The Internet of Things: An Overview

Understanding the Issues and Challenges of a More Connected World

OCTOBER 2015

Table of Contents

Executive Summary

The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.

At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Attention-grabbing headlines about the hacking of Internet-connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges remain and new policy, legal and development challenges are emerging.

This overview document is designed to help the Internet Society community navigate the dialogue surrounding the Internet of Things in light of the competing predictions about its promises and perils. The Internet of Things engages a broad set of ideas that are complex and intertwined from different perspectives. Key concepts that serve as a foundation for exploring the opportunities and challenges of IoT include:

- **IoT Definitions:** The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.

- **Enabling Technologies:** The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include *Ubiquitous Connectivity*, *Widespread Adoption of IP-based Networking*, *Computing Economics*, *Miniaturization*, *Advances in Data Analytics*, and the *Rise of Cloud Computing*.

- **Connectivity Models**: IoT implementations use different technical communications models, each with its own characteristics. Four common communications models described by the Internet Architecture Board include: *Device-to-Device, Device-to-Cloud, Device-to-Gateway*, and *Back-End Data-Sharing*. These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user.

- **Transformational Potential:** If the projections and trends towards IoT become reality, it may force a shift in thinking about the implications and issues in a world where the most common interaction with the Internet comes from passive engagement with connected objects rather than active engagement with content. The potential realization of this outcome – a “hyperconnected world” -- is testament to the general-purpose nature of the Internet architecture itself, which does not place inherent limitations on the applications or services that can make use of the technology.

Five key IoT issue areas are examined to explore some of the most pressing challenges and questions related to the technology. These include security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and development.

- **Security:** While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber attack and expose user data to theft by leaving data streams inadequately protected.

  The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

  As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.

- **Privacy:** The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services.

  Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

- **Interoperability / Standards:** A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet. The use of generic, open, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol) will support greater user benefits, innovation, and economic opportunity.

- **Legal, Regulatory and Rights:** The use of IoT devices raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The questions are wide in scope, and the rapid rate of change in IoT technology frequently outpaces the ability of the associated policy, legal, and regulatory structures to adapt.

  One set of issues surrounds crossborder data flows, which occur when IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing. Further, data collected by IoT devices is sometimes susceptible to misuse, potentially causing discriminatory outcomes for some users. Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses.

  While the legal and regulatory challenges are broad and complex in scope, adopting the guiding Internet Society principles of promoting a user's ability to *connect, speak, innovate, share, choose*, and *trust* are core considerations for evolving IoT laws and regulations that enable user rights.

- **Emerging Economy and Development Issues:** The Internet of Things holds significant promise for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others. As such, IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals.

  The broad scope of IoT challenges will not be unique to industrialized countries. Developing regions also will need to respond to realize the potential benefits of IoT. In addition, the unique needs and challenges of implementation in less-developed regions will need to be addressed, including infrastructure readiness, market and investment incentives, technical skill requirements, and policy resources.

The Internet of Things is happening now. It promises to offer a revolutionary, fully connected "smart" world as the relationships between objects, their environment, and people become more tightly intertwined. Yet the issues and challenges associated with IoT need to be considered and addressed in order for the potential benefits for individuals, society, and the economy to be realized.

Ultimately, solutions for maximizing the benefits of the Internet of Things while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible perils. Rather, it will take informed engagement, dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward.

Introduction

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy-efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network-enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost.[1] IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.

A number of companies and research organizations have offered a wide range of projections about the potential impact of IoT on the Internet and the economy during the next five to ten years. Cisco, for example, projects more than 24 billion Internet–connected objects by 2019;[2] Morgan Stanley, however, projects 75 billion networked devices by 2020.[3] Looking out further and raising the stakes higher, Huawei forecasts 100 billion IoT connections by 2025.[4] McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025.[5] While the variability in predictions makes any specific number questionable, collectively they paint a picture of significant growth and influence.

---

[1] For more information on IoT as it relates with those with disabilities see for example: Valerio, Pablo. "Google: IoT Can Help The Disabled." *InformationWeek*, March 10, 2015. http://www.informationweek.com/mobile/mobile-devices/google-iot-can-help-the-disabled/a/d-id/1319404; and, Domingo, Mari Carmen. "An Overview of the Internet of Things for People with Disabilities." *Journal of Network and Computer Applications* 35, no. 2 (March 2012): 584–96. doi:10.1016/j.jnca.2011.10.015.

[2] "Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI)." *Cisco*, 2015. http://cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

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

[4] "Global Connectivity Index." Huawei Technologies Co., Ltd., 2015. Web. 6 Sept. 2015. http://www.huawei.com/minisite/gci/en/index.html

[5] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

Some observers see the IoT as a revolutionary fully–interconnected "smart" world of progress, efficiency, and opportunity, with the potential for adding billions in value to industry and the global economy.[6] Others warn that the IoT represents a darker world of surveillance, privacy and security violations, and consumer lock–in. Attention-grabbing headlines about the hacking of Internet-connected automobiles,[7] surveillance concerns stemming from voice recognition features in "smart" TVs,[8] and privacy fears stemming from the potential misuse of IoT data[9] have captured public attention. This "promise vs. peril" debate along with an influx of information though popular media and marketing can make the IoT a complex topic to understand.

Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also will likely have varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe.

This overview document is designed to help the Internet Society community navigate the dialogue surrounding the Internet of Things in light of the competing predictions about its promises and perils. It provides a high-level overview of the basics of IoT and some of the key issues and questions that this technology raises from the perspective of the Internet Society and the core values we promote.[10,11] It also acknowledges some of the unique aspects of the Internet of Things that make this a transformational technology for the Internet.

As this is intended to be an overview document, we do not propose a specific course of action for ISOC on IoT at this time. Rather, we see this document as an informational resource and starting point for discussion within the ISOC community on IoT-related issues.

[6] Thierer, Adam, and Andrea Castillo. "Projecting the Growth and Economic Impact of The Internet of Things." George Mason University, Mercatus Center, June 15, 2015. http://mercatus.org/sites/default/files/IoT-EP-v3.pdf

[7] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." *WIRED*, July 21, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] "Samsung Smart TV's Voice Recognition Creates Privacy Concerns." *CBS This Morning*. CBS News, February 10, 2015. http://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/

[9] Bradbury, Danny. "How Can Privacy Survive in the Era of the Internet of Things?" *The Guardian*, April 7, 2015, sec. Technology. http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

[10] "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

[11] A wide range of papers and articles have been written on the topic of IoT. Readers interested in more detail beyond the scope of this paper should investigate the literature noted in the footnotes and in the Reference section at the end of this paper.

We organize this paper into three main sections:

- **What is the Internet of Things?**, which provides an overview of its origins, definitions, and technical connectivity models;
- **What issues are raised by the Internet of Things?**, which provides an introduction and discussion of concerns that have been raised about IoT, and;
- **For Further Information,** which provides additional information and pointers to efforts around the world addressing IoT issues.

What is the Internet of Things?

Origins, Drivers, and Applications

The term “Internet of Things” (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors.[12] Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) tags[13] used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items.

While the term “Internet of Things” is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use.[14] In the 1990s, advances in wireless technology allowed “machine–to–machine” (M2M) enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purpose–built networks and proprietary or industry–specific standards,[15] rather than on Internet Protocol (IP)–based networks and Internet standards.

Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet “device”—an IP–enabled toaster that could be turned on and off over the Internet—was featured at an Internet conference in 1990.[16] Over the next several years, other “things” were IP–enabled, including a soda machine[17] at Carnegie Mellon University in the US and a coffee pot[18] in the Trojan Room at the University of Cambridge in the UK (which remained Internet–connected until 2001). From these whimsical beginnings, a robust field of research and development into “smart object networking”[19] helped create the foundation for today’s Internet of Things.

---

[12] Ashton was working on RFID (radio-frequency identification) devices, and the close association of RFID and other sensor networks with the development of the IoT concept is reflected in the name of the RFID device company that Ashton joined later in his career: “ThingMagic.”

[13] “Radio-Frequency Identification.” *Wikipedia, the Free Encyclopedia*, September 6, 2015. https://en.wikipedia.org/wiki/Radio-frequency_identification

[14] “Machine to Machine.” *Wikipedia, the Free Encyclopedia*, August 20, 2015. https://en.wikipedia.org/wiki/Machine_to_machine

[15] Polsonetti, Chantal. “Know the Difference Between IoT and M2M.” *Automation World*, July 15, 2014. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m

[16] "The Internet Toaster." Living Internet, 7 Jan. 2000. Web. 06 Sept. 2015. http://www.livinginternet.com/i/ia_myths_toast.htm

[17] "The "Only" Coke Machine on the Internet." Carnegie Mellon University Computer Science Department, n.d. Web. 06 Sept. 2015. https://www.cs.cmu.edu/~coke/history_long.txt

[18] Stafford-Fraser, Quentin. "The Trojan Room Coffee Pot." N.p., May 1995. Web. 06 Sept. 2015. http://www.cl.cam.ac.uk/coffee/qsf/coffee.html

[19] RFC 7452, “Architectural Considerations in Smart Object Networking” (March 2015), https://tools.ietf.org/html/rfc7452

If the idea of connecting objects to each other and to the Internet is not new, it is reasonable to ask, "Why is the Internet of Things a newly popular topic today?"

From a broad perspective, the confluence of several technology and market trends[20] is making it possible to interconnect more and smaller devices cheaply and easily:

- *Ubiquitous Connectivity*—Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable''.

- *Widespread adoption of IP–based networking*— IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.

- *Computing Economics*— Driven by industry investment in research, development, and manufacturing, Moore's law[21] continues to deliver greater computing power at lower price points and lower power consumption.[22]

- *Miniaturization*— Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects.[23] Coupled with greater computing economics, this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.

- *Advances in Data Analytics*— New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.

- *Rise of Cloud Computing*– Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.

From this perspective, the IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectors – including automotive, healthcare, manufacturing, home and consumer electronics, and well beyond -- are considering the potential for incorporating IoT technology into their products, services, and operations.

[20] Other views on the converging market trends driving IoT's growth include Susan Conant's article "The IoT will be as fundamental as the Internet itself", available at http://radar.oreilly.com/2015/06/the-iot-will-be-as-fundamental-as-the-internet-itself.html and Intel Corporation's statement to U.S. House of Representatives hearing on IoT, available at http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf.

[21] Moore's Law is named after a trend observed by semiconductor pioneer Gordon Moore that the number of transistors per square inch on integrated circuits doubles roughly every two years, allowing more processing power to be placed into smaller chips over time.

[22] For a discussion about Internet device energy use and low power computing, see the lecture by Jon Koomey at the "How green is the Internet?" summit available at https://www.youtube.com/embed/O8-LDLyKaBM

[23] In addition to other technical advancements, miniaturization of electronic devices is also fueled by Moore's law.

In their report "Unlocking the Potential of the Internet of Things'', the McKinsey Global Institute[24] describes the broad range of potential applications in terms of "settings" where IoT is expected to create value for industry and users.

"Settings" for IoT Applications (Source: McKinsey Global Institute[25])		
Setting	**Description**	**Examples**
Human	Devices attached or inside the human body	Devices (wearables and ingestibles) to monitor and maintain human health and wellness; disease management, increased fitness, higher productivity
Home	Buildings where people live	Home controllers and security systems
Retail Environments	Spaces where consumers engage in commerce	Stores, banks, restaurants, arenas – anywhere consumers consider and buy; self-checkout, in-store offers, inventory optimization
Offices	Spaces where knowledge workers work	Energy management and security in office buildings; improved productivity, including for mobile employees
Factories	Standardized production environments	Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use and inventory
Worksites	Custom production environments	Mining, oil and gas, construction; operating efficiencies, predictive maintenance, health and safety
Vehicles	Systems inside moving vehicles	Vehicles including cars, trucks, ships, aircraft, and trains; condition-based maintenance, usage-based design, pre-sales analytics
Cities	Urban environments	Public spaces and infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring, resource management
Outside	Between urban environments (and outside other settings)	Outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation; real-time routing, connected navigation, shipment tracking

[24] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015. p.3. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

[25] *Ibid.*

Many organizations have developed their own taxonomies and categorizations of IoT applications and use cases. For example, "Industrial IoT'' is a term widely used by companies and associations to describe IoT applications related to the production of goods and services, including in manufacturing and utilities.[26] Others discuss IoT by device type, such as wearables[27] and appliances.[28] Still others focus on IoT in the context of integrated location-based implementations such as "smart homes" or "smart cities''.[29] Whatever the application, it is clear that IoT use cases could extend to nearly every aspect of our lives.

