The Technology Factsheet Series was designed to provide a brief overview of each technology and related policy considerations. These papers are not meant to be exhaustive.

**Technology and Public Purpose Project**
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street, Cambridge, MA 02138

[www.belfercenter.org/TAPP](http://www.belfercenter.org/TAPP)

**CRCS Center for Research on Computation and Society**
Harvard John A. Paulson School of Engineering and Applied Sciences
29 Oxford Street, Cambridge, MA 02138

[crics.seas.harvard.edu](http://crics.seas.harvard.edu)

Statements and views expressed in this report are solely those of the authors and do not imply endorsement by Harvard University, Harvard Kennedy School, the Belfer Center for Science and International Affairs, or the Center for Research on Computation and Applied Sciences.

Design and layout by Andrew Facini

Copyright 2019, President and Fellows of Harvard College
Printed in the United States of America
Executive Summary

The Internet of Things (IoT) generally refers to a network of smart devices that can continuously sense or interact with their environment. These devices are able to communicate and respond to information that they gather, enabling the system to facilitate activities, streamline processes, and inform decision-making. IoT products have become more popular and visible in today’s society, in the form of applications such as consumer smart home electronics, transportation systems, or warehouse automation. Their usage will only continue to grow; 500 billion devices are expected to be connected to the Internet by 2030, with each device collecting data, interacting with the environment, and communicating over a network. This foreseeable outcome should encourage developers and users alike to pursue better awareness of and preparedness for the potential ways in which the public interest could be threatened. Important questions about accountability and transparency that address security and privacy issues must be included in policy conversations. This report offers a brief overview of the technology and its impact on public purpose.

What is the Internet of Things?

There is no single, universally accepted definition for the Internet of Things (IoT), but the term generally refers to the ever-increasing connectedness of everyday objects that can sense and interact with one another and with their environment. After surveying various definitions used by industry and interest groups in 2015, the Institute of Electrical and Electronics Engineers (IEEE) proposed the simple definition of a “network that connects uniquely identifiable ‘Things’ to the Internet,” where the “Things” are devices that can sense and interact according to their hardware and software capabilities.1

A draft report by the National Institute of Standards and Technology (NIST) described IoT as consisting of two foundational concepts, which can be combined to derive a definition:

“Components (some of which may have sensors and actuators that allow them to interact with the physical world) that are connected by a network providing the potential for a many-to-many relationship between components.”2

---

Important features of an IoT system include:

- **Embedded Computers**: Devices are programmed and controlled by an operating system with a specific function within a larger mechanical or electrical system.

- **Sensing/Actuation**: Devices contain sensors that gather information and detect changes in the environment in which they are deployed. Actuators can physically interact with the environment or activate/deactivate functionalities of other devices.

- **Connectivity**: Devices are connected to the Internet, generally through Wi-Fi, Bluetooth, cellular networks or other forms of connectivity.

- **Programmability**: Devices may receive application or system updates that can modify, enhance or alter their functionality.

- **Unique ID**: Devices should be uniquely identifiable, which means that they can be distinguishable and authorized to communicate with a human or another device.

- **Autonomy**: Devices may require some form of decision making capabilities even when disconnected from the Internet or other devices.

- **Ubiquity**: Devices are generally always operating and accessible.

### Common Applications and Market Development

IoT systems will touch on nearly every aspect of life. It is therefore useful to categorize these systems by their applications. One simple and broad way to do so is sorting based on whether the IoT device or system is for consumer or industrial use. The list below provides a useful – but not exhaustive – description of categories for IoT devices. For instance, these categories do not include self-driving cars, embedded medical devices, or other potential systems that would be classified within IoT (for examples of more applications, see Table 1).

- **Smart Wearables**, such as trackers that monitor health metrics, sleep patterns, or sports performance. Also, digital devices for communication, navigation, or entertainment.

- **Smart Home** devices for lighting, heating and air conditioning, security, or sanitation.

---

- **Smart City** projects, such as initiatives for smart infrastructure (e.g., traffic control, smart parking, waste management).

- **Smart Environment** systems that measure air/water quality, monitor climate, facilitate agricultural management, or support disaster prevention.

- **Smart Enterprise** encompasses general purpose functionalities for industry, such as logistics and transportation, product line automation, or retail inventory management.

IoT products or services have been introduced in nearly every area of society. The following table provides leading examples of IoT products that are currently used in different sectors.

### Table 1

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Product Types</th>
<th>Description of Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>Smart farming</td>
<td>Monitor crop field with sensors and automate irrigation system</td>
</tr>
<tr>
<td>Arts, Culture, and Tourism</td>
<td>Personalized hotel rooms</td>
<td>Adjust room settings (temperature, lighting, security, etc.); Provide concierge services</td>
</tr>
<tr>
<td>Business, Research, and Consulting</td>
<td>Supply chain management</td>
<td>Track inventory in retail stores and warehouses</td>
</tr>
<tr>
<td>Consumer Goods</td>
<td>Smart home devices</td>
<td>Assist with household chores (cooking, irrigation, utility controls, etc.)</td>
</tr>
<tr>
<td>Education</td>
<td>E-Learning Tools</td>
<td>Supplement education with connected tools; Introduce interactive modules; Monitor student progress</td>
</tr>
<tr>
<td>Energy and Climate</td>
<td>Energy use tracking</td>
<td>Process usage pattern and adjust use</td>
</tr>
<tr>
<td>Finance and Insurance</td>
<td>Proximity sensors (beacons) in retail banking</td>
<td>Provide customers with secure access and support (biometric authentication on phones; real-time branch analytics; personalized product offers)</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Remote health monitoring</td>
<td>Detect patterns and provide remote health assessment</td>
</tr>
<tr>
<td>Housing, Construction, and Real Estate</td>
<td>Smart buildings</td>
<td>Show building managers patterns in energy use by tracking circuit breakers and power meters; Report in real time on job site progress</td>
</tr>
<tr>
<td>IT and Geospatial</td>
<td>N/A</td>
<td>Location-tracking application</td>
</tr>
<tr>
<td>Media and Communications</td>
<td>Digital content</td>
<td>Deliver customers tailored content based on data collected from various input devices</td>
</tr>
<tr>
<td>Transportation and Logistics</td>
<td>Route mapping</td>
<td>Optimize real-time routing based on sensors</td>
</tr>
</tbody>
</table>
In recent years, more and more companies have entered the IoT market by offering new products and services that are either meant to support an IoT system or be integrated into one. Network companies such as AT&T, Cisco, and Huawei, as well as Cloud platform providers like Amazon, Google, and Microsoft already have IoT business solutions products. Electronics component manufacturers such as Intel and Qualcomm also offer integrated IoT platforms as B2B (business-to-business) services. In the consumer space, device manufacturers such as Bosch, Google, Amazon, Apple, and Samsung compete for a commanding share of the smart home market.

