The Internet of Things

An Internet Society Public Policy Briefing

2 August 2016

Introduction

Internet of Things is a broad term used to describe situations in which Internet connectivity and computing capabilities extend to devices, sensors, and everyday items not ordinarily considered to be computers (e.g., consumer goods, cars and trucks, industrial components, wearable health monitors, and collections of devices working together to create concepts such as "smart cities" and "smart homes"). These objects collect data from their surroundings that are then transmitted and remotely analyzed to create new insights, deliver services, and control other items.

Projections for the impact of IoT on both the Internet and the economy are impressive: as many as 100 billion connected IoT devices[1] and a global economic impact of more than $11 trillion by 2025[2]. IoT promises to provide advances in industrial automation, healthcare, energy conservation, agriculture, transportation, urban management, as well as many other sectors and applications. The potential for tremendous growth innovation, applications, and services is a testament to the open nature of the Internet's architecture and design, which does not place limits on the kinds of devices or services that can connect to it.

At the same time, however, there remain significant challenges associated with IoT that could stand in the way of realizing its potential benefits. Some of the most pressing challenges and questions include issues of security, privacy, interoperability, and standards, as well as regulatory and rights issues, and the readiness of emerging economies to adopt it.

This brief offers an overview of key IoT issues. These same issues are discussed in greater detail in the Internet Society's report, *The Internet of Things: An Overview–Understanding the Issues and Challenges of a More Connected World*.

Often referred to as *the Internet of Things (IoT),* billions of smart devices are expected to come online in the coming decade, bringing with them the promise of global economic opportunities and new innovations that will transform the way we work, live, and play. However, challenges associated with IoT, including security and privacy, must be addressed in order for technology to reach its full potential.

1 "Global Connectivity Index." Huawei Technologies Co., Ltd., 2015. Web. 6 Sept. 2015. http://www.huawei.com/minisite/gci/en/index.html.
2 Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; and Aharon, D. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

Key Considerations

Although interest in connected devices has surged in recent years, the concept of connecting objects and items to communications networks and the Internet is not a new one. Machine-to-machine (M2M) communications systems, which used proprietary networks rather than the Internet, became widespread in industrial settings more than 25 years ago. The first everyday items to be controlled over the Internet emerged in the early 1990s and set the stage for today's Internet of Things.

Today, IoT represents a growing aspect of how people and institutions interact with the Internet in their personal, social, and economic lives. It may also represent a shift in how users engage with and are impacted by the Internet. For example, today's Internet experience is largely characterized by users actively downloading and generating content through their computers and smartphones. Many IoT devices, however, are designed to operate in the background, sending and receiving data on a user's behalf with little human intervention or even awareness; still others are designed to control objects and physical assets in the world, such as vehicles and buildings, or to monitor human behavior.

If the projections and trends about IoT become reality, we would be wise to consider the implications of a world in which the most common interaction with the Internet comes from passive engagement with connected objects, rather than active engagement with content. Governments, for example, will want to ensure that their policies keep pace with the rapidly changing environment.

Policies that promote Internet infrastructure, efficient use of wireless spectrum, data-center development, and user empowerment and choice are critical to the evolution IoT. And as the amount and nature of data collected about users and their environments shifts from IoT, privacy and data security policies should be considered that reflect the evolving technology and its potential impacts on users.

Beyond the direct infrastructure and telecommunication aspects of IoT, other policy areas may benefit from a review. IoT devices will likely touch most aspects of our lives, including devices in our homes, workplaces, schools, hospitals, and other public spaces. As such, privacy, data security, healthcare, transportation, and technology and innovation policies will likely be impacted. This kind of broad reach suggests that policy makers will need to consider the broad policy implications across a wide field of policy goals and initiatives.

While IoT is not a particularly new idea from a technical perspective, its growth and maturity will present both new benefits and new challenges that will require shifts in policy approaches and strategies.

Challenges

A number of challenges need to be addressed in order to fully realize IoT's potential benefits to individuals, societies, and economies.

- **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.

Manufacturers are frequently presented with economic and technical challenges when building and maintaining robust security features in IoT devices. But devices and services with weak security are vulnerable to cyber attacks and can expose user data to theft. Because an increasing number of IoT devices online increases the number of potential security vulnerabilities, this a key IoT challenge.

Ensuring lifetime security in IoT products and services must be a fundamental priority to maintain overall user trust in this technology. Users need to trust that IoT devices and related data services are secure, especially as they become more pervasive and integrated into our daily lives.