As the number of Internet-connected devices grows, the amount of traffic they generate is expected to rise significantly. For example, Cisco estimates that Internet traffic generated by non-PC devices will rise from 40% in 2014 to just under 70% in 2019.[30] Cisco also forecasts that the number of "Machine to Machine" ("M2M") connections (including in industrial, home, healthcare, automotive, and other IoT verticals) will rise from 24% of all connected devices in 2014 to 43% in 2019.

One implication of these trends is that over the next ten years we could see a shift in the popular notion of what it means to be "on the Internet''. As MIT Professor Neil Gershenfied noted, *"…*[T]he rapid growth of the World Wide Web may have been just the trigger charge that is now setting off the real explosion, as things start to use the Net''.[31]

In the popular mindset, the World Wide Web has almost become synonymous with the Internet itself. Web technologies facilitate most interactions between people and content, making it a defining characteristic of the current Internet experience. The Web-based experience is largely characterized by the active engagement of users downloading and generating content through computers and smartphones. If the growth projections about IoT become reality, we may see a shift towards more passive Internet interaction by users with objects such as car components, home appliances and self-monitoring devices; these devices send and receive data on the user's behalf, with little human intervention or even awareness.

IoT may force a shift in thinking if the most common interaction with the Internet -- and the data derived and exchanged from that interaction -- comes from passive engagement with connected objects in the broader environment. The potential realization of this outcome – a "hyperconnected world" -- is a testament to the general-purpose nature of the Internet architecture, which does not place inherent limitations on the applications or services that can make use of the technology.[32]

---

[26] Cicciari, Matt. "What's Missing from the Industrial Internet of Things Conversation? Software." Wired. http://www.wired.com/insights/2014/11/industrial-internet-of-things-software/

[27] "Internet of Things: Wearables." Application Developers Alliance. http://www.appdevelopersalliance.org/internet-of-things/wearables/

[28] Baguley, Richard, and Colin McDonald. "Appliance Science: The Internet of Toasters (and Other Things)." *CNET*, March 2, 2015. http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/

[29] "IEEE Smart Cities." IEEE, 2015. Web. 06 Sept. 2015. http://smartcities.ieee.org/

[30] "Cisco Visual Networking Index: Forecast and Methodology, 2014-2019." Cisco, May 27, 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

[31] "History of the Internet of Things- Postscapes." Postscapes, n.d. Web. 06 Sept. 2015. http://postscapes.com/internet-of-things-history

[32] For a further discussion about the fundamental characteristics of the Internet and its architecture see the Internet Society Paper "Internet Invariants: What Really Matters," available at http://www.internetsociety.org/internet-invariants-what-really-matters

Different Definitions, Similar Concepts

Despite the global buzz around the Internet of Things, there is no single, universally accepted definition for the term. Different definitions are used by various groups to describe or promote a particular view of what IoT means and its most important attributes. Some definitions specify the concept of the Internet or the Internet Protocol (IP), while others, perhaps surprisingly, do not. For example, consider the following definitions.

The Internet Architecture Board (IAB) begins RFC 7452,[33] "Architectural Considerations in Smart Object Networking'', with this description:

> *The term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called "smart objects,'' are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment.*

Within the Internet Engineering Task Force (IETF), the term "smart object networking" is commonly used in reference to the Internet of Things. In this context, "smart objects" are devices that typically have significant constraints, such as limited power, memory, and processing resources, or bandwidth.[34] Work in the IETF is organized around specific requirements to achieve network interoperability between several types of smart objects.[35]

Published in 2012, the International Telecommunication Union (ITU) ITU–T Recommendation Y.2060, *Overview of the Internet of things*,[36] discusses the concept of interconnectivity, but does not specifically tie the IoT to the Internet:

> *3.2.2 Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*
>
> *Note 1—Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.*
>
> *Note 2—From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.*

[33] RFC 7452, "Architectural Considerations in Smart Object Networking" (March 2015), https://tools.ietf.org/html/rfc7452

[34] Thaler, Dave, Hannes Tschofenig, and Mary Barnes. "Architectural Considerations in Smart Object Networking." IETF 92 Technical Plenary - IAB RFC 7452. 6 Sept. 2015. Web. https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf

[35] "Int Area Wiki - Internet-of-Things Directorate." *IOTDirWiki*. IETF, n.d. Web. 06 Sept. 2015. http://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

[36] "Overview of the Internet of Things." ITU, June 15, 2012. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

This definition in a call for papers for a feature topic issue of IEEE Communications Magazine[37] links the IoT back to cloud services:

> *The Internet of Things (IoT) is a framework in which all things have a representation and a presence in the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represents the baseline communication that enables the interactions between Things and applications in the cloud.*

The Oxford Dictionaries[38] offers a concise definition that invokes the Internet as an element of the IoT:

> *Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.*

All of the definitions describe scenarios in which network connectivity and computing capability extends to a constellation of objects, devices, sensors, and everyday items that are not ordinarily considered to be "computers''; this allows the devices to generate, exchange, and consume data, often with minimal human intervention. The various definitions of IoT do not necessarily disagree – rather they emphasize different aspects of the IoT phenomenon from different focal points and use cases.

However, the disparate definitions could be a source of confusion in dialogue on IoT issues, particularly in discussions between stakeholder groups or industry segments. Similar confusion was experienced in recent years about net neutrality and cloud computing, where different interpretations of the terms sometimes presented obstacles to dialogue. While it is probably unnecessary to develop a single definition of IoT, it should be recognized that there are different perspectives to be factored into discussions.

For the purposes of this paper, the terms "Internet of Things" and "IoT" refer broadly to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers. These "smart objects" require minimal human intervention to generate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities.

Networking and communications models for smart objects include those where exchanged data does not traverse the Internet or an IP-based network. We include those models in our broad description of "Internet of Things" used for this paper. We do so as it is likely that the data generated or processed from those smart objects will ultimately pass through gateways with connectivity to IP-based networks or will otherwise be incorporated into product features that are accessible via the Internet. Furthermore, users of IoT devices are likely to be more concerned with the services delivered and the implication of using those services than issues of when or where data passes through an IP-based network.

---

[37] http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps

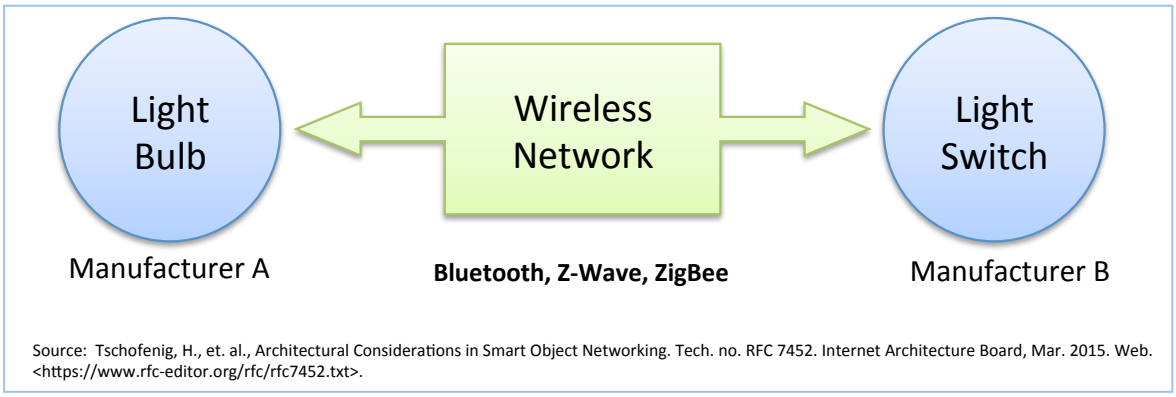
[38] "Internet of Things." Oxford Dictionaries, n.d. Web. 6 Sept. 2015. http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things

Internet of Things Communications Models

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452),[39] which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework.

Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth,[40] Z-Wave,[41] or ZigBee[42] to establish direct device-to-device communications, as shown in Figure 1.



Source: Tschofenig, H., et. al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. <https://www.rfc-editor.org/rfc/rfc7452.txt>.

Figure 1. Example of device-to-device communication model.

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario.

This device-to-device communication approach illustrates many of the interoperability challenges discussed later in this paper. As an *IETF Journal* article describes, "these devices often have a direct relationship, they usually have built-in security and trust [mechanisms], but they also use device-specific data models that

[39] Tschofenig, H., et. al., *Architectural Considerations in Smart Object Networking*. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt

[40] See http://www.bluetooth.com and http://www.bluetooth.org

[41] See http://www.z-wave.com

[42] See http://www.zigbee.org

require redundant development efforts [by device manufacturers]".[43] This means that the device manufacturers need to invest in development efforts to implement device-specific data formats rather than open approaches that enable use of standard data formats.

From the user's point of view, this often means that underlying device-to-device communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol. For example, the family of devices using the Z-Wave protocol is not natively compatible with the ZigBee family of devices. While these incompatibilities limit user choice to devices within a particular protocol family, the user benefits from knowing that products within a particular family tend to communicate well.

Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 2.

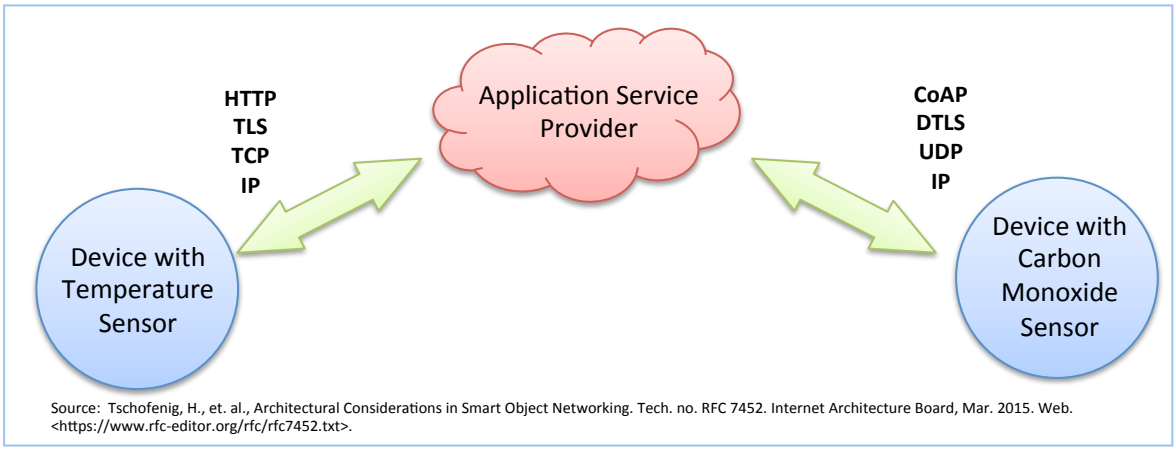


Figure 2. Device-to-cloud communication model diagram.

This communication model is employed by some popular consumer IoT devices like the Nest Labs *Learning Thermostat*[44] and the Samsung *SmartTV*.[45] In the case of the Nest *Learning Thermostat*, the device transmits data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung *SmartTV* technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV. In these cases, the

[43] Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, July 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

[44] "Meet the Nest Thermostat | Nest." Nest Labs. Web. 31 Aug. 2015. https://nest.com/thermostat/meet-nest-thermostat/

[45] "Samsung Privacy Policy--SmartTV Supplement." Samsung Corp. Web. 29 Sept. 2015. http://www.samsung.com/sg/info/privacy/smarttv.html

device-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.

However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor.[46] If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in'', a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 3.

