies general areas of concern.[17] The FTC held a conference in 2013, building on its customary emphasis on privacy and transparency for the development of digital applications. It issued its report in early 2015.[18] With Congressional hearings in the offing,[19] the Aspen Conference provided a timely forum to raise policy concerns and possible approaches to manage IoT risk and promote opportunity.

Any use of IoT applications that involves the collection of personal data implicates privacy. By privacy, we mean both (1) the actual protection and control of personal information and (2) the more general sense that one can secure a sphere of solitude and anonymity in the

world of connected things. Privacy-related policy concerns loom so large that they tend to swallow up other considerations; indeed, they permeate this entire Report and sparked the most vigorous debates at the Conference. This Report begins, however, with an equally fundamental concept. It is the concept of data-as-infrastructure. As the Internet of Things takes off, data becomes infrastructure in the sense that control over and access to data is a basic input into all kinds of economic, civic, personal and social activity.

Data as Infrastructure: Access, Discrimination, Production

The IoT consists of networks of connected devices that generate data and make it actionable. Smart devices get lots of attention, but it's the data that will drive IoT adoption. Data flows use infrastructure. IoT data *itself* is infrastructure—as a vital input to progress much like water and roads, and just as vulnerable to capture, malicious or discriminatory use, scarcity, monopoly and sub-optimal investment. When you conceptualize data as infrastructure, you begin to surface policy questions that are either new or more pressing in the IoT context. Danny Weitzner, Director of the MIT CSAIL Decentralized Information Group, observed that while the Internet looked like an application to many first adopters, "now it looks like infrastructure. That might happen with data as well. There is an infrastructural quality to data."

For Weitzner, what data as infrastructure means is that there should be "a common body of data about the world that will be used in an integrated fashion." We should therefore treat the vast and dynamic collection of data as "a unified resource with common standards and clear, common access conditions that increase the chance it can be subject to integrated analytics." Bob Pepper, Cisco's Vice President of Global Technology Policy, disagreed. He emphasized that IoT data really is not a unified resource because there are going to be so many heterogeneous systems generating data that may be of widespread interest or of little interest outside the entity that generated it.

For Stefaan Verhulst, Co-Founder and Chief Research and Development Officer of the Governance Laboratory (GovLab) at NYU, once you see data as infrastructure, it becomes essential to map data resources. It is important to know what data exists, how robust it is, and what needs to be collected. And critical to this process is citizen

engagement. "How do you involve people in the development of data-collection agendas? How do you engage citizens at all stages?" he said. "How do citizens come to participate in the generation of data that helps them and that they think is important?" A recent report by the President's Council of Economic Advisors, *Big Data and Differential Pricing*, shows that massive data sets can increase discriminatory pricing based on profiling, but they can also reduce discrimination by improving the accuracy of individualized predictions.[20] Which way the process tips depends on transparency, vigilance, education and access to the data that is shaping decisions.

Data Access and Ownership

Access to infrastructure is necessary for competition, innovation, productivity, social inclusion, economic mobility, citizen participation and self-fulfillment. All that is true for access to data. For example, data on disease trends may be an essential input into the development of pharmaceuticals. Traffic data may be an essential input for a small business that wants to locate a restaurant or for a neighbor that wants a new traffic light at a dangerous intersection. Increasingly, journalism relies on sensor data to report what is happening in the world.[21] Who controls data and who has access to it thus becomes a matter of economic vitality as well as social inclusion and political action. The open data movement in government—expressly endorsed by the White House—recognizes the utility of making it easy to access public data.[22]

"The key is to have interoperable standards, not necessarily a common standard." — ***Robert Pepper***

In order for data to be made widely available, there was broad agreement at the Conference that there should be either common or interoperable IoT data formats. As Weitzner noted, "common formats doesn't mean that the data is free." It will often be necessary to charge for data in order to incentivize its production. Pepper cautioned that, given the heterogeneity of the IoT, "the key is to have interoperable standards, not necessarily a common standard."

Johanna Shelton, the Director of Public Policy & Government Relations at Google, urged the development of access and interconnectivity rules for different layers of IoT data stacks. Put most simply, there is raw data, such as raw traffic data, and there is processed data, such as correlations between traffic and weather or other events. Shelton argued for relatively generous access rules to raw data, while allowing companies to restrict access to processed data. She recounted Google's experiment in the health space. The company wanted to "draw the intelligence" out of insurance company data but couldn't get access to the raw data. It may often be the case, she said, that "those who deploy sensors and control the data may not be squeezing all the [socially beneficial] intelligence out of it, and this is an argument for open access to that data."

Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), said the most relevant distinction is not whether data is raw or processed, but whether it is personally identifiable. NOAA data, collected from buoys and atmospheric sensors, is an example of data that is not personally identifiable and that, therefore, should be available to everyone. "This is a sensor network that's not about people; it's about the world around us." Also, "The NOAA data doesn't actuate events…. It provides information about our environment. It does not trigger action against individuals."

Verhulst noted that the really valuable information might not be NOAA's data, but what private companies build on top of the NOAA data, and that's much trickier to open up. Verhulst pointed to Google Flu data as an example where the insights from the analyzed data are of value to the public. The data sets have some of the qualities of a public good. "It's a public service to share the processed data." At the same time, sometimes privacy concerns might compel limited access to data analytics, in addition to or even more than access to raw data. We might also want to have trusted intermediaries to assess data requests and provide discretionary access.

Reed Hundt, CEO of the Coalition for Green Capital, called attention to the intentional analogies of "data infrastructure" and "communications infrastructure." The latter is largely privately owned, but there is a public interest in ensuring that it is robust and universally available. There might be similar interests in data infrastructure. Even as to pri-

vate infrastructure, he said that we might "want the government to step in and say, 'We'd like for this to be universally distributed or made universally available.' There is some layer of data that rides on top of the physical infrastructure that really ought to be publicly owned, publicly allocated, made available by a public democratic process to absolutely everyone." Then on top of this data, private entities can innovate and add analytics and utility.

Extending the telecommunications analogy, it is possible to conceptualize access to data as a right of interconnection. Users may not be entitled to full sets of raw data or processed data, but to interconnect at certain points in order to make use of the data collected by others. MIT's Weitzner raised the concept of "data liberation" and the desirability of applying concepts of access and interconnection to data. Chris Libertelli, Vice President of Global Public Policy at Netflix, on the other hand, objected to applying concepts of interconnection to the IoT. "Those norms and policies are completely inappropriate to the question of whether an independent application developer gets the rights to, say, an energy data set…. As a principle of regulatory humility, there should be a consensus that this old stuff [interconnection] shouldn't apply in the new world of big data meets connectivity."

Joanne Hovis, President of CTC Technology & Energy, worried that the push toward open data for public entities has resulted in the allocation of significant public resources for collecting and making available data sets. This might not be a problem, if it were not for the fact that "private parties make use of the data to benefit only a segment of the population." In other words, there's a transfer of resources from the public to the private sector. We should be attentive to the issue of whether public investment will actually benefit the entire public.

An example of a controversial private-sector purchase of processed public information is Monsanto's acquisition for over $1 billion of the Climate Corporation. The Climate Corporation develops data on climate change by analyzing 50 terabytes of data daily—much gathered by public sector sensors—about weather, soil quality and other data points relevant to farmers.[23] This data is important for farmers' insurance policies and crop production plans. But now it is the private property of a principal vendor of agricultural inputs. The public data remains public, but the value-added or analyzed data is private and owned by a vertically integrated supplier to farmers.

Robert Atkinson, Co-Founder of the Information Technology & Innovation Foundation, suggested that there were three possibilities for the way the IoT information ecosystem might develop: (1) "Proprietary and Balkanized, with every institution having its own data—GE has its data, Ford has its data—and that would be suboptimal,"; (2) proprietary and combined, like the Nest example, where a company invests enough to do great analytics because it has a large universe of data; and (3) open and combined, "which in some ways is the Nirvana." Atkinson argued that every factory would be better off if it had access to the data from all other factories and data sets were combined. Whether or not the private sector will see its own way toward this kind of cooperation is an open question.

Outside the IoT context, we have not yet come to conclusions about how large sets of quasi-public data should be managed. Uber has vast amounts of information in the form of the rides that individuals take. The company has come under fire for inappropriate use of this data in privacy-invasive ways.[24] Another issue is whether Uber should have to share anonymized versions of this data in order to help urban planners and others that want to better understand traffic patterns. This is data that licensed taxis have to share to help policymakers police discrimination in the provision of taxi service. As tasks formerly undertaken by public or publicly licensed entities shift to a less-regulated sector, questions arise as to what should happen to the data. Is there a public claim on the data, and, if so, how are individual privacy and proprietary business interests protected? These questions are not new to the IoT, but they become more pressing as the data sets explode and municipal functions are privatized.

An important piece of the data access issue is data ownership. There will be plenty of situations where claims to data ownership overlap and conflict. The connected car furnishes an example. Bob Pepper of Cisco forecast that by 2018 a quarter of a billion connected cars will be on the road around the world, each one with an average of four modules (e.g., brakes, steering), each module with multiple sensors generating loads of data.[25] He identified questions raised: "That data about my car, my driving…whose is it? Is it mine? Is it the manufacturer's? Is it the dealer's?" New kinds of data collected and transmitted by the connected car could include biometric and behavioral information about the driver, as well as fine-grained location information and automobile performance diagnostics.

Carl Povelites, Assistant Vice President of Public Policy, Mobility at AT&T Services, suggested that ownership has to be pegged to incentives to innovate. "With respect to the onboard diagnostics unit, does the car company own it because it invested in the research and built the systems? Or does the individual own the data so that if the check engine light comes on, they should be able to go to any repair shop?" He argued that "companies that are doing the investment must own the data so that they have the incentive to put forward all that money and capital."

…[data] ownership has to be pegged to incentives to innovate. — *Carl Povelites*

It's not always obvious whether a data set is most useful for public or private purposes, or whether it will be produced absent private ownership. Aggregated health data, for example, may be a public resource with respect to public health but a private resource with respect to disease research. Coming up with rules of use and access to such data that encourages both kinds of uses is most difficult.

Reed Hundt recommended that "government should define some kinds of data that should not be allowed to be the source of private wealth and instead should be turned into a public good." Energy use furnished an example. No one ought to be allowed, Hundt argued, to own and exclude others from accessing data about people's energy use. Instead, it should be collected and publicly reported. That kind of public access would allow entities to tax according to per capita use and would "empower any firm that wanted to offer an energy efficiency solution to use that data so that individuals could avoid the tax."

Michael Calebrese, Director of the Wireless Future Program in the Open Technology Institute of the New America Foundation, added that government should leverage its power as a regulator or property owner to ensure open access to data that bears on public externalities (such as pollution or energy waste). A number of NGOs are working to make sure that municipal sensor data is open and available as soon as it is collected.[26]

EPIC's Rotenberg disagreed that this kind of data should be widely available when it contains personally identifiable information (PII). Indeed, he advised that government should refrain from collecting domestic energy use data that is PII. Gathering such data might even constitute an illegal search, as the Supreme Court found in a case about surveillance of heat emitted from a marijuana grow room.[27] Following the NOAA example earlier, he proposed a way to use data to promote environmental protection without using PII. Authorities could post pollution notifications, similar to automobile speed monitors, which would show varying levels of air pollution. This approach would make use of aggregate data to obtain a public policy outcome without engaging in the collection of PII that creates privacy risks.