As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure that they do not expose users and the Internet itself to potential harm. The actions of industry, government, users, and others will contribute to the secure development, maintenance, and use of IoT devices.

The Internet Society believes that a collaborative approach to IoT security will be needed to develop effective and appropriate solutions that are well-suited to the scale and complexity of the issues.

- **Privacy.** The ability to collect, analyze, and transform data drives much of the value of IoT devices and services, but this data also can be used to paint detailed and invasive profiles of users. Indeed, IoT is redefining the debate about privacy issues, as many implementations can dramatically change the way data is collected, analyzed, and used.

  Specifically, IoT amplifies concerns about a potential increase of surveillance and tracking, and the amount of sensitive data that can be collected by devices operating in our homes, businesses, and public environments. Sometimes these devices collect data about individuals without their knowledge or informed consent. Furthermore, while data from the devices benefit the device's owner, the same data frequently benefit the device's manufacturer or supplier, as well. This becomes a serious privacy consideration when the individuals who are observed by IoT devices have different privacy expectations regarding the scope and use of that data than do the data collectors.

  IoT devices that collect data about people in one jurisdiction may transmit that data to another jurisdiction for data storage or processing. Challenges can arise if the data collected is deemed to be personal or sensitive and is subject to data protection laws in multiple jurisdictions.

  Enabling cross-border data flows that protect privacy and promote legal certainty for users and IoT service providers will be key for promoting the global growth of IoT.

  While the privacy challenges are considerable, they are not insurmountable. Strategies need to be developed that promote transparency, fairness, and user choice in data collection and handling, enhance user privacy rights and

expectations across a range of preferences, and foster innovation in new technology and services.

- **Interoperability and standards.** Interoperability among IoT devices and data streams can encourage innovation and provide efficiencies for device manufactures and users, thereby increasing overall benefits and economic value. McKinsey Global Institute estimates that device interoperability will drive up to 40% of the potential value generated by IoT.[3]

  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, walled gardens (closed platforms or ecosystems), and concern over vendor lock-in. Interoperability and standards considerations also extend to the data collected and processed by IoT services, as incompatible and proprietary data formats can present challenges for users seeking to integrate systems, have the flexibility to move to different services, or perform additional analysis on collected data. In short, a fragmented environment of proprietary technical implementations and data formats[4] will inhibit IoT value and flexibility for both users and the industry.

  Today's marketplace offers a variety of technical approaches to IoT. Some companies see strategic advantages to developing proprietary ecosystems, while others are developing their own approaches because common technologies do not yet exist. A wide range of companies, industry groups, and researchers are working on approaches that create greater IoT interoperability and standards.

  The Internet Society believes that greater interoperability and the use of generic, open, voluntary, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol, or IP) will support greater user benefits, innovation, and economic opportunity.

- **Regulatory, legal, and rights Issues.** IoT amplifies and reintroduces many regulatory and legal questions. There is a danger that the rapid rate of change in IoT technology could outpace the ability of associated policy, legal, and regulatory structures to adapt.

  One such issue includes the potential conflict between law enforcement surveillance and civil rights. IoT devices offer potential benefits to law enforcement, public safety, and public administration. However, they also raise potential civil and human rights concerns regarding the pervasiveness of societal monitoring, the secondary uses of data by the government, and access to data from personal IoT devices by law enforcement or as evidence in legal actions, among other challenging issues.

3 ibid.
4 For information on the recent activities of the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB) to promote IoT standardization and interoperability, see https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf and https://www.iab.org/activities/workshops/iotsi/.

Further, IoT devices pose legal liability questions. One fundamental question is: If someone is harmed as a result of an IoT device's action or inaction, who is responsible? The answer is often complicated, and in many instances there is not enough case law to support a position. Because IoT devices operate in a more complex way than stand-alone products, more complex liability scenarios need to be contemplated.

Given the broad nature of IoT regulatory and policy challenges, a collaborative governance approach to policy development that relies on input and participation by a range of stakeholders is needed for the best outcomes.

- **Emerging economy and development issues.** IoT holds significant promise for delivering social and economic benefits to emerging and developing economies in such areas as sustainable agriculture, water quality and use, healthcare, industrialization, climate monitoring, and environmental management.