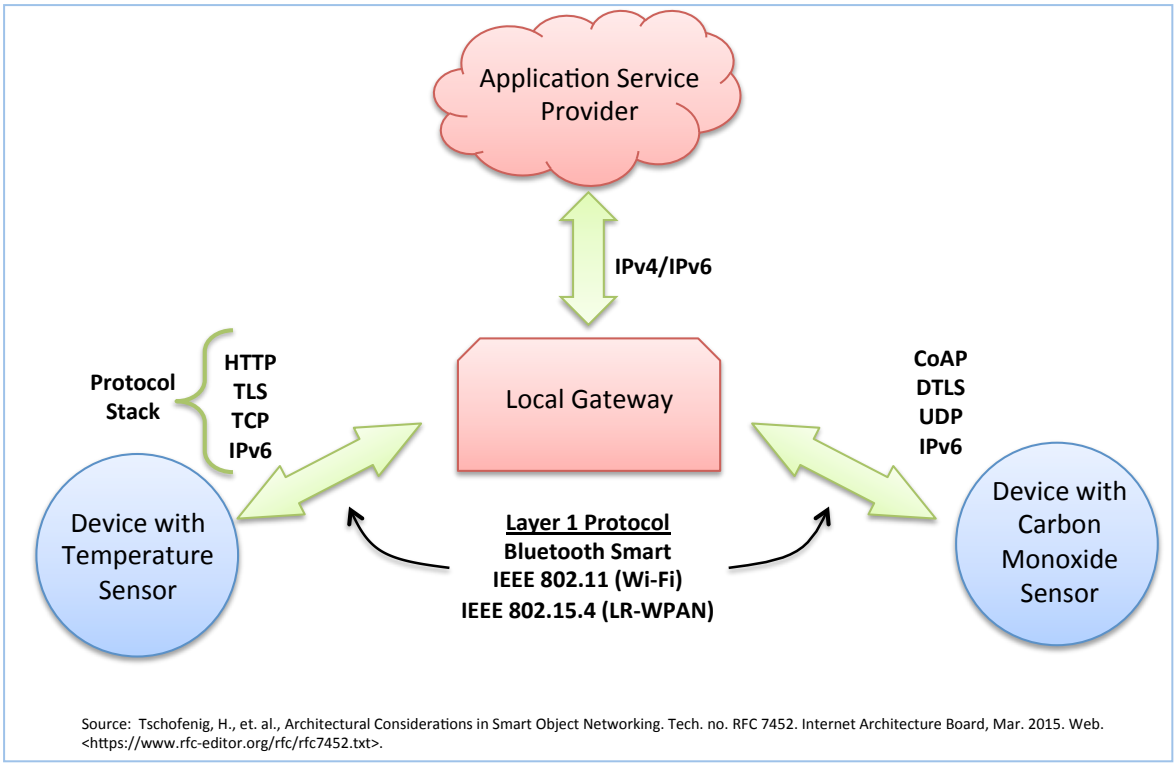


Figure 3. Device-to-gateway communication model diagram.

Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often the

[46] Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, July 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

The other form of this device-to-gateway model is the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the *SmartThings* hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices.[47] It then connects to the *SmartThings* cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection.

From a broader technical perspective, the *IETF Journal* article explains the benefit of the device-to-gateway approach:

> *This [communication model] is used in situations where the smart objects require interoperability with non-IP [Internet protocol] devices. Sometimes this approach is taken for integrating IPv6-only devices, which means a gateway is necessary for legacy IPv4-only devices and services.*[48]

In other words, this communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. A downside of this approach is that the necessary development of the application-layer gateway software and system adds complexity and cost to the overall system.

The IAB's RFC7452 document suggests the outlook for this model:

> *It is expected that in the future, more generic gateways will be deployed to lower cost and infrastructure complexity for end consumers, enterprises, and industrial environments. Such generic gateways are more likely to exist if IoT device designs make use of generic Internet protocols and not require application-layer gateways that translate one application-layer protocol to another one. The use of application-layer gateways will, in general, lead to a more fragile deployment, as has been observed in the past…*[49]

The evolution of systems using the device-to-gateway communication model and its larger role in addressing interoperability challenges among IoT devices is still unfolding.

Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This

[47] "How It Works." *SmartThings*, 2015. http://www.smartthings.com/how-it-works

[48] Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, July 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

[49] *Tschofenig, H., et. al.,* p. 6.

architecture supports “the [user’s] desire for granting access to the uploaded sensor data to third parties”.[50] This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where “IoT devices upload data only to a single application service provider”.[51] A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.

For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end data-sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

The back-end data-sharing model suggests a federated cloud services approach[52] or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud.[53] A graphical representation of this design is shown in Figure 4.

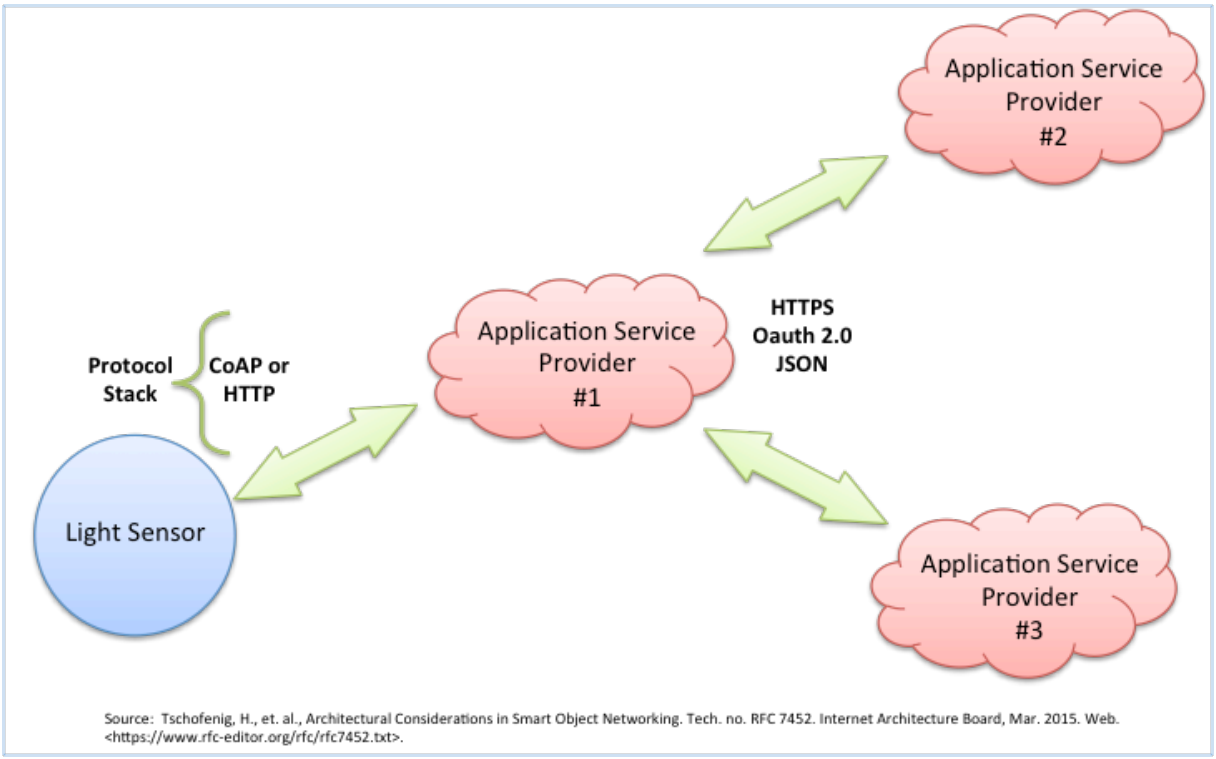


Figure 4. Back-end data sharing model diagram.

[50] *Tschofenig, H., et. al.,* p. 9.

[51] *Ibid.*

[52] A federated cloud services approach is one that combines the resources of separate cloud service providers to meet a larger business need.

[53] An example of a generic (non-IoT) off-the-shelf, federated cloud-sharing tool is *ownCloud,* produced by ownCloud.org. https://owncloud.org/blog/faster-easier-file-sync-and-share-with-federated-self-hosted-owncloud-8-0/

This architecture model is an approach to achieve interoperability among these back-end systems. As the *IETF Journal* suggests, "Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors."[54] In other words, this communication model is only as effective as the underlying IoT system designs. Back-end data sharing architectures cannot fully overcome closed system designs.

Internet of Things Communications Models Summary

The four basic communication models demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems.

From a general user perspective, these communication models help illustrate the ability of networked devices to add value to the end user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. For example, in three of the four communication models, the devices ultimately connect to data analytic services in a cloud computing setting. By creating data communication conduits to the cloud, users, and service providers can more readily employ data aggregation, big data analytics, data visualization, and predictive analytics technologies to get more value out of IoT data than can be achieved in traditional data-silo applications. In other words, effective communication architectures are an important driver of value to the end user by opening possibilities of using information in new ways. It should be noted, however, these networked benefits come with trade-offs. Careful consideration needs to be paid to the incurred cost burdens placed on users to connect to cloud resources when considering an architecture, especially in regions where user connectivity costs are high.

While the end user benefits from effective communication models, it should be mentioned that effective IoT communication models also enhance technical innovation and open opportunity for commercial growth. New products and services can be designed to take advantage of IoT data streams that didn't exist previously, acting as a catalyst for further innovation.

[54] *Duffy Marsan, Carolyn. p.7*

IPv6 and the Internet of Things

Though they differ about the exact numbers, most technology observers agree that billions of additional devices – from industrial sensors to home appliances and vehicles – will be connected to the Internet between now and 2025. As the Internet of Things continues to grow, devices that require true end-to-end Internet connectivity will not be able to rely on IPv4, the protocol most Internet services use today. They will need a new enabling technology: IPv6.

IPv6 is a long-anticipated upgrade to the Internet's original fundamental protocol – the Internet Protocol (IP), which supports all communications on the Internet. IPv6 is necessary because the Internet is running out of original IPv4 addresses. While IPv4 can support 4.3 billion devices connected to the Internet, IPv6 with 2 to the 128th power addresses, is for all practical purposes inexhaustible. This represents about 340 trillion, trillion, trillion addresses, which more than satisfies the demand of the estimated 100 billion IoT devices going into service in the coming decades.

Given the anticipated longevity of some of the sensors and other devices imagined for the Internet of Things, design decisions will affect the utility of solutions decades from now. Key challenges for IoT developers are that IPv6 is not natively interoperable with IPv4 and most low-cost software that is readily available for embedding in IoT devices implements only IPv4. Many experts believe, however, that IPv6 is the best connectivity option and will allow IoT to reach its potential.

For more information on IPv6 visit the Internet Society resource pages at http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6 and http://www.internetsociety.org/deploy360/ipv6/

What issues are raised by the Internet of Things?

It would be impossible to cover the broad scope of issues surrounding the Internet of Things in a single paper. Below, however, we provide an overview of five topics frequently discussed in relation to IoT. These include: security; privacy; interoperability and standards; legal, regulatory and rights; and emerging economies and development.

We begin to examine these issues through the lens of "the Abilities" – the statement of fundamental principles that guide ISOC's work in terms of the capabilities we believe all Internet users should enjoy that must be protected. These include the ability to *connect*, *speak*, *innovate*, *share*, *choose*, and *trust*.[55] With these principles as a guide, we present important aspects of each issue and propose several questions for discussion.

Security Issues

The IoT Security Challenge

As we note in the principles that guide our work, ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting *trust* and use of the Internet.[56] As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don't believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector.

As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the Internet of Things as they are for the computers that have traditionally been

[55] "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

[56] *Ibid.*

the endpoints of Internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts.

Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet *globally*, not just locally. For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection.[57]

To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyperconnected world. In fact, it is increasingly difficult to purchase some devices that are *not* Internet-connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber attack, but we can't so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behavior.

This is why security of IoT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact.

A Spectrum of Security Considerations

When thinking about Internet of Things devices, it is important to understand that security of these devices is not absolute. IoT device security is not a binary proposition of secure or insecure. Instead, it is useful to conceptualize IoT security as a spectrum of device vulnerability. The spectrum ranges from totally unprotected devices with no security features to highly secure systems with multiple layers of security features. In an endless cat-and-mouse game, new security threats evolve, and device manufacturers and network operators continuously respond to address the new threats.

The overall security and resilience of the Internet of Things is a function of how security risks are assessed and managed. Security of a device is a function of the risk that a device will be compromised, the damage such compromise will cause, and the time and resources required to achieve a certain level of protection. If a user cannot tolerate a high degree of security risk as in the case of the operator of a traffic control system or person with an implanted, Internet-enabled medical device, then she may feel justified in spending a considerable amount of resources to protect the system or device from attack. Likewise, if she is not concerned that her refrigerator might be hacked and used to send spam messages, then she may not feel

[57] Starr, Michelle. "Fridge Caught Sending Spam Emails in Botnet Attack - CNET." CNET, 19 Jan. 2014. http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

compelled to pay for a model that has a more sophisticated security design if it makes the device more costly or complicated.

Several factors influence this risk assessment and mitigation calculation. Factors include having a clear understanding of the present security risks and the potential future risks; the estimated economic and other costs of harm if the risks are realized; and the estimated cost to mitigate the risks.[58] While these kinds of security trade-offs are often made from an individual user or organizational perspective, it is also important to consider the interrelatedness of IoT devices as part of a larger IoT ecosystem. The networked connectivity of IoT devices means that security decisions made locally about an IoT device can have global impacts on other devices.

As a matter of principle, developers of smart objects for the Internet of Things have an obligation in ensuring that those devices do not expose either their own users or others to potential harm. As a matter of business and economics, vendors have an interest in reducing their cost, complexity, and time to market. For example, IoT devices that are high–volume, low–margin components that already represent a cost added to that of the product in which they are embedded are becoming quite common; adding more memory and a faster processor to implement security measures could easily make that product commercially uncompetitive.