Jonathan Chaplin, Managing Partner of New Street Research, thought that "we should establish property rights relating to data and make very clear delineation of what's personal data that an individual owns and can cede to an organization or a government. But it's their choice." David Hoffman, Director of Security Policy and Global Privacy Officer at Intel Corporation, thought a model of data ownership "is going to be a huge rat hole for us and a very difficult exercise." Marc Rotenberg agreed that an ownership model may work for materials subject to intellectual property protection, but not for personal information. He said the goal of user control over personal data is typically achieved through laws that establish Fair Information Practice Principles. Johanna Shelton remarked that "individual control over information is a really good sound bite, but we know from implementation of the right to be forgotten in Europe that it can be used to trump public accountability and the public's right to know."

One well-received recommendation was that there be a federal law that individuals have a right of access to their personal IoT or even all data collected by any government or private entity, although the practical difficulties in effectuating such a right are daunting.[28]

Data Production: Government Subsidies and Facilitation

The IoT will yield almost unimaginable quantities of data. But it won't necessarily produce all the data that is needed. As in the production of all public goods, there will be a dearth of commercial incentives

to invest in data collection and analysis that produces public benefit without sufficient benefit capable of private capture.

Reed Hundt, CEO of the Coalition for Green Capital, proposed the creation of a data infrastructure bank that would fund projects that collect and make such data available. This would be a federal funding mechanism for "everything from better utility network data to transportation infrastructure sensors, public video surveillance and the means to collect and analyze performance of educational services." The purpose would be to release traffic and road information so that "anybody in the business of selling an intelligent transportation service would have that data available to them." Judgments would have to be made all the time about privacy, for example excluding license plate information while including pothole information. Another example would be data about the thermal envelope of all buildings so that data about inefficient energy use would be publicly available.

There was widespread agreement that if the government is going to fund collection of data, it should be guided by two principles. First, it should focus on externalities, such as pollution or congestion, on the theory that the private sector doesn't have the motive to gather that data. Second, it should focus on data that is non-rivalrous, meaning that anyone can use it without increasing the cost or diminishing the utility of the data for others.

Chief Democratic Counsel of the U.S. House Committee on Energy and Commerce, Shawn Chang, embraced a "dig once" philosophy for government when it comes to IoT sensors and data collection. Where the government is supporting infrastructure development, for example by excavating for new roads, it should consider how IoT sensors and data fit in. Marjory Blumenthal, Executive Director of the President's Council on Science and Technology, expanded, "If you're thinking about government funded roads, then you could provide an expectation that they would incorporate sensors and use technology to enhance monitoring and support maintenance. Where the public grants a right of way, you could tie that to certain implementations for the public good."

Chang focused on the $7 billion FirstNet—the new interoperable national public safety network that will be funded from federal spectrum auction revenues. The construction of this network provides

great opportunities for government to build sensor networks into first responder operations. Chang recommended "leveraging this network to bake into these future public safety devices or transportation systems IoT capabilities that would be useful to collect information on public works, health or environmental needs." When the ambulance, fire truck or police car is moving, it might as well be collecting information that could be used to improve transportation or environmental functions. This would also have the advantage of developing clients for the FirstNet network, assuming that private and public sector entities valued the collection of this data. Client development is important, given that the FirstNet business model is to "collect fees from users in order to have a sustainable business case going forward."

Christine Varney, an attorney with Cravath, Swaine & Moore LLP, advanced the possibility of building IoT applications into the functions of the Accountable Care Organizations (ACOs) created by the Affordable Care Act. She said these organizations "could use the IoT to gather and disseminate, in a continual loop, health information up and down the chain [assuming privacy controls]. There would be an opportunity to expand access, continue to be more efficient, reduce costs and get better quality outcomes."

Varney point out that the result might be "a sensor on an imaging machine that feeds right into the radiologist and the primary care doctor and the insurer and the prescription, the pharmacy and the pillbox—the entire chain of care." Because ACOs are generally regional, the opportunity exists to experiment across a number of different ACOs. And because ACOs have incentives to reduce costs and keep the savings, they would have every interest in getting smarter about the care they offer by exploiting sensor networks.

GovLab's Verhulst focused on what he called "corporate data philanthropy." To the extent that there is data that is important for the equitable delivery of services, for civic participation and for competition and innovation, how do we get companies involved in creating and sharing this data? He wants to explore ways to incentivize or push companies to create data pools that are open to the public.

Data as Infrastructure Recommendations

Basic Principles: (1) There should be broad accessibility of data and data analytics, with open access to some; (2) government should subsidize and facilitate data production, especially where data is an under-produced public good.

Broad Accessibility of Data and Data Analytics

- New data sources should be exposed in standard formats with interoperable interfaces (APIs). This should be a foundation of IoT architecture to ensure efficiency, consumer welfare and innovation gains.
- Government should publish metadata (e.g., NOAA).
- Government should establish metadata standards to foster interoperability (e.g., for anonymized medical records).
- NIST should use convening power to foster global standards for the IoT, with demonstrable security protection.
- USTR should challenge national/non-global standards as trade barriers.

Data Production: Government Subsidies and Facilitation

- Subject to the development of security safeguards, government should leverage areas of investment to incentivize adoption of IoT systems and to drive IoT innovation through government purchasing and deployment. The following are examples:
    - Health Care: Offer Accountable Care Organizations a common data infrastructure platform for data collection and analysis, create incentives for experimentation, and produce best practices.
    - Public Safety: Build in data sharing concerning other verticals like transportation and infrastructure conditions, and encourage citizen adoption and feedback.
    - Energy: Bring IoT to energy inefficient homes using a race-to-the-top model. Ensure there is no monopoly holder of data.

    - Transport: Dig once. Require new and reconstructed highways to incorporate sensors and support maintenance.
- Make open PII-free data, especially if generated using public property or rights of way. Build in data collection and impact measurement in grant-making.
- Review current regulatory restrictions that may impede the creation of new types of data (e.g., FDA medical device rule).
- Develop a plan for the federal government (e.g., Commerce Department) to track the impact of the IoT. Develop common tools for information assessment, dissemination and engagement.
- Create a data infrastructure bank that provides anonymized versions of data from utility networks and transport infrastructure sensors, as well as from other sectors.
- Continue support for current government open data efforts (e.g., NOAA, anonymized health care billing data).
- Incentivize private investment in both infrastructure and innovative uses of IoT data.
- Improve federal, state and local agency use of data. Incentivize use of digital as a default strategy. Use long-term savings for capital expenditures, equipment and focused adoption efforts.
- Put users first, and understand how needs can be met through the IoT in ways that are agile and subject to iterative improvement. Focus on better data, mass customization, digital by design and budget incentives to promote adoption. Possibly develop a coalition of cities to address scale and resource issues.
- Identify gaps in data availability and subsidize production.
- SBA Initiative: Coordinate with state and local economic development groups to create actionable market intelligence about trends, supply chains, training, etc. Possibly develop "IoT startup-in-a-box."

- Invite states, local governments and NGOs to participate in providing turnkey solutions ("Smart City-in-a-Box"), empowering anchor institutions.

Privacy by Design

Informational privacy discussions frequently turn to the need to design privacy protections into systems from the start. And so it is with the IoT. These design choices would set defaults about how much data and what kind is collected, how and where it is aggregated and for what purpose it can be used.[29] Privacy-by-design principles recognize that individual control may be unrealistic as a practical matter. Moreover, as a matter of principle, there may be a social cost to lax privacy even where individuals are happy to relinquish it.

If we treat excessive sharing of personal information as a social cost, much as pollution is, then we might adopt the equivalents of pollution control strategies. EPIC's Marc Rotenberg recommended that before an entity launches a new sensor network, it do a privacy impact assessment: "Do your privacy impact assessment up front, understand the risks that others might be exposed to, and then go ahead." Comcast Corporation's Senior Strategic Advisor, Joe Waz, called this kind of practice "data hygiene"—determining what data needs to be collected and what shouldn't be collected as a basic principle.

Fair Information Practice Principles…are notice, choice, access, accuracy, data minimization, security and accountability.

Environmental or seismic monitoring may not raise privacy concerns because they are unlikely, at least initially, to rely on personal information. By contrast, smart home and smart street applications will very likely raise concerns, whether the data is anonymized or not. Most experts acknowledge that in a world of big data, a large percentage of anonymized data can be re-identified and become personally iden-

tifiable.[30] The implementation of Fair Information Practice Principles (FIPPs) for all consumer-facing IoT applications thus becomes very important, as the FTC acknowledged in its 2015 IoT report.[31] These principles are notice, choice, access, accuracy, data minimization, security and accountability. In the IoT world, the efficacy and cost of each practice is uncertain and variable. While it might be desirable to preserve choice for individuals to opt-out or control usage of their personal data, user choice will frequently be illusory in a ubiquitously sensed environment. This reality puts more pressure on privacy by design strategies to reduce risks of privacy breaches and impose liability for them.

…IoT transparency is a tricky concept: "It's going to be hard to read privacy notices off of sensors scattered around the roadways." — *Danny Weitzner*

In the world of the IoT, privacy by design that bakes in privacy protections to early-stage system design is even more important than it is in the Internet world because so many IoT applications have little or no user interface. The IoT is often invisible to individuals, using pervasive communications networks to process and convey information without any chance for individual intervention.[32] People can't be constantly queried as they walk into a store or onto a street whether they consent to data gathering or whether they understand how their data will be used. To Danny Weitzner of the MIT CSAIL Decentralized Information Group, IoT transparency is a tricky concept: "It's going to be hard to read privacy notices off of sensors scattered around the roadways."

A recent report by the Federal Trade Commission acknowledged that it is not obvious how traditional data protection and FIPPs (e.g., data minimization, security, notice and choice) can be applied to the IoT.[33] The FTC report emphasized that practical difficulties in providing consumers with choice and meaningful transparency means there should be a greater reliance on privacy by design upfront, such as minimizing data collection and maximizing anonymization techniques.

A Lot of IoT Data Is Personal

Many sensor networks do not gather data from people. Neither NOAA meteorological sensors, nor NASA space sensors, nor a company's gas pipeline need to gather personal data. Policymakers need not concern themselves too much with these kinds of applications as far as privacy goes. With respect to personal information, however, EPIC's Marc Rotenberg and others suggested that any sensor network that gathers information on individual human activities is likely to have privacy implications even if it minimizes personally identifiable information.

Rotenberg argued that data anonymization should be a default rule, and where anonymization cannot be achieved, data should not be collected. Even where anonymization is possible, we must recognize that the possibilities for re-identification are legion. This was one of the themes of the 2014 International Privacy Conference, where privacy officials from around the world met to discuss the IoT and big data, issuing at the end the Mauritius Declaration.[34] Because "sensor data is high in quantity, quality and sensitivity," they concluded that "the inferences that can be drawn are much bigger and more sensitive, and identifiability becomes more likely than not." Similarly, the 2014 White House PCAST report flagged the difficulty of real and permanent anonymization in the big data context, where correlations from discrete data sets enable re-identification.[35]

Like environmental protection, privacy protection is a societal value that can't be achieved at the level of individual consumer actions.