  For example, sensor networks are helping villagers and researchers in Asia and Africa improve clean-water delivery by monitoring the quality of water at its source and the performance of delivery pumps. In addition, wireless soil, weather, and livestock monitors and IoT-automated agricultural equipment have been deployed in developing regions to help farmers increase productivity.[3] In these ways and many others, IoT holds great promise as a tool to achieving the United Nations Sustainable Development Goals.[4]

  Developing regions also present unique challenges related to the deployment, growth, implementation, and use of the technology. These challenges include the deployment of adequate Internet and basic communications infrastructure in rural and remote areas, incentives for investment, and local participation in the development IoT solutions. In order for the benefits of IoT to be truly global, the unique needs and challenges of implementation in less-developed regions will need to be addressed.

Guiding Principles

Given the anticipated adoption of IoT devices, its potential economic and societal benefits, and associated challenges, increased public-sector awareness of IoT technology and the importance of the issues surrounding it is essential. Governments are urged to take the following steps to accommodate and foster IoT deployment.

- **Promote Internet and data-infrastructure growth.** Governments should promote the expansion of both wireless and wireline infrastructure, including in rural and remote areas, and consider IoT needs for both licensed and unlicensed spectrum use. Barriers to data-center development and user-based systems for IoT data analysis, such as burdensome equipment taxes or licensing requirements, should be removed. Governments should review their existing

3 For more examples of how IoT is supporting development, see "Harnessing the Internet of Things for Global Development", https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.
4 Information on the United Nations Sustainable Development Goals can be found at https://sustainabledevelopment.un.org/sdgs.

Internet infrastructure in light of the potential increased data communication needs of IoT devices.

- **Encourage IPv6 deployment.** IPv6 is an enabling technology for Internet growth, and it will become even more critical as IoT drives up the number of connected devices. Governments should make IPv6 adoption a national priority and engage stakeholders in their community to encourage IPv6 rollout.[5]

- **Encourage open, voluntary IoT standards.** Employing greater interoperability and the use of open, voluntary, and widely available standards as technical building blocks for IoT devices will support greater user benefits, innovation, and economic opportunity. Governments should refrain from mandating technical approaches to IoT, and, instead, encourage industry, researchers, and other stakeholders to work together on the development of open, consensus-based standards that support interoperability.

- **Adopt a collaborative, multistakeholder approach to IoT policy discussions.** IoT is a challenging area for policymakers, as it is a rapidly developing environment and its technology spans many industries and uses. A collaborative governance approach, one that draws on the expertise and engagement of a wide range of stakeholders, will be needed to develop effective and appropriate solutions.[6] Policies should aim to promote users' ability to connect, speak, innovate, share, choose, and trust in a manner that both promotes innovation and enables user rights.

- **Encourage a collaborative approach to IoT security**. The Internet Society believes that IoT security is the collective responsibility of all who develop and use IoT devices. Participants in the IoT space should adopt a collaborative approach to security among its broad, multistakeholder community by assuming responsibility, sharing best practices and lessons learned, encouraging security dialog, and emphasizing the development of flexible, shared security solutions that can adapt and evolve as threats change over time. IoT security policy should focus on empowering players to address security issues close to where they occur, rather than centralizing IoT security among a few, while also preserving the fundamental properties of the Internet and user rights.[7]

- **Encourage responsible design practices for IoT sevices.** Security-by-design and privacy-by-design practices for IoT devices should be encouraged. Whether via privacy and data protection regulation, voluntary industry self-regulation, or other incentives or policy means, IoT device developers should be encouraged to respect the end-user's privacy and data security interests and consider those interests a core element of the product-development process. IoT system designers also should consider the full lifecycle of the IoT system to

5 Additional guidance for IPv6 can be found in the ISOC IPv6 policy brief, http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.
6 An overview of the collaborative, multistakeholder model for Internet governance is available at http://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works.
7 An overview of the collaborative security approach is available in the Internet Society's report, *Collaborative Security: An approach to tackling Internet Security Issues,* 2015. http://www.internetsociety.org/collaborativesecurity.

ensure obsolete devices don't pose security risks and are compatible with responsible environmental stewardship.

Additional Resources

The Internet Society has published a number of papers and additional content related to this issue. These are available for free access on the Internet Society website.

- IoT Resource Web page, http://www.internetsociety.org/iot.
- *The Internet of Things (IoT): An Overview - Understanding the Issues and Challenges of a More Connected World.* (2015). http://www.internetsociety.org/doc/iot-overview.
- "Adoption of IPv6". (2016). http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.
- IPv6 Resource Web pages, http://www.internetsociety.org/deploy360/ipv6/.
- *Collaborative Security: An approach to tackling Internet Security Issues.* (2015). http://www.internetsociety.org/collaborativesecurity.