In economic terms, lack of security for IoT devices results in a negative externality, where a cost is imposed by one party (or parties) on other parties. A classic example is pollution of the environment, where the environmental damage and cleanup costs (negative externalities) of a polluter's actions are borne by other parties. The issue is that the cost of the externality imposed on others is not normally factored into the decision-making process, unless, as is the case with pollution, a tax is imposed on the polluter to convince him to lower the amount of pollution. In the case of information security, as discussed by Bruce Schneier,[59] an externality arises when the vendor creating the product does not bear the costs caused by any insecurity; in this case, liability law can influence vendors to account for the externality and develop more security products.

These security considerations are not new in the context of information technology, but the scale of unique challenges that can arise in IoT implementations, as described below, make them significant.

Unique Security Challenges of IoT Devices

IoT devices tend to differ from traditional computers and computing devices in important ways that challenge security:

- Many Internet of Things devices, such as sensors and consumer items, are designed to be deployed at a massive scale that is orders of magnitude beyond that of traditional Internet-connected devices.

[58] A number of organizations have developed guides for conducting risk assessment. For example, the U.S. National Institute of Standards and Technology (NIST) issued a set of guidelines in 2012, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091 and the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) has published the ISO/IEC 31010:2009 "Risk management – Risk assessment techniques" document. http://www.iso.org/iso/catalogue_detail?csnumber=51073

[59] See Bruce Schneider's online article at: https://www.schneier.com/essays/archives/2007/01/information_security_1.html

As a result, the potential quantity of interconnected links between these devices is unprecedented. Further, many of these devices will be able to establish links and communicate with other devices on their own in an unpredictable and dynamic fashion. Therefore, existing tools, methods, and strategies associated with IoT security may need new consideration.

- Many IoT deployments will consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics.

- Many Internet of Things devices will be deployed with an anticipated service life many years longer than is typically associated with high-tech equipment. Further, these devices might be deployed in circumstances that make it difficult or impossible to reconfigure or upgrade them; or these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. These scenarios illustrate that security mechanisms that are adequate at deployment might not be adequate for the full lifespan of the device as security threats evolve. As such, this may create vulnerabilities that could persist for a long time. This is in contrast to the paradigm of traditional computer systems that are normally upgraded with operating system software updates throughout the life of the computer to address security threats. The long-term support and management of IoT devices is a significant security challenge.

- Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical. For example, consider the 2015 Fiat Chrysler recall of 1.4 million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key. The reality is that a high percentage of these autos probably will *not* be upgraded because the upgrade process presents an inconvenience for owners, leaving them perpetually vulnerable to cybersecurity threats, especially when the automobile appears to be performing well otherwise.

- Many IoT devices operate in a manner where the user has little or no real visibility into the internal workings of the device or the precise data streams they produce. This creates a security vulnerability when a user believes an IoT device is performing certain functions, when in reality it might be performing unwanted functions or collecting more data than the user intends. The device's functions also could change without notice when the manufacturer provides an update, leaving the user vulnerable to whatever changes the manufacturer makes.

- Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. Anti-tamper features and other design innovations will need to be considered to ensure security.

- Some IoT devices, like many environmental sensors, are designed to be unobtrusively embedded in the environment, where a user does not actively notice the device nor monitor its operating status. Additionally, devices may have no clear way to alert the user when a security problem arises, making it difficult for a user to know that a security breach of an IoT device has occurred. A security breach might persist for a long time before being noticed and corrected if correction or mitigation is even possible or practical. Similarly, the user might not be aware that a sensor exists in her surroundings, potentially allowing a security breach to persist for long periods without detection.

- Early models of Internet of Things assume IoT will be the product of large private and/or public technology enterprises, but in the future "Build Your own Internet of Things" (BYIoT) might become more commonplace as exemplified by the growing *Arduino* and *Raspberry Pi*[60] developer communities. These may or may not apply industry best practice security standards.

IoT Security Questions

A number of questions have been raised regarding security challenges posed by Internet of Things devices. Many of these questions existed prior to the growth of IoT, but they increase in importance due to the scale of deployment of IoT devices. Some prominent questions include:

a) **Good Design Practices.** What are the sets of best practices for engineers and developers to use to design IoT devices to make them more secure? How do lessons learned from Internet of Things security problems get captured and conveyed to development communities to improve future generations of devices? What training and educational resources are available to teach engineers and developers more secure IoT design?

b) **Cost vs. Security Trade-Offs.** How do stakeholders make informed cost-benefit analysis decisions with respect to Internet of Things devices? How do we accurately quantify and assess the security risks? What will motivate device designers and manufacturers to accept additional product design cost to make devices more secure, and, in particular, to take responsibility for the impact of any negative externalities resulting from their security decisions? How will incompatibilities between functionality and usability be reconciled with security? How do we ensure IoT security solutions support opportunities for IoT innovation, social and economic growth?

c) **Standards and Metrics**. What is the role of technical and operational standards for the development and deployment of secure, well-behaving IoT devices? How do we effectively identify and measure characteristics of IoT device security? How do we measure the effectiveness of Internet of Things security initiatives and countermeasures? How do we ensure security best practices are implemented?

d) **Data Confidentiality, Authentication and Access Control.** What is the optimal role of data encryption with respect to IoT devices? Is the use of strong encryption, authentication and access control technologies in IoT devices an adequate solution to prevent eavesdropping and hijacking

[60] See the Arduino open source community http://www.arduino.cc and the Raspberry Pi Foundation http://www.raspberrypi.org/

attacks of the data streams these devices produce? Which encryption and authentication technologies could be adapted for the Internet of Things, and how could they be implemented within an IoT device's constraints on cost, size, and processing speed? What are the foreseeable management issues that must be addressed as a result of IoT-scale cryptography? Are concerns about managing the crypto-key lifecycle and the expected period during which any given algorithm is expected to remain secure being addressed? Are the end-to-end processes adequately secure and simple enough for typical consumers to use?

e) **Field-Upgradeability.** With an extended service life expected for many IoT devices, should devices be designed for maintainability and upgradeability in the field to adapt to evolving security threats? New software and parameter settings could be installed in a fielded IoT device by a centralized security management system if each device had an integrated device management agent. But management systems add cost and complexity; could other approaches to upgrading device software be more compatible with widespread use of IoT devices? Are there any classes of IoT devices that are low-risk and therefore don't warrant these kinds of features? In general, are the user interfaces IoT devices expose (usually intentionally minimal) being properly scrutinized with consideration for device management (by anyone, including the user)?

f) **Shared Responsibility.** How can shared responsibility and collaboration for IoT security be encouraged across stakeholders?

g) **Regulation.** Should device manufacturers be penalized for selling software or hardware with known or unknown security flaws? How might product liability and consumer protection laws be adapted or extended to cover any negative externalities related to the Internet of Things and would this operate in a cross-border environment? Would it be possible for regulation to keep pace and be effective in light of evolving IoT technology and evolving security threats? How should regulation be balanced against the needs of permission-less innovation, Internet freedom, and freedom of expression?

h) **Device Obsolescence.** What is the right approach to take with obsolete IoT devices as the Internet evolves and security threats change? Should IoT devices be required to have a built-in end-of-life expiration feature that disables them? Such a requirement could force older, non-interoperable devices out of service and replace them with more secure and interoperable devices in the future. Certainly, this would be very challenging in the open marketplace. What are the implications of automatic decommissioning IoT devices?

The breadth of these questions is representative of the wide-ranging security considerations associated with Internet of Things devices. However, it's important to remember that when a device is *on* the Internet, it is also *part of* the Internet,[61] which means that effective and appropriate security solutions can be achieved only if the participants involved with these devices apply a Collaborative Security approach.[62]

[61] Kolkman, Olaf. "Introducing Collaborative Security, Our Approach to Internet Security Issues." Web log post. Internet Society, 13 Apr. 2015. http://www.internetsociety.org/blog/public-policy/2015/04/introducing-collaborative-security-our-approach-internet-security-issues

[62] *Collaborative Security: An Approach to Tackling Internet Security Issues*. Internet Society, Apr. 2015. http://www.internetsociety.org/collaborativesecurity

The collaborative model has emerged as an effective approach among industry, governments, and public authorities to help secure the Internet and cyberspace, including the Internet of Things. This model includes a range of practices and tools including bidirectional voluntary information sharing; effective enforcement tools; incident preparedness and cyber exercises; awareness raising and training; agreement on international norms of behavior; and development and recognition of international standards and practices. Continued work is needed to evolve collaborative and shared risk management-based approaches that are well suited to the scale and complexity of IoT device security challenges of the future.

Privacy Considerations

Internet of Things Privacy Background

Respect for privacy rights and expectations is integral to ensuring *trust* in the Internet, and it also impacts the ability of individuals to *speak*, *connect,* and *choose* in meaningful ways. These rights and expectations are sometimes framed in terms of ethical data handling, which emphasizes the importance of respecting an individual's expectations of privacy and the fair use of their data.[63] The Internet of Things can challenge these traditional expectations of privacy.

IoT often refers to a large network of sensor-enabled devices designed to collect data about their environment, which frequently includes data related to people. This data presumably provides a benefit to the device's owner, but frequently to the device's manufacturer or supplier as well. IoT data collection and use becomes a privacy consideration when the individuals who are observed by IoT devices have different privacy expectations regarding the scope and use of that data than those of the data collector.

Seemingly benign combinations of IoT data streams also can jeopardize privacy. When individual data streams are combined or correlated, often a more invasive digital portrait is painted of the individual than can be realized from an individual IoT data stream. For example, a user's Internet-enabled toothbrush might capture and transmit innocuous data about a person's tooth-brushing habits. But if the user's refrigerator reports the inventory of the foods he eats and his fitness-tracking device reports his activity data, the combination of these data streams paint a much more detailed and private description of the person's overall health. This data-aggregation effect can be particularly potent with respect to IoT devices because many produce additional metadata like time stamps and geolocation information, which adds even more specificity about the user.

In other situations, the user might not be aware that an IoT device is collecting data about the individual and potentially sharing it with third parties. This type of data collection is becoming more prevalent in consumer devices like smart televisions and video game devices. These kinds of products have voice recognition or vision features that continuously listen to conversations or watch for activity in a room and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A person might be in the presence of these kinds of devices without knowing their conversation or activities are being

[63] Wilton, Robin. *CREDS 2014 - Position Paper: Four Ethical Issues in Online Trust*. Issue brief no. CREDS-PP-2.0. Internet Society, 2014. https://www.internetsociety.org/sites/default/files/Ethical Data-handling - v2.0.pdf

monitored and their data captured. These kinds of features may provide a benefit to an informed user, but can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used.

Independent of whether the user is aware of and consents to having their IoT data collected and analyzed, these situations highlight the value of these personalized data streams to companies and organizations seeking to collect and capitalize on IoT information. The demand for this information exposes the legal and regulatory challenges facing data protection and privacy laws.

These kinds of privacy problems are critical to address because they have implications on our basic rights and our collective ability to trust the Internet. From a broad perspective, people recognize their privacy is intrinsically valuable, and they have expectations of what data can be collected about them and how other parties can use that data. This general notion about privacy holds true for data collected by Internet of Things devices, but those devices can undermine the user's ability to express and enforce privacy preferences. If users lose confidence in the Internet because their privacy preferences aren't being respected in the Internet of Things, then the greater value of the Internet may be diminished.

Unique Privacy Aspects of Internet of Things

Generally, privacy concerns are amplified by the way in which the Internet of Things expands the feasibility and reach of surveillance and tracking. Characteristics of IoT devices and the ways they are used redefine the debate about privacy issues, because they dramatically change how personal data is collected, analyzed, used, and protected. For example:

- The traditional "notice and consent" online privacy model, in which users assert their privacy preferences by interacting directly with information presented on a computer or mobile screen (e.g. by clicking "I agree"), breaks down when systems provide no mechanism for user interaction. IoT devices frequently have no user interface to configure privacy preferences, and in many IoT configurations users have no knowledge or control over the way in which their personal data is being collected and used. This causes a gulf between the user's privacy preferences and the data-collecting behavior of the IoT device. There might be less incentive for IoT vendors to offer a mechanism for users to express their privacy preferences if they regard the data collected as being non-personal data. However, experience shows that data not traditionally considered personal data might actually be personal data or become personal data when combined with other data.