The digital dossiers emerging from the IoT might include not only online activities but also constant and perfect location tracking, eating habits, conditioning, sleep patterns and so on. Therefore, the Declaration says that this data should be regarded and treated as personal data even when individual data points are not personally identifiable. It must be protected as a public good, as "a joint responsibility of all actors in society," and not just a matter of individual choice. Many Conference participants reached similar conclusions. Marc Rotenberg

expressed doubt that individuals have sufficient information or incentive to make privacy choices. Instead, these need to be macro choices about what kinds of architectures we want deployed. Like environmental protection, privacy protection is a societal value that can't be achieved at the level of individual consumer actions.

But what to do? Is the standard menu of Internet privacy strategies sufficient, including transparency, user control and local processing of data? Conference participants disagreed about the appropriateness and adequacy of these strategies for the IoT.

Preserving Choice

While recognizing the difficulty of relying on individuals to police IoT data collection practices, there was discussion about giving people the right to exercise control over data gathering and usage where possible. These opt-in or opt-out scenarios are most closely associated with the civil liberties frame of privacy.

Some Conference participants argued that individuals should have recourse to a "cone of silence." Others aspired to a "silence of the chips"[36] or a "Do Not Track" for the IoT. Marc Rotenberg said, "I think we really need to talk about the off switch." As data flows away from us through our health and ambient temperature monitors, all the processing takes place in the background. Rotenberg continued that the consumer has "no notice and choice, so we really need to get serious about the intrusions that are entirely opaque to consumers."

MIT's Danny Weitzner emphasized the importance of "protecting an individual's zone of solitude or control or autonomy…in relation to all this data being collected." He suggested that the solution might be to allow a user to enter a room and know, based on some notice that pops up on a mobile device, "here's the privacy status of this room." You can leave or you can push a button to exclude yourself from data collection. Joanne Hovis, of CTC Technology & Energy, also emphasized the importance of being able to check-out of sensor networks.

But Eli Noam, Director of the Columbia Institute for Tele-Information and Garrett Professor of Public Policy and Business Responsibility at Columbia Business School, cautioned that individual opt-outs may result in bad data, with especially harmful consequences

for efforts to monitor and control disease outbreaks. The Boston-based app called Streetbump seeks to use individuals as sensor networks to crowdsource information about where there are potholes that need to be filled in the municipality. Voluntary participation means that where people agree to download and use the app will determine whose potholes become visible. As much as privacy may be a public good, there are countervailing public goods that are advanced by full participation in sensor networks.

Relatedly, as IoT applications become more pervasive, it may become more difficult to maintain the opt-out option. Consider the trivial example of EZPass or other sensor-based smart card payment systems. Society has to decide that it will maintain an alternate payment system for those who want to opt-out. Or institutions can try to adopt systems where non-PII is shared. Atkinson remarked that he would be more inclined to support these kinds of opt-outs as long as the individual opting out did not impose "negative externalities" on everyone else. By removing their data from the analytical "pool," what is rational for the individual can be irrational for society. To counter this, we may want to consider systems where those who opt-out should pay for any added expense imposed by their choices. Opting for privacy, as has been well-documented, is expensive.[37]

Data Aggregation and Location

Others, such as New Street Research's Jonathan Chaplin, said that the privacy protection measures should not be designed into data *collection* functions, but into protocols around data *usage*. What we should worry about is that data can be used in harmful ways, not that some set of data has been assembled.

David Hoffman, Director of Security Policy and Global Privacy Officer for Intel Corporation, refined this idea. He thought that the most important moment in the life of IoT data is neither the moment of its collection nor the moment of its usage. Rather, what's most important is the point of aggregation. Where data is aggregated will impact how it is used. Data can reside locally in the things that transmit, receive and process it. At the other extreme, data can reside in the distant cloud. In between, there is the "fog"—a repository for data that is more proximate than the cloud, perhaps aggregating data at

the individual or institutional level.[38] Proponents of privacy by design will often advocate for data localization as a way to reduce the risks of privacy-compromising re-identification and unwanted usages. For privacy, security and efficiency reasons, Cisco's Bob Pepper advocated the use of "fog" storage as an alternative to cloud storage.

Hoffman agreed that if the data is held at or near the point of collection, data privacy and usage controls will be easier to enforce. If the data is aggregated more centrally, it becomes an attractive target for theft and runs the risk that advanced analytics will be used against the larger data set. Hoffman emphasized, however, that there is a trade-off here. More centralized data storage may yield more efficient and useful data analytics. So, for example, you might want to insist on surveillance video being stored locally at the edges of the network for processing rather than being aggregated in some more central place where it can be cross-referenced with lots of other data (and rather than not being collected at all). This local storage will promote privacy interests, though probably at the price of some utility.

Another issue in designing networks is how long to retain data in order to mitigate risk. Hoffman said he prefers to think of the assessment as a risk assessment rather than a privacy assessment "because there are non-privacy risks that emerge from access to this huge quantity of data that we'll have from sensors." These include security concerns, like a terrorism risk. These risks can be reduced if data doesn't hang around forever.

Christine Varney of Cravath, Swaine & Moore LLP, raised the possibility of data minimization policies that "make data evaporate after certain periods of time." But Weitzner worried that it was "magical thinking" to base policy on the ability to destroy data after its principal use: "You either have to define primary purpose so narrowly that we'll lose huge benefits from the data, or you define it so broadly that it's completely meaningless." We might want to know, for example, what happened to someone 40 years ago in order to understand disease patterns. Columbia University's Eli Noam said he believes we can solve this problem by having presumptions about the longevity of data collection that can be overcome in particular use cases.

On the issue of personal information, David Hoffman noted that the reason the OECD has eight different Fair Information Practice

Principles[39] is because some of what's not personally identifiable information can become identifiable in the future, so different restrictions are required at different stages. He thinks that it might be time for comprehensive federal privacy legislation "with the idea that we can articulate a process that would describe socially productive uses for data that should be allowed, and uses that we would never allow for data."

…it might be time for comprehensive federal policy legislation…. — *David Hoffman*

Risk-Reward

In the end, Weitzner noted, we have to face the real challenge: "We want lots of benefits from this data, and we're unlikely to give most of those up, so we'd better figure out how to make sure that people aren't harmed in the process."

One example of this risk-reward trade-off is the issue of territorial data localization. Bob Pepper of Cisco emphasized the global nature of the IoT. If the function of the IoT is to convert data to knowledge and then to actionable intelligence, then he thought we should be wary of the data localization policies currently being considered and adopted around the world. These could present significant barriers to the most innovative uses of data. The argument is that data localization requirements are incompatible with the free flow of data and optimal (distributed) system architecture.

For the most part, Conference participants seemed to think that IoT privacy approaches should be risk-based depending on the kind of data collected. We should not view privacy protections as binary, but rather should adopt different levels of control depending on the risks to privacy. The group produced the following risk categories, recognizing that lots of data (e.g., location information) fall between or across categories:

Category 1: Clear risk of misuse or harm from personal information (or easily re-identifiable information) on sensitive matters. Examples would be health information and associations. Possible con-

trol: requirements like the Fair Credit Reporting Act and the Genetic Information Nondiscrimination Act to ensure data accuracy, decisional fairness, user control, accountability mechanisms and possibly collection restrictions.

Category 2: Lower risk of misuse or harm from personal information (or easily re-identifiable information) on less sensitive matters. Examples would be information on purchasing choices or energy usage, where the purpose of data use is for marketing and less consequential profiling. Possible control: user control mechanism.

Category 3: Very little risk of misuse or harm from non-personal information (with no re-identification). Examples: environmental pollution, traffic patterns. No controls.

"This line between PII and non-PII is key for privacy and for innovation, as the collection of personal data necessarily carries responsibilities and liability, while techniques that achieve the same outcomes without PII avoid these regulatory burdens." — *Marc Rotenberg*

Marc Rotenberg of EPIC did not support this taxonomy and cautioned that the better approach is one that simply distinguishes between data that is personally identifiable and data that is not. IoT systems should be designed to avoid collecting PII at all by using privacy enhancing techniques. Where systems do collect PII, Rotenberg said they should employ Fair Information Practice Principles: "This line between PII and non-PII is key for privacy and for innovation, as the collection of personal data necessarily carries responsibilities and liability, while techniques that achieve the same outcomes without PII avoid these regulatory burdens."

Privacy Recommendations

Basic Principles: (1) IoT systems should design in privacy controls that minimize collection of personally identifiable information; (2) IoT systems should effectuate Fair Information Practice Principles to the extent possible, including anonymization and data minimization; (3) individuals should have a way to control collection and transmission of their personal data.

- IoT applications should minimize the collection and retention of personally identifiable information, recognizing that non-PII may become PII once analytics have been applied.
- IoT systems should implement Fair Information Practice Principles, including transparency (machine readable) about data collection and use, data minimization and consumer access and opportunity to correct.
- There should be an individual right to disconnect (not feasible in all cases).
- The privacy value of processing as much data as possible locally must be balanced against the utility of aggregating data.
- There needs to be accountability through mandatory logging of all transactions. There should be individual right of access and tools for analysis to reveal responsibility for rules violations.

Equity, Inclusion and Opportunity

Data as infrastructure raises prospects of citizen empowerment and, likewise, of disempowerment. Who and what is "checked-in" to the network, who and what becomes visible as a result of data sharing, who has power and who is subject to unwanted surveillance or control? As our environments become smarter, they may adjust to our presence in ways that presuppose our wishes and needs. The delivery of services then becomes smarter for those who are sensed accurately, but faulty predictions and un-sensed needs are problems.

Ensuring that the IoT becomes an IoT for everyone requires attention to the same technology adoption issues that have long troubled broadband rollouts. Lee Rainie, Director of the Pew Internet & American Life

Project, thought that we ought to apply learning from the broadband adoption literature to the IoT. It takes lots of tech support and convincing non-adopting members of the public that there's a value proposition for them. Shawn Chang of the U.S. House Committee on Energy and Commerce emphasized the need to subsidize buildout for underserved communities. Julia Johnson, President of Net Communications, focused on digital literacy as a key component, as well as empowering anchor institutions and community-based groups to bridge gaps in technology diffusion.

Data as infrastructure raises prospects of citizen empowerment and, likewise, of disempowerment…. The delivery of services then becomes smarter for those who are sensed accurately, but faulty predictions and un-sensed needs are problems.

The broadband adoption experience teaches that we should have technology adoption strategies for (consumer-facing) IoT systems that aim at full participation. Blair Levin, a Fellow in the Aspen Institute Communications and Society Program, worried that the IoT "is not a very attractive vision, particularly for the under-adopting community" because it's about things. He thought that proponents need to communicate a vision of the collective goods that are created, and not just private or consumer goods. There must be a narrative about the IoT that is about more than smart toasters and smart energy. The IoT must not only respect privacy but also give people agency, a sense that they're empowered to contribute and an understanding about how personal inputs create a desirable broader outcome.

In order to make the IoT interesting to low adopters, there has to be data that's relevant to those communities. Shawn Chang also emphasized respect: "You can't just come into a community and tell them: 'This is what you need and this is the value proposition for you.'" It's important to empower leaders within communities to demonstrate the benefits of adoption and to shape the kinds of sensor networks that are developed.