- Assuming an effective mechanism can be developed to enable a user to express informed consent of their privacy preferences to IoT devices, that mechanism needs to handle the large number of IoT devices a user must control. It is not realistic to think that a user will directly interact with each and every IoT device they encounter throughout the day to express their privacy preferences. Instead, privacy interface mechanisms need to be scalable to the size of the IoT problem, while still being comprehensive and practical from a user perspective.

- The Internet of Things can threaten a person's expectations of privacy in common situations. There are social norms and expectations of privacy that differ in public spaces versus private spaces, and IoT

devices challenge these norms. For example, IoT monitoring technologies like surveillance cameras or location tracking systems that normally operate in public spaces are migrating into traditionally private spaces like the home or personal vehicle in which our expectations of privacy are very different. In doing so, they challenge what many societies recognize as the "right to be left alone" in one's home or private space. Also individuals' expectations of privacy in spaces they consider to be public (e.g. parks, shopping malls, train stations) are being challenged by the increased nature and extent of monitoring in those spaces.

- IoT devices often operate in contexts in which proximity exposes multiple people to the same data collection activity. For example, a geolocation tracking sensor in an automobile would record location data about all occupants of the vehicle, whether or not all the occupants want their location tracked. It may even track individuals in nearby vehicles. In these kinds of situations, it might be difficult or impossible to distinguish, much less honor, individual privacy preferences.

- Big data analytics applied to aggregated personal data already represents a substantial risk of privacy invasion and potential discrimination. This risk is amplified in the Internet of Things by the scale and greater intimacy of personal data collection. IoT devices can collect information about people with an unprecedented degree of specificity and pervasiveness; aggregation and correlation of these data can create detailed profiles of individuals that create the potential for discrimination and other harms. The sophistication of this technology can create situations that expose the individual to physical, criminal, financial or reputational harm.

- The ubiquity, familiarity, and social embrace of many IoT devices might create a false sense of security and encourage individuals to divulge sensitive or private information without full awareness or appreciation of the potential consequences of doing so.

IoT Privacy Questions

These privacy issues would be challenging even if the interests and motivations of all of the participants in the IoT ecosystem were well aligned. However, we know that there can be unbalanced or unfair relationships and interests between those who are exposed to personal data collection and those who aggregate, analyze, and use the data. The data source might see an unwelcome intrusion into private space, often without consent, control, choice, or even awareness. The data collector, however, might consider this a beneficial resource that can add value to products and services as well as provide new revenue streams.

Because IoT challenges our notions of privacy in new ways, key questions need to be asked when re-evaluating online privacy models in the context of IoT. Some questions that have been raised include:

a) **Fairness in Data Collection and Use.** How do we resolve the marketplace relationship between data sources and data collectors in the context of IoT? Personal data has personal and commercial value that sources and collectors value differently, both individually and in aggregate; both parties have legitimate interests that may conflict. How might those distinct interests be expressed in a way that leads to fair and consistent rules for both sources and collectors concerning access, control, transparency, and protection?

b) **Transparency, Expression, and Enforcement of Privacy Preferences.** How can privacy policies and practices be made readily available and understandable in the context of IoT? What are the alternatives to the traditional "notice and consent" privacy model that will address the unique aspects of the Internet of Things? What is an effective model for expressing, applying, and enforcing individual privacy preferences and multi-party preferences? Could such a multi-party model be constructed, and if so, what would it look like? How might it be applied to specific circumstances involving individual privacy preferences? Is there a market for outsourcing the management of privacy settings to commercial services designed to put users' preferences into effect? Is there a role for a privacy proxy that would express and enforce a user's preferences across an array of devices, while eliminating the need for direct interaction with each one?

c) **Wide-Ranging Privacy Expectations.** Privacy norms and expectations are closely related to the social and cultural context of the user, which will vary from one group or nation to another. Many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the Internet of Things? How can IoT devices and systems be adapted to recognize and honor the range of privacy expectations of the users and different laws?

d) **Privacy by Design.** How can we encourage IoT device manufacturers to integrate privacy-by-design principles into their core values? How do we foster the inclusion of consumer privacy considerations in every phase of product development and operation? How do we reconcile functionality and privacy requirements? In principle, manufacturers should expect that privacy-respecting products and practices build long-term customer trust, satisfaction, and brand loyalty. Is that a sufficiently compelling motivation, when matched against the competing desires for design simplicity and speed to market? Should devices be designed with default settings configured for the most conservative data collection mode (i.e. opt out of data collection by default)?

e) **Identification.** How should we protect data collected by IoT that appears not to be personal at the point of collection or has been "de-identified", but may at some point in the future become personal data (e.g. because data can be re-identified or combined with other data)?

The Internet of Things creates unique challenges to privacy that go beyond the data privacy issues that currently exist. Strategies need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new IoT technology.

Interoperability / Standards Issues

IoT Interoperability / Standards Background

In the traditional Internet, interoperability is the most basic core value; the first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings.

Interoperability is so fundamental that the early workshops for Internet equipment vendors were called "Interops";[64] and it is the explicit goal of the entire Internet Standards apparatus centered on the Internet Engineering Task Force (IETF).[65]

Interoperability is also a cornerstone of the open Internet.[66] Barriers deliberately erected to obstruct the exchange of information can deny Internet users the ability to *connect*, *speak*, *share*, and *innovate,* which are four of ISOC's fundamental principles.[67] So-called "walled gardens'', in which users are permitted to interoperate with only a curated subset of sites and services, can substantially diminish the social, political, and economic benefits of access to the entire Internet.

In a fully interoperable environment, any IoT device would be able to connect to any other device or system and exchange information as desired. In practicality, interoperability is more complex. Interoperability among IoT devices and systems happens in varying degrees at different layers within the communications protocol stack between the devices. Furthermore, full interoperability across every aspect of a technical product is not always feasible, necessary, or desirable and, if artificially imposed (such as through government mandates), could provide disincentives for investment and innovation. The standardization and adoption of protocols that specify these communication details, including where it is optimal to have standards, are at the heart of the interoperability discussion for IoT.

Beyond the technical aspects, interoperability has significant influence on the potential economic impact of IoT. Well-functioning and well-defined device interoperability can encourage innovation and provide efficiencies for IoT device manufacturers, increasing the overall economic value of the market. Furthermore, the implementation of existing standards and development of new open standards where necessary help lower barriers to entry, facilitate new business models, and build economies of scale.[68]

A 2015 McKinsey Global Institute report states, "[on] average, interoperability is necessary to create 40 percent of the potential value that can be generated by the Internet of Things in various settings."[69] The report continues, "Interoperability is required to unlock more than $4 trillion per year in potential economic impact for IoT use in 2025, out of a total impact of $11.1 trillion across the nine settings that McKinsey analyzed."[70] While some companies perceive competitive advantages and economic incentives in building proprietary systems, overall economic opportunities may be constrained in a marketplace of silos.

---

[64] "A History of the Internet: 1988." Web log post. Computer Information, 12 Aug. 2010. Web. 6 Sept. 2015. http://inthistory4u.blogspot.com/2010/08/1988.html

[65] See http://www.ietf.org

[66] "Open Internet: What is it, and how to avoid mistaking it for something else," Internet Society 3 Sept. 2014. https://www.internetsociety.org/doc/open-internet-what-it-and-how-avoid-mistaking-it-something-else

[67] "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

[68] The European Commission Rolling plan for ICT Standardisation 2015 section 3.5.6 Internet of Things has a discussion on IoT standards from a competitiveness and policy perspective. See https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation

[69] Manyika, James, et. al., *The Internet of Things: Mapping the Value beyond the Hype*. McKinsey Global Institute, June 2015. p. 2. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

[70] *Ibid.* 4.

Also, interoperability is fundamentally valuable from the perspective of both the individual consumer and organizational user of these devices. It facilitates the ability to choose devices with the best features at the best price and integrate them to make them work together. Purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, concern over vendor lock-in, or fear of obsolescence due to changing standards.

Key Considerations and Challenges in IoT Interoperability / Standards

Interoperability, standards, protocols, and conventions are a primary issue in the early development and adoption of IoT devices. While not exhaustive, a number of key considerations and challenges include:

- **Proprietary Ecosystems and Consumer Choice.** Some device manufacturers see a market advantage to creating a proprietary ecosystem of compatible IoT products, sometimes called "walled gardens", which limit interoperability to only those devices and components within the brand product line. These manufacturers can create user lock-in to their particular device ecosystem by increasing the switching cost for the consumer to change to a different brand in the future or substitute components from another vendor. For example, in the home automation market, light bulbs from one vendor may not be interoperable with a light switch or control system manufactured by another.

  Interoperability supporters view these practices as an impediment to user choice because it deters users from changing to alternative products. They also view this practice as a barrier to innovation and competition because it limits the ability of competitors to create new products based on the ecosystem's foundational infrastructure. Some device manufacturers, however, see a closed ecosystem approach as a benefit to users by providing a protocol that can be adapted more quickly and easily when technical or market demands require change.

  Interoperability considerations also extend to the data collected and processed by IoT services. One of the primary attractions of connected devices is the ability to transmit and receive data to services "in the cloud", which in turn provide valuable information or services based upon that data. While this is extremely useful, it also can present challenges for a user who wants to move to a competing service. Even if access to the data generated by devices is made available to users, obtaining the data will be useless if the data is in a proprietary format. Only if the source data is freely available to the originating user, in an open standard format, will users be free to move to another service provider, or to perform analyses on their own.

- **Technical and Cost Constraints.** As manufacturers develop IoT devices, there are inherent technical, time to market, and cost constraints that factor into device interoperability and design. Some devices are constrained by technical factors like limited internal processing resources, memory, or power consumption demands. Similarly, manufacturers are under pressure to reduce the unit cost of the device by minimizing part and product design costs. Manufacturers make cost-benefit analyses to decide whether the additional costs and potentially reduced product performance is worth the extra benefits of implementing standards. In the short-term, it can be more costly to design interoperability features into a product and test for compliance with a standards specification. In some contexts, the cheapest path to market may be to use proprietary protocols and systems.

This needs to be compared, however, against the long-term product lifecycle gains afforded by interoperability.

- **Schedule Risk.** In a globally competitive market, there is often a first-mover advantage to bringing a product to market quickly and establishing market share, and this certainly applies to IoT device manufacturers. A problem arises for IoT device interoperability when the device manufacturer's product design schedule outpaces the availability of interoperability standards. An IoT device manufacturer that is eager to bring a product to market may view lack of certainty in standards development schedules and processes as business risk to be minimized or avoided. This can make design alternatives to open interoperability standards more attractive, particularly in the short term.

- **Technical Risk.** When an IoT device manufacturer or user is planning the development of a product, they need to assess technical design risks of protocols in the development process. Incorporating existing and proven standards into product or system designs can represent a lower technical risk compared to the development and use of proprietary protocols. The use of generic, open and widely available standards (such as the Internet Protocol suite) as building blocks for devices and services can bring other benefits, such as access to larger pools of technical talent, developed software, and cheaper development costs. These factors are discussed in Internet Architecture Board (IAB) RFC 7452, "*Architectural Considerations in Smart Object Networking".* [71]

- **Devices Behaving Badly.** Lack of standards and documented best practices have a greater impact than just limiting the potential of IoT devices. In a passive way, absence of these standards can enable bad behavior by IoT devices. In other words, without standards to guide manufacturers, developers of these devices sometimes design products that operate in disruptive ways on the Internet without much regard to their impact. These devices are worse than simply not being interoperable. If poorly designed and configured, they may have negative consequences for the networking resources they connect to and the broader Internet.

  In an essay, Internet expert Geoff Huston describes the proliferation of such devices as the "Internet of stupid things''.[72] Huston describes an example of a consumer-grade cable modem produced by one manufacturer that hard-coded the IP address of the network time protocol (NTP) server operated by the University of Wisconsin into the product, which is a breach of commonly accepted design practices. As Huston explains, "The more units that were sold, the greater the aggregate traffic volume that was sent to the university's server."[73] Not only were these devices behaving badly by funneling all of the NTP requests to a single server, but the vendor's poor design compounded the difficulty because it provided no effective mechanism to fix the problem.

  There is an opportunity for the deployment of IoT standards and best practices to significantly diminish this class of problems over time

[71] Tschofenig, H., et. al., *Architectural Considerations in Smart Object Networking*. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://tools.ietf.org/html/rfc7452

[72] Huston, Geoff. "The Internet of Stupid Things." *APNIC Labs*., 28 Apr. 2015. https://labs.apnic.net/?p=620

[73] *Ibid*.

- **Legacy Systems.** Interoperability standardization is a challenge for new IoT devices that need to interface with systems already deployed and operating. This is relevant to many industry-specific and application-specific environments that have established networks of devices.[74] IoT engineers are faced with design trade-offs to maintain compatibility with legacy systems while still trying to achieve greater interoperability with other devices through the use of standards.

- **Configuration.** Users will face increasing challenges in managing larger numbers of IoT devices. One such challenge is the need to quickly and easily modify the configuration settings of many IoT devices on a network. When facing the daunting prospect of configuring hundreds of individual devices, it will be essential to have thoughtful design and standardization of configuration tools, methods, and interfaces.[75]

- **Proliferation of Standards Efforts**. Many new industry coalitions have emerged alongside traditional Standards Developing Organizations (SDOs) to increase efforts to assess, develop, modify, or harmonize standards and protocols related to IoT. This includes, for example, long-standing SDOs such as the IETF, ITU, and IEEE, and comparatively new efforts such as the Industrial Internet Consortium, Open Interconnection Consortium, ZigBee Alliance, and AllSeen Alliance, among many others.[76]

  The time and investment required by industry and other stakeholders to participate in the wide range of standardization efforts will likely be costly. Further, there is likely to be overlap and even conflicting standardization strategies between some efforts.[77] In addition to increasing the costs of standards development, the absence of coordination across efforts could ultimately produce conflicting protocols, delay product deployment, and lead to fragmentation across IoT products, services, and industry verticals.

Interoperability Questions

Interoperability and standards pose challenges and questions for the future of IoT devices, including:

a) In what areas are interoperability standards most needed and desirable? Are these sufficiently similar or different across the wide range of potential IoT applications and use cases (such as consumer goods, industrial applications and medical appliances)? What are the generic and widely available standards (such as the Internet Protocol suite) that could be used as building blocks for IoT devices and services? How would a lack of interoperability impact users' ability to connect, speak, share, and innovate?

[74] Examples of legacy system protocols include: SCADA (Supervisory Control and Data Acquisition), a protocol used for communication of industrial devices; CAN Bus (Control Area Network) protocols for vehicle and industrial sensors.

[75] Vint Cerf, personal communications, 9 September 2015.

[76] See section "For More Information" at the end of this paper for a list of standards bodies, consortiums, and alliances working on IoT standards issues.

[77] Lawson, Stephen. "Why Internet of Things 'Standards' Got More Confusing in 2014." *PCWorld*, December 24, 2014. http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

b) What are the optimal roles of Standards Developing Organizations (SDOs), industry consortia, and stakeholder groups in IoT standards development? What is the potential for bringing together the wide range of groups working on IoT technical implementations for broader discussions about interoperability and standards implementation? Can competing standards, duplication, and conflicts stemming from SDOs and consortia tackling similar or overlapping issues be avoided without adding undue coordination overhead? More practically, how can industry players and other interested parties keep track of all of the activities happening in this broad space?

c) What is the best approach to educate and engage user and developer communities about the problems of badly behaving IoT devices and lack of standards implementation? What types of best practices or implementation reference models would be effective, given the broad range of IoT applications and use cases?

d) How will the Internet of Things impact the consumption of bandwidth and other resources and to what extent will standards need to be modified to support those evolving needs? Given the importance of cloud-enabled services to the Internet of Things, what are the challenges related to cloud-to-cloud interoperability?

Overall, the importance of IoT interoperability and standards to the market and consumers is undeniable. Ultimately, the challenge of developing and employing interoperability standards is central to the discussion of innovation, competition, and user choice of services, which are embedded in ISOC's core principles.

Regulatory, Legal, and Rights Issues

The application of IoT devices poses a wide range of challenges and questions from a regulatory and legal perspective, which need thoughtful consideration. In some cases, IoT devices create new legal and regulatory situations and concerns over civil rights that didn't exist prior to these devices. In other cases, these devices amplify legal issues that already existed. Further, technology is advancing much more rapidly than the associated policy and regulatory environments. Several potential regulatory and legal issues that affect the full spectrum of IoT applications are discussed below.

Data Protection and Crossborder Data Flows

Data collected by IoT devices may not be constrained from being sent across jurisdictional boundaries. These devices use the Internet to communicate, and the Internet spans jurisdictional boundaries at all levels. IoT devices can collect data about people in one jurisdiction and transmit that data to another jurisdiction for data storage or processing, often with few or no technical roadblocks. This can quickly become a legal problem, for example, if the data collected is deemed to be personal or sensitive data and subject to data protection laws in multiple jurisdictions. To further complicate matters, the data protection laws in the jurisdiction where the device and data subject reside might be inconsistent or incompatible with the laws in the jurisdiction where the data is stored and processed.

These situations are described as crossborder or transborder data flows, and they raise questions about the legal scope of regulations that might be applicable. In other words, which legal regime governs the device collecting the data, and which governs the storage and use of the collected data? This scenario also raises normative questions. Can these laws be modified to reduce the degree of Internet fragmentation they cause while still protecting the rights of users? Should a jurisdiction with more-restrictive data protection laws for handling and transmission of certain IoT-enabled data be able to project those legal requirements onto other jurisdictions?

While many of these crossborder data flow questions have been raised and addressed in the context of traditional Internet data traffic,[78] IoT devices pose a new challenge in this regard. Increasingly, these devices will be able to automatically connect to other devices and systems and transmit information across borders without the knowledge of the user. This could create situations where a user becomes liable for crossborder data flow requirements, and he is unaware that the activity is happening. These are complex issues, and only growing more so, as technology continues to outpace policy.

IoT Data Discrimination

The data collected by IoT devices can paint a detailed portrait about the people interacting with them, and this data can be used for both beneficial and discriminatory purposes. Consider the case of personal fitness tracking devices. Frequently, a person wears a fitness tracker continuously over a span of days or weeks, and it collects finely detailed information about the person's movements and other biometric data. This data is analyzed by a software application to determine a person's level of fitness, estimate calories burned, track hours slept, and characterize the quality of sleep. This analysis is clearly beneficial for the user as a way to quantify their activity when they are trying to reach a weight-loss or fitness goal.

But this same data can be used in potentially discriminatory ways. Some health insurance plans in the United States are incentivizing participants to provide the insurer with access to this fitness tracker data in return for lower insurance premiums.[79] This can be viewed as a positive situation, by giving preferential pricing to those people who are willing to give up their biometric data in return for a discount. On the other hand, this may have the potential to be discriminatory, especially for those who are economically disadvantaged. As one commentator writes:

> *Imagine [an insurance] pricing scheme that would punish sleep-deprived single parents or the dietary habits of the working poor. And the financial incentives for giving insurers and others access to your health data might become so compelling that "choosing" to participate becomes the only viable choice.*[80]

[78] Typically, cross border data flows are addressed in regional and international privacy frameworks (e.g. OECD Privacy Guidelines, Council of Europe Convention 108, APEC Privacy Framework) and special arrangements (e.g. APEC Cross Border Privacy Rules system, EU Binding Corporate Rules). But, this is a patchwork approach, not a globally applicable solution.

[79] *Big Doctor Is Watching*. Slate, 27 Feb. 2015. http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html

[80] *Ibid.*

Similar scenarios are becoming more prevalent. Newer vehicles are equipped with GPS-enabled transponders and data links, which communicate location and data indicative of driving habits (e.g. speeding and hard braking) to remote systems, or are used to provide driver assistance or enhanced travel services. While these features provide benefits to the user, the data can be used in potentially discriminatory ways. For example, fleet operators can use this data to pervasively monitor the performance of its drivers without an option for those drivers to opt out of being observed. These are relatively straightforward examples of ways IoT data can be used in discriminatory ways, but it is unclear how different combinations of IoT data might be used to discriminate in the future.

Further, the potential for discriminatory pricing practices or unfair services practices may be amplified by the quality, specificity, and volume of IoT-produced data about users. IoT data can often be tagged with metadata like date and timestamps and geolocation tags, which dramatically increase the quality of the data for analytical purposes. Additionally, IoT sensors are usually narrow in the functions they perform. This means that the sensor data is frequently associated with a specific operational situation, which affords a high degree of specificity when correlating the data with a person or set of people. In fact, the device might be uniquely identified with a specific person because it is implanted within that person, as in the case of an Internet-enabled pacemaker or insulin pump. In other scenarios, this level of specificity is undesirable and can cause unintended discriminatory results. IoT sensors owned or operated by third parties can collect identifiable data about people without their knowledge or consent. This data could be used in ways that are detrimental to the person being monitored.

Lastly, these devices provide large streams of continuous data without human intervention. The combination of these data qualities makes analysis of IoT data very descriptive and useful for research, product development, and other areas. Big data algorithms can examine massive quantities of IoT data and look for statistical and semantic correlations to determine groupings or clusters of related characteristics among users. But at the same time, these algorithms are susceptible to unfairly categorizing users and exploiting their characteristics.

Using IoT data in this fashion raises practical, legal, and regulatory issues. First, how are discriminatory or unfair practices against users detected? Are there discriminatory practices that are practically impossible to detect? Are there any legal differences if the discrimination decision is made by a person or by a machine? It is a challenging area of academic research to develop tools to detect unfair algorithmic practices, especially since most data analytics algorithms are company secrets and not in the public domain. How do we balance the tremendous commercial and societal benefits of IoT data analytics against the likelihood of discriminatory practices against users? How do we encourage the principles of permissionless innovation in the IoT domain while protecting users from unfair practices? How do we improve transparency? Are existing privacy and consumer protection laws sufficient to address this scenario? What remedies should be available in the event of discrimination? Should IoT devices be categorized and regulated based on the nature of the data they produce, especially when that data is prone to misuse?

IoT Devices as Aids to Law Enforcement and Public Safety

IoT devices offer potential benefits to law enforcement and public safety, but the legal and societal ramifications need to be carefully considered. Clearly, IoT devices and the data they generate can be used

as effective tools to fight crime. Surveillance cameras have been deployed inside retail establishments to collect video footage and track shopper activity, which has proven valuable as evidence in criminal prosecution and as a deterrent to crime.[81] More recently, On-Star Corporation, a subsidiary of General Motors, can provide in-car sensor data to police to aid in recovering stolen cars and can remotely disable a stolen vehicle.[82] The Nassau County Police Department in New York uses a network of deployed sound sensors called *ShotSpotter*, which can detect and pinpoint the exact source of gunfire in neighborhoods in which it is deployed.[83] These are all examples of the benefits that the Internet of Things technology can offer to law enforcement to fight crime and improve public safety.

However, the deployment and use of these kinds of IoT technologies cause concern among some civil rights advocates and others. Potential causes of concern include the pervasiveness of the data monitoring activities, the data retention and destruction policies, and the secondary uses of the data by government officials, as well as the potential inadvertent exposure of that data to bad actors. Additionally, the potentially adverse impact on socially beneficial activity arising from communities or societies that are monitored needs to be carefully considered.

Other law enforcement and public safety situations are less straightforward. For example, in the product release of the iPhone 6 smartphone and its iOS 8 operating system, Apple Corporation removed a "backdoor" access method that existed on previous iPhone versions. The backdoor feature enabled police officials to gain access to the data on a user's phone for law enforcement purposes. Apple removed this feature in the new iPhone, and it now encrypts the internal contents of the phone in a way that is not easily defeated, and for which Apple does not hold the keys and thus cannot enable access.[84] This prohibits access to the content on the phone by anyone other than the owner. Federal law enforcement officials claim this hinders prosecution of criminal behavior,[85] while civil liberty supporters view this as a victory for protecting the privacy of user data.[86] This device encryption controversy applies to other IoT devices as well. What is the appropriate role of device encryption to protect an IoT device from criminal attacks versus legitimate access to user data inside a device for law enforcement and public safety interests?

[81] Goforth Gregory, Jennifer. "5 Ways Tech Is Stopping Theft." *Entrepreneur*, November 7, 2013. http://www.entrepreneur.com/article/229674

[82] Bond, Jr., Vince. "Lawyers Reaching for In-car Data." *Automotive News*, 14 Sept. 2014. http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data

[83] Weis, Todd R. "Cool Cop Tech: 5 New Technologies Helping Police Fight Crime." *Computerworld*. N.p., 16 Feb. 2012. Web. 03 Aug. 2015. http://www.computerworld.com/article/2501178/government-it/cool-cop-tech--5-new-technologies-helping-police-fight-crime.html?page=2

[84] Timm, Trevor. "Your IPhone Is Now Encrypted. The FBI Says It'll Help Kidnappers. Who Do You Believe?" The Guardian, 30 Sept. 2014. http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

[85] *Ibid.*

[86] Timberg, Craig. "Apple Will No Longer Unlock Most IPhones, IPads for Police, Even with Search Warrants." *Washington Post*. The Washington Post, 18 Sept. 2014. http://wapo.st/XGGwDi

IoT Device Liability

IoT devices pose thought-provoking legal liability questions that need consideration. A fundamental underlying question with respect to IoT devices is: If someone is harmed as a result of an IoT device's action or inaction, who is responsible? The answer is frequently complicated, and in many instances there is not yet much case law to support a particular position. IoT devices operate in a more complex way than a simple stand-alone product, which suggest more complex liability scenarios need to be considered. For example:

- IoT devices are likely to be used in ways never anticipated by the manufacturer. An IoT device manufacturer cannot reasonably perform product assurance testing on all possible use cases of IoT devices.