Data discrimination is a big concern, as noted in the White House report on big data.[40] The IoT produces data from an ever expanding array of sources and experiences. As big data becomes bigger, data correlations that could lead to discriminatory actions become ever more difficult to understand or even identify.[41] Nicole Turner-Lee, Vice President and Chief Research & Policy Officer of the Minority Media and Telecommunications Council, urged consideration of economic disparities when it comes to the IoT. The Fitbit device that tracks exercise, diet and sleep patterns is being used to lower insurance premiums or create other entitlements.[42] What happens to the poor, the chronically ill and others who, for whatever reason, are not introduced to these technologies? Jonathan Barzilay, Director of Freedom of Expression at the Ford Foundation, urged, "If there is some health benefit that derives from having a home or body that is connected to the IoT, we have to ask who gets to participate in that benefit?" This is a matter of fairness, but also efficiency. Where there are network effects, everyone gets better when anyone gets better. For example, Barzilay pointed out that "if there's a highway where one-third of the cars have perfect information and two-thirds that are distracted and confused, you're not actually going to realize the benefits."

Turner-Lee raised the difficulty of distinguishing between the mere convenience and the necessity of participating in the IoT. When a public benefits agency requires its beneficiaries to wear a Fitbit, the choice about IoT ceases to be a real choice, but a matter of health care. She thinks that the energy sector provides an excellent opportunity to address the issue of how the IoT can be used to foster equity among consumers: "Low income families spend about 35 percent of their net income on their energy bill, and people on fixed income rely upon stable energy pricing in order to make ends meet. The energy industry is still relatively highly regulated. Therefore, government has some leverage here to make the IoT work in ways that bring economic benefits to the most people."

She noted that in some areas, there are vertically integrated utilities that have a lot of rich data that is not being put to the best use. How can that data be opened up? Another source of opportunity is the technology shift that's already happening to smart grids, smart meters and other power-saving incentives. Julia Johnson observed that "we're seeing a friction between environmental groups and low income

groups, because low income groups believe that most of the advances being proposed to help the environment will negatively impact their ability to pay their bills and then be productive citizens." We should think about how IoT data might show that some existing energy pricing mechanisms are regressive, while other new mechanisms could benefit the environment and low-income communities at once. This would be "a real win/win."

"The Internet of Things cannot be all that it should be unless everybody is on…." — *Blair Levin*

Broadband adoption and inclusion efforts not only inform our understanding of the IoT future; broadband access and adoption are prerequisites for equitable IoT deployment. Returning to a central plank in the broadband adoption platform, Aspen Fellow Blair Levin urged that governments use the IoT as another prompt to ensure agencies adopt a digital-first strategy to move all government services to digital, thereby spurring digital adoption: "The Internet of Things cannot be all that it should be unless everybody is on, and we have to get everybody on the Internet before everyone is on the IoT, and getting everybody on requires digital readiness, not just connectivity." A Brookings Institute report, *Getting Smarter About Smart Cities*, similarly concluded that smart cities have to prioritize broadband and educational inclusion.[43] Recent efforts to extend the functionality and reach of public libraries have similarly emphasized the role of community anchor institutions in democratizing technological advances.[44] Several Conference participants emphasized the potential role of anchor institutions in making IoT innovations available and meaningful to community members who trust and have access to local health clinics, schools and libraries.

To avoid the retrofitting that has characterized the Internet with respect to disabled access, Fernando Laguarda, Time Warner Cable's Vice President, External Affairs and Policy Counselor, stressed the importance of designing accessibility into the IoT from the start: "There's a lot of benefit to the government's getting in early to establish the importance of inclusion, accessibility and engineering design principles that foster inclusion."

For example, the IoT presents great opportunities to design sensor networks for medical telemetry in ways that make services more accessible for individuals with disabilities. Touch screens may be difficult to manipulate, and if these concerns were considered in advance, we could design intelligent home products and services that are accessible for everyone, and we would have a better deployment when it comes to being able to include a community that depends a lot on automation. Danny Weitzner of the MIT CSAIL Decentralized Information Group argued that accessibility does not need to be engineered from scratch: "What you really want is to make sure that IoT apps have general web accessibility (HTML5) compliance built into them."

Kevin Werbach, Associate Professor of Legal Studies at the Wharton School, said he was concerned that masses of IoT-generated data increase the dangers of institutions acting in a discriminatory or anti-competitive manner. The risk was of "algorithmic monopolies"—a topic of heated discussion in big data and digital platform regulatory debates. There was some pushback coming from Marjory Blumenthal of the President's Council on Science and Technology and Danny Weitzner about the focus on algorithms as an object of regulatory interest rather than the anti-competitive or discriminatory behaviors they might abet.

Equity, Inclusion and Opportunity Recommendations

Basic Principles: (1) Inclusion by design should be built into IoT systems to ensure accessibility to disabled and underserved; (2) IoT rollouts should benefit the entire population and small businesses.

- The federal government should convene engineers/user groups to develop specifications for inclusion by design, including accessibility specifications. Industry should be encouraged to adopt these specs and the government should use them for procurement.
- SBA, NIST and the Manufacturing Extension Partnership should initiate a Startup America initiative around the IoT, including coordination with state and local economic development groups to develop actionable market intelligence for small business.

- IoT participation incentives should be directed in a way that promotes social inclusion (e.g., energy credits).
- The IoT rollout must avoid technology redlining.
- Cities need narratives about how IoT systems benefit the public in terms of economic, social and civic advancement.

Civic Engagement

Social inclusion is one concern in rolling out the IoT, lest segments of the population be left behind. Civic participation is another concern, lest new IoT technologies fail to realize their potential for increasing democratic accountability. How can we use IoT-connected devices to enable and promote civic engagement?

Communications and Society Fellow Blair Levin suggested that "you actually want to see if all of this technology that we're creating does something to improve the way we collectively build the human enterprise." Citizen engagement should be at the forefront so that when government or even the private sector deploys sensor networks, they should be thinking about how to build in opportunities for citizen feedback about how their institutions and services are being run. This is like the "talk back" or comment component of the Internet. One might think of it as "feedback by design."

The IoT can transform the availability of feedback, moving away from mere civic petitioning.

Stefaan Verhulst of NYU's GovLab saw the challenge in this way: "How can we empower citizens to use the wearables that they already have to increase and improve the services that are delivered to them?" The IoT can transform the availability of feedback, moving away from mere civic petitioning. "We can also use these sensors for co-creation so that we actually can start developing improved services themselves and share feedback."

David Hoffman of Intel connected the issue of citizen engagement to privacy controls. He noted that "the same kinds of interfaces that would allow people to express their feedback about the cleanliness of public bathrooms could also be used to express choices about how people want their data to be collected from a privacy perspective." For example, Intel has made a large investment in a headphone company. A new earbud product will be able to read a lot of information about individuals and their health data, as well as information about the surrounding environment, including noise levels. One could imagine that government would like that information in order to assess noise pollution in particular areas. We might want a principle that prevents the government from collecting that data without individual consent. We might also want to engage citizens in a discussion about what amount of noise pollution is unacceptable.

Reed Hundt of the Coalition for Green Capital provided an example of how the IoT could transform regulatory compliance. For example, the FCC is increasingly unable to monitor compliance with its rules. Hundt posited a net neutrality rule that all consumers who pay for a certain broadband speed are entitled to get all their content at that speed. There could be a requirement that consumer devices record broadband speeds and report back to a centralized hub, allowing regulators and service providers (and consumers) to know when the rule is violated.

Citizen Engagement Recommendations

Basic Principles: IoT systems should engage citizens in making their governments more accountable and technology deployment more useful.

- Governments should experiment with pilot projects to enable immediate citizen feedback to government services, using push polls and sensor data. The feedback will inform government on experiments in the IoT such as location-based service delivery systems and IoT in public places. It will enable citizens as sensors to provide actionable intelligence on matters of importance to them.
- Citizens should be empowered to use wearables to improve services.

Telecommunications Network Architecture

IoT network technology that is open may better promote competition and service innovation. On the other hand, many applications may be so embedded in industrial applications that interoperability is unnecessary and merely exposes systems to added expense and insecurity. Most likely, the ecosystem will be a mixture of open and closed systems, but the appropriate mixture and the points of possible intervention present a governance challenge.

Government has long played a convening role that can help to promote interoperability using the U.S. voluntary standard setting context. The White House Office of Science and Technology Policy has demonstrated the capacity and interest to convene parties to discuss innovation issues, including interoperability. The Commerce Department's National Institute of Standards and Technology (NIST) can make an important contribution. Marjory Blumenthal, Executive Director of the President's Council on Science and Technology, said NIST should be encouraged "to play a role in global standards setting because we don't want to be in a situation where somebody else in another country with a different economic structure and different innovation base is trying to push standards on us."[45]

Most IoT connectivity will be conducted over wireless networks. Werbach of the Wharton School noted that wireless capabilities designed for 300 million mobile phones will have to scale to accommodate 50 billion IoT devices. We will also depend on wired infrastructure to move more data and move it farther.

The majority of connected things will place trivial demands on the network. Columbia University's Eli Noam noted that most IoT applications will generate only "a trickle" of data, which he estimated for the United States being no more than 200 gigabits per second: "The entire machine-to-machine bursty traffic will be less than my Manhattan apartment building's traffic on Netflix at night." Noam acknowledged that there will be applications, like security cameras and telemetry, which will place more substantial demands on the network. Continuity of data transmission will also vary hugely. Some IoT applications will transmit constantly, for example video cameras, while others will be intermittent. It is this heterogeneity that makes network configuration complicated.

Another network challenge is interoperability. Do differential bandwidth demands argue for separate networks? For Noam, this is a desirable outcome. Noam suggested it would be preferable "to have different countries and different companies, different industry constellations" having different network arrangements competing with each other. For some applications, either for privacy (health) or national security (electrical grid), we would not want the equivalent of a public Internet for the IoT, he maintains. It is also very likely that providers of these applications will come very quickly to monopolize their verticals. Robert Atkinson of ITIF disagreed and noted that it should and will be interoperable IP traffic even if some data does not run on the public Internet. Atkinson observed that it isn't necessarily bad to have private networks. It all depends on the consequences.

Is it possible that network heterogeneity taken too far could frustrate competition and innovation? Are we better off with a real *Internet* of Things, with highly interconnected networks, connections across verticals (home, health, transport) and common platforms? As in other technology roll-outs, there are the trade-offs between having APIs being open to competing devices and locking users into a particular ecosystem. Conference participants' disagreement about the appropriate balance between interconnectivity and heterogeneity at the level of network architecture echoed other disagreements about open vs. proprietary data and data analytics and, of course, reflects fundamental differences about how best to promote innovation.

Is it better to have heterogeneous networks of things and distinct addressing systems around the world, or should there be some coordination and harmonization?

Privacy, security, cost, competition, innovation and access may all hang in the balance. A highly interconnected IoT could reduce costs, increase functionality and spur innovation and competition for applications that use common standards. On the other hand, the more

interconnected the IoT is, the greater are the privacy and security risks. There may be no reason for your car to speak to your refrigerator, and no reason that they should be using anything like common APIs or continuous addressing. On the other hand, society may have a greater interest in ensuring that pollution data gathered by disparate private and public sensor networks is made available in ways that make it useful for a wide array of health devices. European Union regulators have begun to ask whether it is better to have heterogeneous networks of things and distinct addressing systems around the world, or whether there should be some coordination and harmonization. The responses have been decidedly mixed.

Security

Given the vast interconnectivity of things envisioned, IoT development could increase security vulnerabilities at both the level of individual devices and at systemic levels. Scary scenarios have penetrated media narratives. Writers for the Showtime thriller *Homeland* scripted the remote murder of the fictional vice president by means of hacking into a cardiac device.[46] Researchers have shown that they can remotely hack into an automobile to control the car's basic functions.[47] Real hackers had no trouble getting into the connected home security cameras of TRENDnet's SecurView in 2013. In a Federal Trade Commission enforcement action, the government found that a system marketed as "secure" was in fact run on faulty software that left cameras open to online viewing, and in some cases listening, by anyone with the cameras' Internet address.[48]

A recent Hewlett Packard study of the 10 most popular consumer IoT applications revealed that most of these devices had security vulnerabilities ranging from insufficiently strong password protection to lack of encryption. Most collected some form of personal information, such as name, address, date of birth, health information and even credit card numbers, and then connected this data flow to the cloud. Once this information is transmitted unencrypted on a home network, "users are one network misconfiguration away from exposing this data to the world via wireless networks."[49]

In 2008, the National Intelligence Council released a study of long-term risks to U.S. national security interests. The IoT was one of them. Its study modeled different implementation and adoption scenarios of the IoT and found opportunities and risks. Starting with the opportunities, it found that "if the United States executes wisely, the IoT could work to the long-term advantage of the domestic economy and to the U.S. military. Streamlining—or revolutionizing—supply chains and logistics could slash costs, increase efficiencies and reduce dependence on human labor." It went on to note that the "ability to fuse sensor data from many distributed objects could deter crime and asymmetric warfare."[50]

The report also offered this view of the future:

> [B]y 2025, robotic supply chains are common and considered more secure and less prone to human tampering than traditional shipping and receiving. At ports, containers report their contents to heavy equipment, which routes goods to trucks automatically; at distribution points, pallets and forklifts similarly communicate and route goods which arrive in stores largely untouched by human hands. RFIDs in individual food packages drive popular adoption of RFID readers in cell phones that provide an indication of food origins and provenance.[51]

But there are also risks. The very same technologies that are adopted to reduce security risks may actually exacerbate them. These technologies may make supply chains more vulnerable as mission-critical material arriving on U.S. shores are contaminated by malware. The study warned that "an open market for aggregated sensor data could…help criminals and spies identify vulnerable targets." Despite best efforts, "We may be unable to deny access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals and mischief makers. Foreign manufacturers could become both the single-source and single-point-of-failure for mission-critical Internet-enabled things. Manufacturers could also become vectors for delivering everyday objects containing malicious software that causes havoc in everyday life."[52]

Conference participants expressed concern about these and other security vulnerabilities. They considered whether IoT systems and device providers should have to make security vulnerability notifications, similar to data breach notifications that many states require today for large data processors.[53] So, for example, if the vendor of auto-

matic license plate readers finds that there's a vulnerability and the system is hackable, it would have to notify the authorities and the public. Participants also discussed the possibly of a product liability framework around IoT devices. Generally, software, as a service, is excluded from product liability regimes, which focus on goods. The IoT combines the software service and the hardware good into a single actuator and, therefore, clouds the distinction between goods and services.

Intel's David Hoffman raised the issue of large appliances that are connected to the IoT but not replaced as frequently as the Internet devices most used today. In these cases, there will be many devices whose software cannot be adequately updated and thus present a problem for the entire network. He proposed a rule to sunset these devices before they can export their vulnerabilities into the network: "If the devices are not affirmatively renewed, they should die at some point."

The 2015 FTC report on the Internet of Things noted that for many IoT devices "if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch."[54] A leading scholar of the IoT has proposed as a central governance principle that devices "should have some knowledge about their own functionality and be able to 'call for help' in case of failure."[55]

IoT security vulnerabilities start at the point of data collection. Most of the sensors currently deployed are simply not capable of establishing an encrypted link for communications because they have been designed to optimize battery power and minimize computing requirements. This is the finding of the EU's Article 29 Data Protection Working Party.[56] FTC Chairwoman Edith Ramirez emphasized that "data security is huge when it comes to the Internet of Things. As a general matter, companies today are not doing enough on this front. Government needs to set standards."

Security Recommendations

Basic Principles: (1) Device reliability; (2) data integrity; and (3) safety for active systems

- IoT systems should adopt security-by-design principles, deploying risk-based security measures.

- Governments should continue to develop protection, disaster response and redundancy plans for critical-infrastructure, focusing on the special threats that the IoT poses.
- The private sector and government should adopt expiration dates for autonomous IoT devices.
- There should be NIST standards development for safety and security practices, including resilience after a breach (e.g., cybersecurity framework, encryption).

The Smart City Use Case

Municipal deployment of IoT technologies to improve the efficiency and quality of service delivery is among the most developed use cases for the IoT. The "smart city" also raises some of the most pointed policy questions and presents early opportunities to get these policies right.

The term "smart city" usually refers to the use of ubiquitous sensors within urban infrastructure to generate data about usage patterns and service needs.[57] And it is also the umbrella term for more sector-specific notions of "smart growth," tools like the "smart grid" and many other "smart" innovations for urban prosperity and livability. Smart city initiatives cover the waterfront, from civic engagement, sustainability and transportation to education, telecommunications and health services.[58]

In Europe, the "smart city" has quasi-official status, with the European Parliament ranking cities in 28 nations based on performance in governance, human flourishing, livability, mobility, economy and environment. The UK has created a smart cities office to promote the synthesis of "hard infrastructure, social capital including local skills and community institutions, and (digital) technologies to fuel sustainable economic development and provide an attractive environment for all."[59] In the United States, the President's Council of Advisors on Science and Technology has held meetings on smart cities and technological implementation.

Although imprecise, these conceptions of the smart city all share two features: They emphasize public-private partnerships and place information and communications technologies (ICT) at the core of smart urban operation.[60] The smart city seeks "to address public issues via

ICT-based solutions on the basis of a multi-stakeholder, municipally based partnership."[61] In the ideal smart city, robust Internet connectivity and big data analytics support the delivery of services and creation of opportunity, enabling residents to live in more sustainable, productive, healthy and civically engaged ways.[62]

In the ideal smart city, robust Internet connectivity and big data analytics support the delivery of services and creation of opportunity, enabling residents to live in more sustainable, productive, healthy and civically engaged ways.

Benefits of the Smart City

Bob Pepper, Vice President of Global Technology Policy for Cisco Systems, presented Cisco's vision of the smart city and the results of its partnership with the city of Barcelona: "What makes a city smart is that it recognizes the central importance of technology and information to improve its processes." Technology fundamentally becomes part of a city's strategic vision and mission. Barcelona has realized cost-savings by using sensor networks to improve the efficiency of ordinary city services like "traffic management, trash collection, public safety policing, road management, road maintenance and snow removal."

For example, sensor networks tell the sanitation department when a trash bin is full and should be emptied. Until it's full, no truck needs to stop. Pepper continued, "Barcelona has saved $58 million a year on its connected water management by identifying where there's leakage and where there are spills. The city's connected street lighting has already reduced those bills by 33 percent, or $37 million a year. Barcelona's parking revenue has already increased by about $50 million a year while also reducing emissions, because 30 percent of congestion in a city is people driving around looking for parking places." San Francisco is experimenting with the same system. IBM has undertaken a public-private partnership with Dade County, Florida, to use sensor networks and analytics to reduce water consumption by 20 percent.

Concerns About the Smart City

The literature on smart cities can be decidedly utopian. This is particularly true when it casts its gaze on new cities, like Sangdo, South Korea—built over the past decade with smart city technology at its core. There is also a dystopian strain in smart city commentary, which focuses on the dangers of surveillance and ways in which the prerogatives of data may increase the power of private corporations over public functions and public resources.[63]

Conference participants focused on the issue of "technology redlining." Shawn Chang, Chief Democratic Counsel of the U.S. House Committee on Energy and Commerce, expressed concern that many smart city applications depend on an equal distribution of technology that does not exist. In his words, there "are dark fibers in the cities that cannot be lit because of legal and other obstacles" and that has to be addressed.

FCC Commissioner Mignon Clyburn related the smart city challenge to the more general digital inclusion challenge: "The 29% of the public that aren't digitally enabled have to be part of the discussion." She thought that Chicago has managed to develop its urban technology vision "without leaving anybody behind." It has placed five technology schools in disadvantaged areas and attracted teens to libraries with offerings around innovation and makers labs.

Chicago issued a technology plan for the city in 2013, after convening public and private stakeholders.[64] Among its 28 initiatives are to implement policies and infrastructure that make the city a leader in environmental sensing, use data to drive public efficiency, increase and improve city data, research data-driven solutions to major urban challenges and support civic hackers. While not exclusively an IoT or smart cities agenda, IoT applications are important for implementation of the Chicago technology plan.

Then there are the privacy issues. It may be valuable to monitor buildings for heat loss as a way to enable more efficient building construction and energy use choices. However, the Electronic Privacy Information Center's Executive Director, Marc Rotenberg, worried that much of this monitoring can easily be linked to personally identifiable information. "These systems can be a form of mass surveillance, because you've got video cameras, you've got license plate readers,

you've got things that are hooked into Homeland Security that are performing public safety functions in an automated way."

The surveillance aspects of the smart city have a differential impact on different populations. Nicole Turner-Lee, Vice President and Chief Research & Policy Officer of the Minority Media and Telecommunications Council, observed that "a smart city for somebody who lives on the South Side of Chicago means more cameras to monitor your movement on the street. That's not necessarily something that people want to see in their community. They probably would rather see a connected library or connected park district."

"The stove piping of the smart city application, without integrating it with the smart citizen, is holding back a lot of the transformative impact."
— Stefaan Verhulst

Stefaan Verhulst, Co-Founder and Chief Research and Development Officer of the Governance Laboratory (GovLab) at NYU urged a more holistic approach to all digital initiatives and greater integration of the IoT with the "Internet of People." There is the e-government approach, which is all about technology and technology infrastructure for the ends of conducting city business online. Then there is the open government approach, which is quite often about open data. And then there is the social innovation approach, which is about crowd-sourced knowledge and citizen engagement. "At a certain point they all have to start working together. The stove piping of the smart city application, without integrating it with the smart citizen, is holding back a lot of the transformative impact."

Creating the Smart City

Creating smart cities poses problems of both leadership within particular cities and scaling innovation across cities. It takes strong leadership to implement smart city solutions. This is especially true where, as is often the case, the municipal department that realizes savings or additional revenue (e.g., streets or sanitation) may not be the depart-

ment that has to develop the systems to make it work. There has to be the will and wherewithal to invest capital in systems upfront that will be paid for out of operational expense savings over the longer term. In Barcelona, the executive has substantial power over municipal functions and the deputy mayor has been tasked with making the city smart.

Even where there is leadership and vision within a city, there is the problem of scaling solutions that work in one city to the more than 20,000 cities in the United States. Julia Johnson, President of Net Communications, worries that local governments lack the expertise and resources to implement innovative technology solutions. Kaseem Reed, Mayor of Atlanta, reportedly said in an earlier forum that if someone comes to him with a plan, the city can implement it, but the city does not have the expertise to fashion one. This willingness to partner raises questions about the role of industry in municipal governance and operations.