- There is the potential for IoT devices to connect and interact with other IoT devices in untested and unforeseen ways. As interoperability of these devices increases, they may be able to form *ad hoc* network connections among themselves. Therefore, it is difficult for a manufacturer or user to account for all potentially harmful scenarios in advance of deploying these devices.

- These devices can have long service lives in the field and are susceptible to future security threats that are presently unknown. Accordingly, these devices might become compromised and maliciously reprogrammed to damage themselves or other devices, or to reveal sensitive information in unintended and unnoticed ways.

- IoT devices will be integrated into autonomous systems like driverless cars, which incorporate adaptive machine-learning algorithms to control their behavior based on sensor inputs from IoT devices. The actions of these systems cannot be fully known and tested in advance.

These scenarios and others raise questions. If harm results from one of these scenarios, do existing liability laws adequately address legal culpability and clarify the liability exposure of parties involved? Do liability laws need reconsideration for intelligent IoT devices that learn from their environment and modify themselves over time? If autonomous systems are instructed by the end user rather than by their internal algorithms, what happens in cases of user error? Should IoT devices be smart enough to have a "do what I meant" instruction? To what extent will current liability laws for conventional products extend to products that become Internet-enabled? What can we as a community do to better inform legislators and policy makers, so that they are not as susceptible to the vast amounts of misinformation and biased advice they are receiving? And, what can we do to better inform the users and buyers of these devices, so that they understand all of the factors affecting their use?

Proliferation of IoT Devices Used in Legal Actions

Data collected by IoT devices can often serve as evidence in a variety of legal proceedings, and as IoT data becomes more prevalent, it is likely to be used increasingly in legal actions. For example, lawyers in the United States have used time and location data enabled by electronic highway toll devices in automobiles to

catch cheating spouses in divorce proceedings.[87] And in 2014, a Canadian woman used her own personal fitness tracker data to substantiate her claim in a personal injury lawsuit.[88]

In more deliberate uses of IoT devices in legal actions, Internet-enabled devices can be installed in automobiles to act as payment assurance devices for those who default on payment obligations. If the driver doesn't make their lease or car loan payment, the lease agent or lender can disable the vehicle remotely via the installed device until payment is made.[89] These IoT devices have been installed in more than two million cars in the US.[90]

These kinds of scenarios raise new legal and regulatory questions about IoT devices. Should device manufacturers include technologies like data encryption in these devices to restrict access to data streams in a fashion analogous to the Apple iPhone? Conversely, should device manufacturers be designing IoT devices that facilitate the demand for use data in legal proceedings? Are standards needed to specify design requirements for IoT data to support legal chain of custody of data in legal proceedings? Should there be consumer protection regulations placed on certain IoT devices?

Regulatory, Legal, and Rights Issues Summary

The range of legal, regulatory and rights issues associated with the Internet of Things is broad. IoT devices create new legal and policy challenges that didn't previously exist, and they amplify many challenges that already exist. For example, accessibility requirements for IoT devices for those with disabilities offer new challenges arising from the introduction of new kinds of IoT devices, while remaining compatible with existing accessibility standards and guidelines.[91] On the other hand, the enormous scale of wireless IoT devices and the radio frequency (RF) noise and interference they produce is an example of the way IoT devices amplify the existing difficulty of regulating the use of the RF spectrum.[92] Legal and regulatory concerns of intellectual property issues, environmental issues (e.g. disposal of devices), and legal ownership of devices (e.g. will devices be owned or rented) are emerging challenges as well for IoT devices.

Along with the complexities of deciding the appropriate regulatory or policy strategies for IoT problems, there is the added complexity of deciding where in an IoT system architecture is the best place to achieve the desired outcomes. Should the regulatory controls be placed on the device, on the flow of the data, on the

[87] Newmarker, Chris. "E-ZPass Records out Cheaters in Divorce Court." *Msnbc.com*. NBC News.com, 10 Aug. 2007. http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/ - .Vbp9KnjfbFI

[88] Olson, Parmy. "Fitbit Data Now Being Used In The Courtroom." *Forbes*. Forbes Magazine, 16 Nov. 2014. http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

[89] Picchi, Aimee. "Why the Repo Man Can Remotely Shut off Your Car Engine." *CBS News*, September 25, 2014. http://www.cbsnews.com/news/why-the-repo-man-can-remotely-shut-off-your-car-engine/

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

[91] Various public sector procurement rules provide a baseline for accessibility requirements for information and communication technology (ICT) products, which should be considered in the context of IoT device compatibility. Examples include the United States Access Board Section 508 Standards and the European Standard EN 301 549 V1.1.1.

[92] McHenry, Mark A., Dennis Roberson, and Robert J. Matheson. "Electronic Noise Is Drowning Out the Internet of Things." *IEEE Spectrum*, no. September 2015 (August 18, 2015). http://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things

gateway, on the user, or in the cloud where data is stored? The answers to these questions and others depend on the perspective taken to analyze the situation. Regulatory analysis of IoT devices is increasingly viewed from a general, technology-neutral perspective legal lens, such as consumer protection laws and regulations.[93] Assessing legal implications of IoT devices from the perspective of preventing unfair or deceptive practices against consumers[94] can help inform decisions of privacy and security among others.[95]

Lastly, the resolution of challenges in this space, and their impacts, need to be considered with respect to the guiding Internet Society principles that promote the ability to *connect*, *speak*, *innovate*, *share*, *choose*, and *trust*.[96]

Emerging Economy and Development Issues

Ensuring IoT Opportunities are Global

The spread and impact of the Internet is global in nature, providing opportunity and benefits to developed and developing regions alike. At the same time, there are often unique challenges in developing regions related to the deployment, growth, implementation, and use of technology, including the Internet. It is reasonable to expect the same to be true for the potential benefits and challenges associated with the Internet of Things.

From an Internet Society principle perspective, we believe that the Internet should be a source of empowerment globally, regardless of a user's location, region, or state of economic development, and that the full range of abilities and principles[97] that drive our work and the success of the Internet apply globally. From early in the history of the Internet, the Internet technical community, civil society, governmental organizations, and private industry, among others, have focused on the opportunities and challenges related to the Internet in emerging economies. So this also should be true regarding opportunities and challenges related to the Internet of Things.[98]

Economic and Development Opportunities

In terms of opportunity, McKinsey Global Institute notes that IoT technology has significant potential in developing economies. By 2025, they project that as much as 38% of annual economic impact of IoT

[93] Botterman, Maarten. *Policy Paper on IoT Future Technologies: Opening towards a New Reality*. Issue brief no. D5.2. 39. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

[94] US Federal Trade Commission Act, 15 U.S. Code § 45(a).

[95] The Internet Governance Forum's Dynamic Coalition on the Internet of Things (DC IoT) has proposed an "ethical approach" for framing solutions to IoT challenges. See for example: http://www.iot-dynamic-coalition.org/intersessional-meetings/dresden-meeting-2015/ and http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/

[96] "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

[97] *Ibid.*

[98] The Internet Governance Forum Dynamic Coalition on the Internet of Things (DC IoT) has been particularly active in considering the impact and challenges of IoT in emerging and developing economies. See the DC IoT website at http://www.iot-dynamic-coalition.org/ for related discussions.

applications will derive from less developed regions.[99] From an economic perspective, it is expected that both demographics and marketplace trends will drive opportunity. For example, developing countries have a high potential number of IoT users (particularly in China), global economic growth is shifting to developing economies, and industrial IoT applications (such as in factories, worksites, and transportation) are expected to drive economic value creation.[100]

Should expectations regarding innovation and application of the technology be realized, IoT implementations could hold considerable promise as fundamental enablers of social development, including the achievement of the United Nations Sustainable Development Goals.[101] The Sustainable Development Goals, or SDGs, are a set of 17 goals framing over 100 development targets aimed at guiding efforts to achieve dignity, well-being, and equality for all the world's people -- especially the poor and underserved. They cover the vast range of fundamental development challenges, including sustainable agriculture, energy, water availability, industrialization, and management of terrestrial and maritime resources, among others.

In considering the potential for smart object and Internet of Things technology to meaningfully address development challenges, the opportunities appear compelling. For example, the application of sensor networks to environmental challenges, including water quality and use, sanitation, disease, and health, climate change, and natural resource monitoring, could have significant impact beyond resource management. The data derived from such applications also could be used in research contexts, assisting local scientists and universities in making unique contributions to the broader body of global scientific knowledge and providing an incentive for local academic talent to stay in country to conduct research.

The growing world population, particularly in emerging economies, and challenges associated with providing access to quality, safe, and affordable food are set to grow over time. The potential use of IoT to combat hunger and promote sustainable agricultural has received particular attention, perhaps more than any other development issue.[102] From managing agricultural production cycles, disease threats, and growing inputs through to automated harvesting, distribution logistics, and quality monitoring, IoT-enabled "smart agriculture" techniques are envisioned across the entire value chain to improve the sustainability and productivity of the food supply.[103,104]

[99] Manyika, James, et. al., *The Internet of Things: Mapping the Value beyond the Hype*. McKinsey Global Institute, June 2015. p. 4. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

[100] Manyika, James, et. al., p. 4-5.

[101] The list of United Nations Sustainable Development Goals and targets is available at https://sustainabledevelopment.un.org/topics.

[102] Members of the Internet Society have formed a Special Interest Group (SIG) to specifically investigate issues at the intersection of the Internet, IoT, and the food sector. More information on the ISOC Internet of Food SIG can be found at http://internet-of-food.org/

[103] Botterman, Maarten. *Policy Paper on IoT Future Technologies: Opening towards a New Reality*. Issue brief no. D5.2. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

[104] "Digital Farm Set for Internet's next Wave." *The Guardian*, September 20, 2015, sec. connecting the future. http://www.theguardian.com/connecting-the-future/2015/sep/21/digital-farm-set-for-internets-next-wave

Harnessing IoT for Global Development

Across the globe, the Internet of Things (IoT) is being deployed to solve some of the most pressing issues in global development. From poverty alleviation to improving sustainable water and sanitation management, connected technologies are being used to improve service delivery and development outcomes.

Driven by the declining cost of sensors and microprocessors, coupled with a growing array of affordable connectivity technologies, the IoT represents the next frontier in the role of information and communications technologies (ICTs) in development (ICT4D). While over 90% of the global population is covered by mobile cellular networks, with two-thirds covered by 3G signals providing robust data communications, a variety of other short- and long-range technologies also provide a wide range of options for data connectivity. As affordability in devices and service continues to increase, IoT interventions in development (IoT4D) will spread. Already today, for example, when equipped with sensors that monitor temperature and location, cold chains – specifically those that facilitate the transportation and distribution of essential vaccines – are more secured and efficient, with a larger percentage of shipments making it to intended destinations without spoiling. In east Africa, village hand pumps are being deployed equipped with water flow sensors with 2G SMS modules that can inform local municipalities, government offices and donor communities on the rate of water usage and resulting in decreased downtime of malfunctioning pumps.

The agricultural sector has benefitted from IoT as well. More targeted feeding and monitoring of livestock is possible via name/number tags containing information on a radio-frequency identification (RFID) chip. Electrochemical sensors embedded in soil can measure sunlight exposure, as well as levels of water saturation and presence of key nutrients like phosphorus and nitrogen. Additionally, low income families living in remote areas, as well as urban areas without access to the formal electrical grid, are using IoT technologies coupled with off-grid solar cells to power their homes with electricity. The upfront capital costs of the solar units are amortized and paid through mobile money services, with the solar cells communicating battery level and usage on a regular basis via data communications.

These and many other examples highlight the IoT's impact as a tool for achieving the United Nations' Millennium Development Goals (MDGs) and the upcoming Sustainable Development Goals (SDGs). However, challenges remain, particularly with regard to infrastructure, technical capacity and fostering regulatory environments that are welcoming of IoT interventions. Greater attention to the potential of IoT4D will help increase its impact and efficacy in tackling some of the most pressing development challenges of our time.

Source: "Harnessing the Internet of Things for Global Development" by Cisco and the ITU/UNESCO Broadband Commission for Sustainable Development (forthcoming).