Reed Hundt, CEO of the Coalition for Green Capital, supposed that more than 90% of U.S. cities lack funds or IT competence to be in the smart city conversation: "Why shouldn't the federal government create a smart city in a box and give it to cities?" He raised the possibility of using FirstNet funds, as well as universal service funds, to support municipal IT systems and IoT systems. "Instead of us all admiring Chicago and Barcelona, why don't we just say that the federal government should create a 'smart city in a box' and give it to all 20,000 cities?" he asked. " Why should just the rich cities be smart cities?" In fact, Citymart in Europe and Bloomberg Philanthropies in the United States are trying to create and disseminate smart city tools to free cities from having to reinvent systems from scratch.

Robert Atkinson, Founder and President of The Information Technology and Innovation Foundation, observed that smart cities are really just cities that have smart implementations of technology. He thought one key role of the federal government should be to stoke competition among cities, help them override unions and other forms of resistance and help incentivize intermediary organizations that develop and deploy smart city applications (e.g., streetbump.org). "I think the role of the federal government could be to put out $500 million or so and have a competition in five cities that want to bid for that and transform everything at once, so that we can do the data analytics around it and open up the data."

Marjory Blumenthal, Executive Director of the President's Council on Science and Technology, emphasized the importance of "change agents" in spearheading technological innovation in government and in making competitive challenges effective. It was a Presidential Innovation Fellow who was behind the SmartAmerica Challenge—a White House effort to showcase smart city/IoT solutions. Intel's David Hoffman agreed that this kind of challenge accelerates municipal innovation. Intel participated in the SmartAmerica Challenge, focusing on job creation. "This is a great role for government," he said. This focus may be particularly important in the smart cities context because, as Joe Waz, Senior Strategic Advisor for Comcast Corporation, noted, cities are often reluctant to implement technology solutions because it puts them at odds with unions, which fear that technology will kill jobs.

Joanne Hovis, President of CTC Technology & Energy, thought that cities actually were capable of implementing many smart city ideas, but were not convinced of the value proposition. "Some of what seem to us as very clear and quantifiable benefits might seem a little bit more speculative from their standpoint." Shawn Chang, Chief Democratic Counsel of the U.S. House Committee on Energy and Commerce, observed that for cities to really participate in smart city initiatives, they will have to be able to leverage existing infrastructure resources like dark fiber.

Dale Hatfield, Adjunct Professor & Senior Fellow at the Silicon Flatirons Center, University of Colorado at Boulder, recommended the building of a reference architecture so cities know what they can do with different sources of sensor data. NIST has already taken steps in this direction, starting with its 2014 SmartAmerica Challenge, which organized an exposition to feature and "accelerate advances in the field by providing a venue for innovators to present concepts for interconnected [IoT] technology, programs and test beds to demonstrate the potential of improving the economy, fueling job creation, creating new business opportunities and saving lives."[65] The second step was the launch of NIST's Global Cities program, which seeks to build teams and partnerships worldwide to create an "IoT Global Connectivity Fabric Strategy of architectures and guidelines for interconnected 'systems of systems' and a common data exchange/data analytics model for large scale IoT deployments."[66]

Nicol Turner-Lee of the Minority Media and Telecommunications Council praised the MacArthur Foundation for its role in supporting the initial Chicago plan and thought this was a story about the role of philanthropy in convening stakeholders and funding smart cities.[67] When developing effective models, she urged that stakeholders focus on the "central core of what they're trying to accomplish. If it's economic development, stay in that lane."

Conclusion

There are outsized expectations for the Internet of Things—in both utopian and dystopian directions. Longtime theorist of technology Jeremy Rifkin predicts that the IoT and related systems will give individuals unprecedented control over the production of goods and services, and thereby the conduct of their lives.[68]

In a more humorous vein, Matt Honen writes for *Wired* a scenario in which the hapless homeowner is marooned in a dysfunctional connected home, with appliances rendered inoperable by obsolete operating systems, closed standards and security flaws.[69]

Each perspective is rooted in very different visions of where power lies in the IoT world, and each finds support as networked devices are rolled out. Sometimes the very same scenario can be used to support both visions. For example, there is the case of vehicles leased to subprime borrowers on the condition that the lender can remotely disable the ignition in the event of a late payment or default.[70] On the one hand, the system expands access to car loans. On the other hand, it raises questions about a "self-help" solution for lenders that allows for erroneous decisions and may leave borrowers literally stranded.

The Conference reflected a range of views about the promise and perils of the IoT and how policy can contribute to netting the most benefit from networked matter. There was greatest consensus among participants on some basic principles:

- Treat IoT data *itself* as infrastructure—an essential building block for all kinds of economic, social and civic activity.
- Design-in security controls that reduce threats to connected devices and systems, and ensure that these security controls can be kept current.

- Design-in privacy controls that minimize collection of personally identifiable information and effectuate Fair Information Practice Principles.
- Promote broad accessibility of data and data analytics, which will require interoperable standards in many parts of the IoT ecosystem.
- Government should promote adoption and diffusion of technology, including building out IoT capabilities when it invests in infrastructure (known as a "dig once" proposal).
- IoT systems should ensure accessibility for the disabled and underserved through inclusion by design.
- The IoT should act as a vehicle for citizen participation and empowerment.
- Government should promote common standards for smart cities and other applications.
- Government should use procurement powers and regulatory powers to promote privacy and security.

In testimony to Congress delivered months after the Conference, Intel advocated that the United States develop a national IoT strategy over the next three to five years.[71] Hopefully, the findings and recommendations of the Conference will be useful to any such strategic policy process.

Endnotes

1. Kevin Ashton, "That "Internet of Things" Thing," *RfiD Journal*, June 22, 2009. Available online: http://www.rfidjournal.com/articles/view?4986.

2. Bruce Sterling, *The Epic Struggle Of The Internet Of Things*, Moscow: Strelka Press, 2014.

3. OECD, "Machine-to-Machine Communications: Connecting Billions of Devices," OECD Digital Economy Papers, No. 192, OECD Publishing. Available online: http://dx.doi.org/10.1787/5k9gsh2gp043-en.

4. See http://www.gartner.com/technology/home.jsp.

5. Dave Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco White Paper, April 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

6. "Disruptive Technologies: Advances That Will Transform Life, Business, and the Economy," McKinsey Global Institute, May 2013. Available online: http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx.

7. Catherine Crump and Matthew Harwood, "Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything," ACLU Blog, March 25, 2014. Available online: https://www.aclu.org/blog/technology-and-liberty-free-speech-national-security/invasion-data-snatchers-big-data-and.

8. Flavio Bonomi et al., "Fog Computing and Its Role in the Internet of Things," *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, August, 2012. Available online: http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf.

9. The object naming service (ONS) is currently the basis for IoT. See Rolf H. Weber and Romana Weber, *Internet of Things: Legal Perspectives*, Zurich: Springer, 2010, 5–6.

10. Jayavardhana Gubbi et al., "Internet of Things: A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, 29 no. 7, (2013): 1649.

11. Rolf H. Weber, "Internet of Things—Governance Quo Vadis?" *Computer Law & Security Report* 29 no. 4 (2013): 341–347, doi:10.1016/j.clsr.2013.05.010.

12. Sterling, *The Epic Struggle of the Internet of Things.*

13. The U.S. Department of Homeland Security defines critical infrastructure as "the power we use in our homes, the water we drink, the transportation that moves us and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (http://www.dhs.gov/what-critical-infrastructure).

14. The Fair Information Practice Principles are a set of eight principles rooted in the Privacy Act of 1974, 5 U.S.C. § 552a, as amended (Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing). They have been adopted in many U.S. governmental programs and disseminated abroad through, among other vehicles, the OECD. See http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

15. See Executive Office of the President, President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* May 2014. Available online: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

16. Tom Goodwin, "Intimate Data Will Be Key to the Internet of Things: From New Screens to Flow Advertising, Messages Will Be More Personal," *Advertising Age*, February 6, 2015. Available online: http://adage.com/article/digitalnext/intimate-data-key-internet-things/297005/.

17. European Commission, *Report on the Public Consultation on IoT Governance*, January 16, 2013. Available online: http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.

18. FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World*, 2015. Available online: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

19. Deb Fischer et al., Letter to U.S. Senate Committee on Commerce, October 20, 2014. Available online: http://www.fischer.senate.gov/public/_cache/files/e0a5801e-e239-4db8-812f-b9843f111b7d/internet-of-things-commerce-hearing-letter-1-.pdf.

20. Executive Office of the President, *Big Data and Differential Pricing*, February 2015. Available online: http://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf.

21. Lily Bui, "A (Working) Typology of Sensor Journalism Projects," September 19, 2014. Available online: https://medium.com/@dangerbui/a-working-typology-of-sensor-journalism-projects-c0042a0410af.

22. On May 9, 2013, President Obama signed an executive order that made open and machine-readable data the new default for government information. The White House has also launched Project Open Data, designed to share best practices, examples and software code to assist federal agencies with opening data. See http://www.whitehouse.gov/open.

23. Michael Specter, "Climate by Numbers: Can a Tech Firm Help Farmers Survive Global Warming?" *The New Yorker*, 89 no. 36 (2013): 38. Available online: http://www.newyorker.com/magazine/2013/11/11/climate-by-numbers.

24. Nancy Scola and Andrea Peterson, "Data Is Uber's Business. But Protecting It May Be Its Biggest Weakness," *The Switch* (blog), *Washington Post*, November 18, 2014. Available online: http://www.washingtonpost.com/blogs/the-switch/wp/2014/11/18/data-is-ubers-business-but-protecting-it-may-be-its-largest-weakness/.

25. The features of a connected car are described here: Future of Privacy Forum, *The Connected Car and Privacy: Navigating New Data Issues*, 2014. Available online: http://www.futureofprivacy.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf.

26. Puneet Kishor, "Sensored City," n.d. Available online: http://science.creativecommons.org/sensoredcity/. *See also* SensingCity, "Project to Create 'Sensing Cities' Launches in Christchurch," September 4, 2013. Available online: http://www.sensingcity.org/stay-informed/project-to-create-'sensing-cities'-launches-in-christchurch.

27. In Kyllo v. United States [533 U.S. 27 (2001)], the U.S. Supreme Court found it to be an illegal search when the government used an infrared thermometer to measure the temperature of the exterior of a house suspected of containing a Marijuana grow room.

28. See President's Council of Advisors on Science and Technology, *Big Data and Privacy*, 48.

29. Ovidiu Vermesan and Peter Fries, eds., *Internet of Things – From Research and Innovation to Market Deployment,* Aalborg, Denmark: River Publishers, 2014, 92. Available online: http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf.

30. See Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values,* May 2014. Available online: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

31. FTC, *Internet of Things: Privacy & Security in a Connected World.*

32. Gubbi, "Internet of Things," 1646.

33. FTC, *Internet of Things: Privacy & Security in a Connected World.*

34. *Mauritius Declaration on Internet of Things*, 36th Annual Conference of Data Protection and Privacy Commissioners, October 14, 2014. Available online: http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf.

35. See President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* 38.

36. Weber and Weber, *Internet of the Things,* 39.

37. Julia Angwin, *Dragnet Nation: A Quest for Privacy Security and Freedom in a World of Relentless Surveillance*, New York: Henry Holt, 2014.

38. "Cisco Technology Radar," Cisco Systems, December 2014. Available online: https://techradar.cisco.com/pdf/cisco-technology-radar.pdf.

39. The Fair Information Practice Principles are a set of eight principles rooted in the Privacy Act of 1974, 5 U.S.C. § 552a, as amended (Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing). They have been adopted in many U.S. governmental programs and disseminated abroad through, among other vehicles, the OECD. See http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

40. President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective.*

41. See for example Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Change How We Live, Work and Think*, New York: Houghton Mifflin, 2013; Omer Tene and Jules Polonetsky, "Judged by the Tin Man: Individual Rights in the Age of Big Data," *Journal of Telecommunications and High Technology Law*, 11 no. 2, 2013, 351.

42. Parmy Olson, "The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business," Forbes, April 17, 2014. Available online: http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/.

43. Brookings Institution, *Getting Smarter About Smart Cities*, Washington, 2014. Available online: http://www.brookings.edu/~/media/Research/Files/Papers/2014/04/smart%20cities/BMPP_SmartCities.pdf.

44. Ellen P. Goodman, " 'Smart Cities' Meet 'Anchor Institutions': The Case of Broadband and the Public Library," 2014. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2476159.

45. NIST established a cyber-physical systems public working group in June 2014. The working group is composed of four subgroups: cybersecurity and privacy; definitions, taxonomy and reference architecture; use cases; and timing and synchronization.

46. The writers may have been inspired by a real-life scenario. The doctor for then-Vice President Dick Cheney insisted that the wireless feature of Cheney's implanted defibrillator be disconnected, for fear that terrorists would hack into it. See Denise Schrier Cetta and Maichael Radutzky (producers), "Dick Cheney's Heart," *60 Minutes* (CBS), Oct. 20, 2013. Available online: http://www.cbsnews.com/news/dick-cheneys-heart/.

47. John Markoff, "Researchers Show How a Car's Electronics Can Be Taken Over Remotely," *New York Times*, March 9, 2011. Available online: http://www.nytimes.com/2011/03/10/business/10hack.html?_r=2&.

48. "In the matter of Trendnet, Inc." Federal Trade Commission consent order no. 122 3090, 2013. Available online: http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetorder.pdf.

49. Craig Smith and Daniel Miessler, *Internet of Things Research Study*, HP Fortify, June 2014. Available online: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

50. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025*, CR 2008-07, 2008, v. Available online: http://fas.org/irp/nic/disruptive.pdf.

51. Ibid., 30.

52. Ibid., 27.

53. See generally, Scott R. Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent," *Texas Law Review*, 93 no. 1 (2014): 1–84. Available online: http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf.

54. FTC, *Internet of Things*, 13. See also Bruce Schneier, "The Internet of Things is Wildly Insecure – And Often Unpatchable," *Wired*, January 6, 2014. Available online: http://wired.com/2014/01/theres-no-good-way-to-patch-the-interent-of-things-and-thats-a-huge-problem.

55. Weber, "Internet of Things – Governance Quo Vadis?" 346.

56. Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things*, 2014, 9. Available online: http://ec.eduopa.edu/justice/data-protection/article-29/documentation.opinion-recommendation/files/2014/wp223_en.pdf.

57. IDC Government Insights, *Smart Cities and the Internet of Everything: The Foundation for Delivering Next-Generation Citizen Services*, White Paper #GI243955, Alexandria, VA, 2013. Available online: https://www.cisco.com/web/strategy/docs/scc/ioe_citizen_svcs_white_paper_idc_2013.pdf. IBM has a branded "smarter cities" initiative to produce data management systems for the delivery of city services, from police work to trash collection. See http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/.

58. See, for example, Taewoo Nam and Theresa A. Pardo, "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions," *The Proceedings of the 12 Annual International Conference on Digital Government Research*, College Park, MD, 2011. Available online: http://www.ctg.albany.edu/publications/journals/dgo_2011_smartcity/dgo_2011_smartcity.pdf; Paul Foley, "Defining Smart Cities," Digital Agenda for Europe, May 31, 2013. Available online: http://ec.europa.eu/digital-agenda/en/content/defining-smart-cities.

59. UK Department for Business Innovation and Skills, *Smart Cities Background Paper*, 2013, 7. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246019/bis-13-1209-smart-cities-background-paper-digital.pdf.

60. Robert G. Hollands, "Will the Real Smart City Please Stand Up?" City, 12 no.3, (2008): 303–320; L. Anthopoulos and P. Fitsilis, "Digital to Ubiquitous Cities: Defining a Common Architecture for Urban Development", *Proceedings of the 6th International Conference on Intelligent Environments*, Kuala Lumpur, Malaysia, July, 2010, doi: 10.1109/IE.2010.61.; Rosabeth Moss Kanter & Stanley S. Litow, *Informed and Interconnected: A Manifesto for Smarter Cities*, Harvard Business School Working Paper, 09-141, 2009. Available online: http://www.hbs.edu/faculty/Publication%20Files/09-141.pdf; European Parliament, *Mapping Smart Cities in the EU,* 2014. Available online: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

61. European Parliament, *supra*, note 16 at 9.

62. Anthony Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia,* New York: Norton, 2013.; Emmanouil Tranos and Drew Gertner, *Smart Networked Cities? Innovation: The European Journal of Social Science Research* 25 no. 2, (2012), 176–177; Rosabeth Moss Kanter & Stanley S. Litow, *Informed and Interconnected: A Manifesto for Smarter Cities*, Harvard Business School Working Paper, 09-141, 2009. Available online: http://www.hbs.edu/faculty/Publication%20Files/09-141.pdf.

63. Adam Greenfield, *Against the Smart City*, New York: Do Projects, 2013.

64. *City of Chicago Technology Plan*, September 2013. Available online: http://techplan.cityofchicago.org/.

65. NIST, SmartAmerica Expo, June 27, 2014. Available online: http://www.nist.gov/el/smartamerica.cfm.

66. NIST, Global City Teams Challenge—SmartAmerica Round Two, August 25, 2014. Available online: http://www.nist.gov/cps/sagc.cfm.

67. See Sean Thornton, *The Smart Chicago Collaborative: A New Model for Civic Innovation in Cities, Data-Smart City Solutions*, Dec. 2, 2013. Available online: http://datasmart.ash.harvard.edu/news/article/the-smart-chicago-collaborative-a-new-model-for-civic-innovation-in-cities-. Chicago is also the recipient of a Bloomberg Philanthropies Mayors Challenge, http://mayorschallenge.bloomberg.org/index.cfm?objectid=7E9F3B30-1A4F-11E3-8975000C29C7CA2F.

68. Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, New York: Palgrave Macillan, 2014.

69. Mat Honen, "The Nightmare on Connected Home Street," *Wired*, June 13, 2014. Available online: http://www.wired.com/2014/06/the-nightmare-on-connected-home-street/.

70. Michael Corkery and Jessica Silver-Greenberg, "Miss a Payment? Good Luck Moving That Car," *New York Times*, September 24, 2014. Available online: http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_r=0.

71. Statement of Intel Corporation for the United States Senate Committee on Commerce, Science & Transportation on The Connected World: Examining the Internet of Things, Feb. 11, 2015. Available online: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=c88aece5-8769-4afd-8c51-81c69d961cb9.

APPENDIX

Developing Policies for the Internet of Things

August 13-16, 2014
Aspen, Colorado

Conference Participants

Robert Atkinson
Founder and President
The Information Technology and Innovation Foundation

Jonathan Barzilay
Director, Freedom of Expression
Ford Foundation

Marjory Blumenthal
Executive Director
President's Council on Science and Technology
White House Office of Science and Technology Policy

Michael Calabrese
Director, Wireless Future Program
Open Technology Institute
New America Foundation

Shawn Chang
Chief Democratic Counsel
U.S. House Committee on Energy and Commerce

Jonathan Chaplin
Managing Partner
New Street Research

Mignon Clyburn
Commissioner
Federal Communications Commission

Donna Epps
Vice President
Public Policy & Strategic Alliances
Verizon Communications

Charlie Firestone
Executive Director
Communications and Society Program
The Aspen Institute

Ellen Goodman
Professor
Rutgers University School of Law

Note: Titles and affiliations are as of the date of the conference.

Dale Hatfield
Adjunct Professor & Senior Fellow
Silicon Flatirons Center
University of Colorado at Boulder

Alex Hoehn-Saric
Senior Vice President, Regulatory
Charter Communications

David Hoffman
Director of Security Policy and
Global Privacy Officer
Intel Corporation

Joanne Hovis
President
CTC Technology & Energy and
Immediate Past President
NATOA

Reed Hundt
CEO
Coalition for Green Capital

Julia Johnson
President
Net Communications

Fernando Laguarda
Vice President, External Affairs and Policy Counselor
Time Warner Cable

Blair Levin
Fellow
Communications and Society Program
The Aspen Institute

Chris Libertelli
Vice President - Global Public Policy
Netflix

Eli Noam
Professor of Economics and Finance
Columbia Business School
Columbia University

Sarah Oh
Ph.D. Candidate, Economics
George Mason University

Emmett O'Keefe
Vice President, Federal Affairs
Cablevision

Robert Pepper
Vice President, Global Technology Policy
Cisco Systems

Carl Povelites
Assistant Vice President
Public Policy, Mobility
AT&T Services, Inc.

Lee Rainie
Director
Pew Internet & American Life Project

Note: Titles and affiliations are as of the date of the conference.

Edith Ramirez
Chairwoman
Federal Trade Commission

Marc Rotenberg
Executive Director
Electronic Privacy Information Center (EPIC)

Johanna Shelton
Director, Public Policy & Government Relations
Google

Alfredo Tímermans
CEO
Telefonica Internacional USA, Inc.

Nicol Turner-Lee
Vice President
and
Chief Research & Policy Officer
Minority Media and Telecommunications Council

Christine Varney
Attorney
Cravath, Swaine & Moore LLP

Stefaan Verhulst
Co-Founder
Chief Research and Development Officer
NYU Wagner School
Governance Laboratory (GovLab)

Joe Waz
Senior Strategic Advisor
Comcast Corporation

Danny Weitzner
Director
MIT CSAIL Decentralized Information Group

Kevin Werbach
Associate Professor of Legal Studies
Wharton School
University of Pennsylvania

Staff:

Ian Smalley
Senior Project Manager
Communications and Society Program
The Aspen Institute

Note: Titles and affiliations are as of the date of the conference.

About the Author

Professor Ellen P. Goodman, Rutgers University School of Law, is a public media and media policy expert. She co-directs and co-founded the Rutgers Institute for Information Policy and Law and teaches media law, copyright, intellectual property law, advertising law, animal law and property law. Professor Goodman has published extensively on media and spectrum policy, regulation through disclosure and advertising law in the *Cornell Law Review, Texas Law Review, Harvard Journal of Law & Technology,* and *Berkeley Journal of Law & Technology* among other journals and books.

In 2013-2014, she was a Senior Visiting Scholar at the London School of Economics and recently served as Distinguished Visiting Scholar with the Federal Communications Commission, responsible for the nonprofit media section of the landmark 2011 Information Needs of Communities Report. She has had visiting appointments at the University of Pennsylvania's Annenberg School of Communications, as well as Penn's Wharton School of Business and Law School and Bar Ilan University. Prior to joining the Rutgers faculty, Professor Goodman was a partner at Covington & Burling LLP, where she practiced in the information technology area.

A graduate of Harvard College and Harvard Law School, Professor Goodman was a law clerk for Judge Norma Shapiro on the federal court for the Eastern District of Pennsylvania. She lives near Philadelphia with her husband and three children.