IoT Emerging Economy and Development Questions

To ensure that the opportunities and benefits related to IoT are global, the specific needs and potential challenges related to emerging economies must be considered. The matters discussed in the preceding issue sections are not unique to industrialized countries, and should be considered applicable to developing markets as well. However, the unique circumstances often found in emerging economies raise additional questions about maximizing the benefits and managing challenges of IoT. While by no means exhaustive, some areas for consideration include:

a) **Infrastructure Resources:** Internet and communications infrastructure has spread rapidly across the developing world, yet gaps remain in ensuring reliable, high-speed, and affordable access in many countries, including for commercial and business use. To what extent will the Internet of Things place pressure on Internet and telecommunications infrastructure and resources? Will current challenges curb the opportunity for IoT in emerging regions, or could IoT be a demand-driver for additional build-out of infrastructure? Does special attention need to be paid to spectrum management, given that wireless technology underpins many IoT implementations? As cloud services and related data analysis drive value in many IoT services, will the relative lack of data center infrastructure in emerging economies hinder deployment?

b) **Investment:** In industrialized countries, investment in IoT research and product development is being driven by market opportunities for products and services. To what extent will the market drive investment in IoT implementations in developing countries, especially beyond applications in industries and settings that have the prospect of clear, near-term returns? On the other hand, could IoT deployments in emerging economies be more efficient and cost effective, and even leap-frog technology in the rest other world, as fewer legacy systems are often in place? Is there a role for governments to incentivize the development of innovative technical solutions by local researchers and local industries?

c) **Technical and Industry Development:** To what extent are researchers and entrepreneurs from developing countries involved in IoT technical development and deployment? What should be done to encourage participation in development of technical solutions and applications that meet the needs and opportunities of these markets, while being respectful of cultural norms, and building in appropriate levels of security and privacy protection? What new skills may be required in emerging economies to build, deploy, and manage IoT systems? Are industries in emerging economies ready to benefit from IoT technology? Will they be left behind or are they better positioned to leap-frog older industrial technologies? How can researchers and industries in countries with emerging economies be positioned to develop solutions to local economic and social challenges that have direct impact on their societies?

d) Policy and Regulatory Coordination: Policymakers and regulators in emerging economies have made significant progress over the past 10 years to develop and adapt policies and regulations to encourage Internet growth and address related challenges. The demands on technology policymakers in emerging economies are steep, particularly in light of rapid developments and

resource constraints. While IoT promises new opportunities, it also will add a new dimension of complexity. What information and resources do policymakers in emerging economies need now to plan for policy demands and questions that will arise with the growth of IoT?

Conclusion

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the “Internet of Things’’. IoT promises to usher in a revolutionary, fully interconnected “smart” world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be “online”.

While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision – particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders. The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks.

The Internet Society cares about IoT because it represents a growing aspect of how people and institutions are likely to interact with and incorporate the Internet and network connectivity into their personal, social, and economic lives. Solutions to maximizing the benefits of IoT while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible perils. Rather, it will take informed engagement, dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward.

For More Information

A vast range of organizations, alliances, and government efforts are taking place around the world to address issues related to the Internet of Things. The following list of additional information sources is by no means exhaustive. Rather, is meant as a starting point for further investigation.

Organizations and Alliances Working on the Internet of Things

AIOTI – The Alliance for Internet of Things Innovation (AIOTI) was launched by the European Commission to support the development of a European IoT ecosystem, including standardization policies. https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti

AllSeen Alliance – A 180-member industry group, the AllSeen Alliance promotes widespread adoption of an interoperable peer communications framework based on AllJoyn for devices and applications in IoT. https://allseenalliance.org/

ETSI – ETSI's Connecting Things effort is developing standards for data security, data management, data transport and data processing related to potentially connecting billions of smart objects into a communications network. http://www.etsi.org/technologies-clusters/clusters/connecting-things

IEC 62443/ISA99 – Industrial Automation and Control System Security Committee develops standards, technical reports and procedures for implementing secure industrial automation and control systems. http://isa99.isa.org/ISA99%20Wiki/Home.aspx

IEEE (including P2413) – The IEEE has a dedicated IoT initiative and clearinghouse of information for the technical community involved in research, implementation, application and usage of IoT technologies. http://iot.ieee.org/

IERC – The European Research Cluster on the Internet of Things coordinates ongoing activities in the area of IoT across Europe. http://www.internet-of-things-research.eu/

Internet Engineering Task Force (IETF) – The Internet's premier standards setting body has an IoT Directorate that is coordinating related efforts across its working groups, reviewing specifications for consistency, and monitoring IoT-related activities in other standards groups. https://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

IIC – The Industrial Internet Consortium (IIC) has teamed up with the OIC to accelerate the delivery of an industrial grade IoT architectural framework. IIC released a reference architecture for IoT in 2015. http://www.industrialinternetconsortium.org/

Internet Governance Forum -- IGF sponsors the Dynamic Coalition on IoT, which hosts open meetings to discuss global challenges that need to be addressed regarding IoT deployment. http://www.intgovforum.org/cms/component/content/article?id=1217:dynamic-coalition-on-the-internet-of-things

Internet of Things Consortium – This industry group provides consumer research and market education aimed at driving adoption of IoT products and services. http://iofthings.org/#home

IP for Smart Objects (IPSO) Alliance – Dedicated to enabling IoT, IPSO seeks to establish IP as the basis for connecting smart objects through education, research and promotion. http://www.ipso-alliance.org/

ISO/IECJTC-1 – ISO issued a preliminary report on IoT in 2014 as well as a Smart Cities report. The group has ongoing subcommittees in both areas. http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

ISOC's Internet of Food SIG – This special interest group leads discussion on the technical infrastructure standards needed for the food industry in the future. http://internet-of-food.org/

ITU – The ITU hosted an IoT Global Standards Initiative, which concluded its activities in July 2015, followed by the formation of a new Study Group 20 focused on IoT applications. http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx

MAPI Foundation -- The Manufacturers Alliance for Productivity and Innovation (MAPI) s developing Industrie 4.0 for industrial applications of IoT. https://www.mapi.net/research/publications/industrie-4-0-vs-industrial-internet

OASIS – OASIS is developing open protocols to ensure interoperability for IoT. The group chose Message Queuing Telemetry Transport (MQTT) as its messaging protocol of choice for IoT and has optimized MQTT-S-N for wireless sensor networks. OASIS has three technical committees in IoT overseeing MQTT and two other standards, Advanced Message Queuing Protocol (AMQP) and OASIS Open Building Information Exchange (oBIX). https://www.oasis-open.org/committees/tc_cat.php?cat=iot

oneM2M – Dedicated to developing machine-to-machine communications architecture and standards, this multi-vendor group is focused on telemedicine, industrial automation, and home automation. Its goal is a common M2M Service Layer that can be embedded in hardware and software. http://www.onem2m.org/

Online Trust Alliance – This group of security vendors has developed a draft trust framework for IoT applications, focused on security, privacy, and sustainability. https://otalliance.org/initiatives/internet-things

Open Interconnection Consortium – OIC is defining a common communication framework based on industry standards to wirelessly connect and manage the flow of information among IoT devices. It sponsors the IoTivity Project, an open source software framework for device-to-device connectivity. http://openinterconnect.org/

The Open Management Group – This technical standards consortium is developing several IoT standards, including Data Distribution Service (DDS) and Interaction Flow Modeling Language (IFML) along with dependability frameworks, threat modeling, and a unified component model for real-time and embedded systems. http://www.omg.org/hot-topics/iot-standards.htm

Open Web Application Security Project -- OWASP sponsors an IoT Top Ten Project, which is designed to help manufacturers, developers, and consumers understand related security issues with its list of the most significant attack surface areas for IoT.
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Smart Grid Interoperability Panel -- SGIP has an effort called EnergyIoT focused on new opportunities for IoT within the energy industry. The group's OpenFMB is a utility-led project that is incorporating common utility data models and IoT communication protocols to create an Open Field Message Bus.
http://sgip.org/focus-resilience

Thread Group – This group of smart home vendors is developing a common networking protocol that will support IP-enabled devices in the home such as appliances, lighting, and security systems.
http://threadgroup.org/About.aspx

Government Policy, Research, and Coordination Efforts

Australia - Australia Commonwealth Scientific and Industrial Research Organisation (CISRO), Australia's national science agency, is leading research and development efforts into IoT technology.
http://www.csiro.au/en/Research/DPF/Areas/Autonomous-systems/IoT

China – The Central People's Government of the People's Republic of China has issued a programmatic document "Guidance on Pushing for an Orderly and Healthy Development of Internet of Things" which outlines China's national policy on IOT. http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm

China - Ministry of Industry and Information Technology of the People's Republic of China has issued the "12th five-year plan," an Internet of Things developmental planning document.
http://kjs.miit.gov.cn/n11293472/n11295040/n11478867/14344522.html

European Union - European Commission Digital Agenda for Europe, Internet of Things – The Commission has been working with member states toward the future deployment of IoT. The group has compiled lists of European IoT research and pilot projects. http://ec.europa.eu/digital-agenda/en/Internet-things

European Union - European Commission Internet of Things Expert Group (EO2514) – This group of experts advises the Commission on technical, legal and organizational challenges to IoT deployment across Europe. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514

India – The Government of India's Ministry of Communications & IT is focusing on developing an IoT industry ecosystem as a top initiative for transforming India into a digital-empowered society and knowledge economy. http://deity.gov.in/content/internet-things

Republic of Korea - In 2014, Republic of Korea Ministry of Science, ICT, and Future Planning issued a "Master Plan for Building the Internet of Things (IOT) that leads the hyper-connected, digital revolution" (available through the Korea IOT Association website at http://karus.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf).

Singapore - SPRING Singapore, the Infocomm Development Authority of Singapore (IDA) and the Information Technology Standards Committee (ITSC), under the purview of the Singapore Standards Council (SSC), have laid out an Internet of Things (IoT) Standards Outline in support of Singapore's Smart Nation initiative. http://www.spring.gov.sg/NewsEvents/PR/Pages/Internet-of-Things-(IoT)-Standards-Outline-to-Support-Smart-Nation-Initiative-Unveiled-20150812.aspx

https://www.ida.gov.sg/Tech-Scene-News/Tech-News/Tag?tag=internet+of+things

United Kingdom – In 2015, the UK Government Chief Scientific Advisor issued a report outlining its IoT goals, ``The Internet of Things: making the most of the Second Digital Revolution.''https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

United Kingdom – The UK's communications regulator, Ofcom, has identified several priority areas for fostering IoT deployments, including spectrum availability, data privacy, network security, and resilience and network addresses. http://stakeholders.ofcom.org.uk/consultations/iot/next-steps/

United States – The US Federal Trade Commission formed the Office of Technology Research and Investigation (OTRI) to explore privacy, security, and payment issues related to IoT among other topics. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Notes and Acknowledgements

The Internet of Things: An Overview

Understanding the Issues and Challenges of a More Connected World

This paper was authored by:

Karen Rose - Senior Director, Strategy and Analysis, Internet Society
Scott Eldridge - Principal, Cam & Sprocket LLC and Internet Society Individual Member
Lyman Chapin – Principal, Interisle Consulting Group and Internet Society Individual Member

The authors would like to thank the staff members of the Internet Society cross-organizational working group that honed the concept for this paper and provided critical guidance and feedback throughout the course of its development: Michael Kende, Graham Minton, Steve Olshansky, Robin Wilton, Greg Wood, and Dan York. Further thanks are due to the Internet Society staff across the organization who contributed to the review of this paper and provided their valuable input and insights: Joyce Dogniez, Olaf Kolkman, Megan Kruse, Ted Mooney, Christian O'Flaherty, Maarit Palovirta, Bastiaan Quast, Andrei Robachevsky, Phil Roberts, Christine Runnegar, Sally Wentworth, Fernando Zarur and Jan Žorž.

Our special appreciation also goes to the Internet Society community of Members, Chapters and collaborators who generously volunteered their time and expertise to review and comment on previous drafts of this paper: Nicolas Antoniello, Grunela Astbrink, Hosein Badran, Maarten Botterman, Vint Cerf, Sri Chandra, Glenn Deen, Tim Denton, Patrik Fältström, John Garrity, Andrés Gomez, Richard Hill, Howard Lee, Mike O'Reirdan, Robert Pepper, Alejandro Pisanty, Chip Sharp, Bert Wijnen, and Paul Wilson.

Editor: Carolyn Marsan
Cover designer: Michelle Speckler

For more information please see https://www.internetsociety.org/iot

Internet Society

Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Email: info@isoc.org

report-InternetofThings-20151015-en