About the Communications and Society Program

www.aspeninstitute.org/c&s

The Communications and Society Program is an active venue for framing policies and developing recommendations in the information and communications fields. We provide a multidisciplinary space where veteran and emerging decision-makers can develop new approaches and suggestions for communications policy. The Program enables global leaders and experts to explore new concepts, exchange insights, develop meaningful networks, and find personal growth, all for the betterment of society.

The Program's projects range across many areas of information, communications, and media policy. Our activities focus on issues of open and innovative governance, public diplomacy, institutional innovation, broadband and spectrum management, as well as the future of content, issues of race and diversity, and the free flow of digital goods, services, and ideas across borders.

Most conferences employ the signature Aspen Institute seminar format: approximately 25 leaders from diverse disciplines and perspectives engaged in a moderated roundtable dialogue, with the goal of driving the agenda to specific conclusions and recommendations. The program distributes our conference reports and other materials to key policymakers, opinion leaders, and the public in the United States and around the world. We also use the Internet and social media to inform and ignite broader conversations that foster greater participation in the democratic process.

The Program's Executive Director is Charles M. Firestone. He has served in this capacity since 1989 and also as Executive Vice President of the Aspen Institute. Prior to joining the Aspen Institute, Mr. Firestone was a communications attorney and law professor who has argued cases before the United States Supreme Court. He is a former director of the UCLA Communications Law Program, first president of the Los Angeles Board of Telecommunications Commissioners, and an appellate attorney for the U.S. Federal Communications Commission.

Select Publications from the Aspen Institute Communications Policy Project

Video Veritas: Building a 21st Century Video Platform for a High-Performance Society, by John B. Horrigan

The Twenty-Eighth Annual Aspen Institute Conference on Communications Policy focused on the future of video regulation. The resulting report, written by John B. Horrigan, looks at the changing landscape of video regulation and the fundamental shift in how video is being viewed. While cable and broadcast television continue to be the dominant modes of transmission, over the top delivery of content via the Internet provides new ways to distribute personalized and targeted programming directly to the viewer. This, and the proliferation of mobile devices and tablets can deliver video to the viewer anywhere, anytime. As a result, the advertising-based broadcast business model is undergoing significant challenge and change. This report examines the evolving video ecosystem and offers recommendations for policy that can accommodate the new video market. 2014, 54 pages, ISBN Paper: 0-89843-603-6, $12.00

Spectrum as a Resource for Enabling Innovation Policy,
by William Webb

The 2012 Aspen Institute Roundtable on Spectrum Policy (AIRS) convened shortly after the presidential election to consider ways that spectrum policy could improve the economy through innovation. The 32 leading communications policy experts in attendance focused on how spectrum policies could help create an environment that makes it easier to use spectrum as a resource for innovative new goods and services. The participants first identified problems facing new entry and innovation today, and then recommended solutions, looking specifically at the interstices among licensed and unlicensed approaches, spectrum sharing and flexibility, and new institutional arrangements to manage these solutions. The report, written by British spectrum expert William Webb, sets forth 11 recommendations that he gleaned from the conference dialogue

to guide future spectrum policy development with regard to facilitating innovation. 2013, 45 pages, ISBN Paper: 0-89843-584-6, $12.00

Rethinking Communications Regulation, by Richard Adler

As the Internet and other information and communications technologies grow exponentially, and as a new ecosystem is emerging that could conflate previously distinct methods of communication into a single digital medium, questions arise as to whether the traditional silos of regulation are still appropriate. The report resulting from the 27th Annual Aspen Institute Communications Policy Conference addresses the overarching concern as to whether the Communications Act needs a radical revision. Written by rapporteur Richard Adler, the report considers the key goals of a new communications regime and offers regulatory and non-regulatory approaches for achieving these goals in a digitally connected world. 2013, 65 pages, ISBN Paper: 0-89843-583-8, $12.00

The Reallocation Imperative: A New Vision for Spectrum Policy, by Preston Marshall

The report resulting from the 2011 Aspen Institute Roundtable on Spectrum Policy addresses new ways of allocating, clearing, using and/or sharing spectrum controlled by private parties and government agencies. Written by rapporteur Preston Marshall, the report attempts to step back and establish a broad vision for reallocating spectrum in the United States in the public interest, discussing new approaches that will facilitate more effective and efficient spectrum use. A number of recommendations are laid forth to guide future spectrum policy development, Congressional actions, and technology explorations. 2012, 54 pages, ISBN Paper: 0-89843-570-6, $12.00

Updating Rules of the Digital Road: Privacy, Security, Intellectual Property, by Richard Adler

Given the current growth and importance of the Internet, the report of the 2011 Aspen Institute Conference on Communications Policy titled *Updating Rules of the Digital Road: Privacy, Security, Intellectual Property*, highlights the elements that will allow for greater use of broadband as the common medium: security, privacy and intellectual property regulation. Written by rapporteur Richard Adler, the report explores

a range of threats that plague the use of today's communications media and provides a series of recommendations which aim to ensure that users' communications are secure, private and protected.

The report reflects the issues and ideas raised by business leaders, academics, and policy experts at the Twenty-Sixth Annual Aspen Institute Conference on Communications Policy. 2012, 70 pages, ISBN Paper: 0-89843-563-3, $12.00

Spectrum for the Next Generation of Wireless, by Mark MacCarthy

Spectrum for the Next Generation of Wireless explores possible sources of spectrum, looking specifically at incentives or other measures to assure that spectrum finds its highest and best use. It includes a number of recommendations, both private and federal, of where and how spectrum can be repurposed for wireless use. In November 2010, the Aspen Institute Communications and Society Program convened the Aspen Institute Roundtable on Spectrum Policy, where 31 experts and leaders addressed the consequences and solutions to the increasing demand for spectrum. Spectrum for the Next Generation of Wireless is the report resulting from the Roundtable discussions. 2011, 68 pages, ISBN Paper: 0-89843-551-X, $12.00

Rewriting Broadband Regulation, by David Bollier

The report of the 25th Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado, considers how the United States should reform its broadband regulatory system. Participants looked at international models and examples and examined how data and communications should be protected in the international arena. The resulting report explores a range of policies for U.S. broadband regulation, many of them derivative of the National Broadband Plan adopted by the Federal Communications Commission only a few months before the conference.

Participants also ventured into new and interesting territory with the novel concept of "digital embassies." They saw this as a way of dealing with jurisdictional issues associated with the treatment and protection of data in the cloud, i.e., data that is provided in one country but stored or manipulated in another. The concept is that the data would be treated throughout as if it were in a kind of virtual embassy, where the

citizenship of the data (i.e., legal treatment) goes along with the data. This policy seed has since been cultivated in various other regulatory environments. 2011, 37 Pages, ISBN Paper: 0-89843-548-X, $12.00

Scenarios for a National Broadband Policy, by David Bollier

The report of the 24th Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado, captures the scenario building process that participants used to map four imaginary scenarios of how the economy and society might evolve in the future, and the implications for broadband policy. It identifies how certain trends—economic, political, cultural, and technological—might require specific types of government policy intervention or action. 2010, 52 pages, ISBN Paper: 0-89843-517-X, $12.00

Rethinking Spectrum Policy: A Fiber Intensive Wireless Architecture, by Mark MacCarthy

Rethinking Spectrum Policy: A Fiber Intensive Wireless Architecture is the report resulting from the Aspen Institute Roundtable on Spectrum Policy, held at the Aspen Wye River Conference Center in November 2009. Written by rapporteur Mark MacCarthy, the report captures the insights of the participants, exploring innovative ways to respond to the projections of exponential growth in the demand for wireless services and additional spectrum. In addition to discussing spectrum reallocations, improved receivers, shared use and secondary markets as important components for meeting demand, the report also examines opportunities for changes in network architecture, such as shifting the mix between fiber and wireless. 2010, 58 pages, ISBN Paper: 0-89843-520-X, $12.00

ICT: The 21st Century Transitional Initiative, by Simon Wilkie

The report of the 23rd Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado addresses how the United States can leverage information and communications technologies (ICT) to help stimulate the economy and establish long-term economic growth. The report, written by Roundtable rapporteur Simon Wilkie, details the Aspen Plan, as developed in the summer of 2008, prior to the economic meltdown beginning in September 2008 and prior to the election of Barack Obama as President. The Plan recommends how

the Federal Government—through executive leadership, government services and investment—can leverage ICTs to serve the double bottom line of stimulating the economy and serving crucial social needs such as energy efficiency and environmental stewardship. 2009, 80 pages, ISBN Paper: 0-89843-500-5, $12.00

A Framework for a National Broadband Policy, by Philip J. Weiser

While the importance of broadband access to functioning modern society is now clear, millions of Americans remain unconnected, and Washington has not yet presented any clear plan for fixing the problem.

Condensing discussions from the 2008 Conference on Communications Policy and Aspen Institute Roundtable on Spectrum Policy (AIRS) into a single report, Professor Philip Weiser of the University of Colorado at Boulder offers a series of specific and concrete policy recommendations for expanding access, affordability, and adoption of broadband in the United States. 2008, 94 pages, ISBN Paper: 0-89843-484-X, $12.00

The Future of Video: New Approaches to Communications Regulation, by Philip J. Weiser

As the converged worlds of telecommunications and information are changing the way most Americans receive and relate to video entertainment and information, the regulatory regimes governing their delivery have not changed in tune with the times. These changes raise several crucial questions: Is there a comprehensive way to consider the next generation of video delivery? What needs to change to bring about a regulatory regime appropriate to the new world of video? The report of the 21st Annual Conference on Communications Policy in Aspen, Colorado, outlines a series of important issues related to the emergence of a new video marketplace based on the promise of Internet technology and offers recommendations for guiding it into the years ahead. 2006, 70 pages, ISBN Paper: 0-89843-458-0, $12.00

Clearing the Air: Convergence and the Safety Enterprise, by Philip J. Weiser

The report describes the communications problems facing the safety enterprise community and their potential solutions. The report offers several steps toward a solution, focusing on integrating communications across the safety sector on an Internet-Protocol-based backbone

network, which could include existing radio systems and thus make systems more dependable during emergencies and reduce costs by taking advantage of economies of scale. The conference participants stressed that the greatest barriers to these advances were not due to lagging technology but to cultural reluctance in adopting recent advances. Writes Weiser, "The public safety community should migrate away from its traditional reliance on specialized equipment and embrace an integrated broadband infrastructure that will leverage technological innovations routinely being used in commercial sectors and the military." 2006, 55 pages, ISBN Paper: 0-89843-4, $12.00

Reforming Telecommunications Regulation, by Robert M. Entman

The report of the 19th Annual Aspen Institute Conference on Telecommunications Policy describes how the telecommunications regulatory regime in the United States will need to change as a result of technological advances and competition among broadband digital subscriber lines (DSL), cable modems, and other players, such as wireless broadband providers. The report proposes major revisions of the Communications Act and FCC regulations and suggests an interim transitional scheme toward ultimate deregulation of basic telecommunications, revising the current method for universal service subsidies, and changing the way regulators look at rural communications. 2005, 47 pages, ISBN Paper: 0-89843-428-9, $12.00

Reports can be ordered online at *www.aspeninstitute.org/publications* or by sending an email request to *publications@aspeninstitute.org.*