Public Purpose Considerations

Due to its ubiquitous nature, a fully realized IoT ecosystem will impact nearly every aspect of life. There are multiple areas of public purpose that are, and increasingly will be, highly relevant for IoT governance.

Security

As the number of connected devices in the Internet of Things continues to grow at a rapid pace, so do the opportunities to exploit potential security vulnerabilities. An increase in the “attack surface,” in cybersecurity terms. Bad actors could use poorly secured devices as entry points to access and compromise the security of anything connected to those devices. With the highly interconnected nature of IoT devices, any single poorly secured device can become a serious security issue for the entire network. The following are just a few examples of IoT security concerns:

- **Physical safety**: The ability to remotely access and control IoT-enabled devices presents a serious risk to the physical safety of users. These examples can range from hacked pacemakers and cars, which can result in death, to hacked smart home devices, which can enable theft and property damage.

- **System security**: Enterprises (industrial plants, energy utilities, or traffic control systems) using IoT systems for daily operations could become compromised, causing disruptions in crucial infrastructure and/or commercial activities and incurring huge economic costs. It is also important to note that the ever-increasing level of interconnectivity within and across networks means that even seemingly small security breaches have potential national security ramifications.

- **Data security**: As the quantity and quality of data tracked by the Internet of Things grows, so does the importance of protecting that data from theft and/or misuse. As mentioned above, increasing levels of interconnectedness in IoT systems also makes the sheer scale of potential data breaches that much larger and harder to manage.
Privacy

As the Internet Society puts it, “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.” The ubiquitous nature of IoT also makes privacy protection incredibly challenging, given the technology’s ability to produce quite invasive digital profiles of individuals by aggregating even anonymized data from disparate sources. Here are several examples of key privacy issues relevant to the Internet of Things:

- **New model of consent**: With ubiquitous linked sensors amassing information in real time, people's knowledge or control over the way in which their personal data is collected or used will become increasingly limited. To further complicate matters, the traditional “notice and consent” model breaks down when IoT systems don’t provide ways for users to interact with the devices and configure their privacy preferences.

- **Access by law enforcement**: IoT devices like security cameras and motion sensors can be quite useful for law enforcement in fighting crime and improving public safety. However, civil rights advocates and other groups have raised concerns about how private data is collected, stored, and used by government officials. Rules surrounding when and how law enforcement personnel can access and use someone's private data are ambiguous at best.

- **Bias and Inclusion**: As with any instance of data collection, IoT will predictably raise deep concerns about discrimination, especially with regard to how the collected data is used in decision-making processes. Possible areas where such data discrimination practices may arise include new employee recruitment, housing applications, or insurance claim assessments.4

---

4 Tschider, Charlotte. “Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age.” 2018
Current Governance and Regulation

Most relevant regulation so far has been focused on enabling technologies of IoT or adjacent technology areas, but legislation specifically addressing the Internet of Things has started to be introduced and will likely grow more prevalent in coming years.

**IoT-specific legislation**

- **IoT Cybersecurity Improvement Act** (S.734): Requires that “devices purchased by the U.S. government meet certain minimum security requirements” in order to address security risks that are growing with the proliferation of Internet-connected devices.  

- **SMART IoT Act** (H.R. 6032): “Directs the Secretary of Commerce to conduct a study on the state of the internet-connected device industry.”

- **Precision Agriculture Connectivity Act** (H.R. 4881): “establishes a task force, operating under the direction of the FCC and in collaboration with USDA, which will begin efforts to identify and recommend policies that will improve access to broadband on rural, agricultural lands and help farmers increase crop yields, reduce operating costs, and promote environmentally sustainable practices.”

- **California Senate Bill 327; Assembly Bill 1906**: Manufacturers are required to equip connected devices with a “reasonable security feature or features” that can protect the device and its information from “unauthorized access, destruction, use, modification or disclosure” (Both of these laws will take effect on January 1, 2020).

- **Secure by Design**: While technically not true legislation, this voluntary code of practice (CoP) was developed by the U.K. Department for Digital, Culture, Media and Sport (DCMS) to address security vulnerabilities of consumer IoT devices. Manufacturers of such devices who sign the CoP commit to implementing a certain minimum standard of security into the design of their products.

---


7 Ibid.


IoT-relevant governance

- The **General Data Protection Regulation (GDPR)** of the EU enforces protections for data privacy rights.\(^{10}\)

- The **EU Resolution on the Civil Law Rules in Robotics** sets forth general principles surrounding robotics development and AI use; ethical principles; IP rights and data; autonomous vehicles; drones; care and medical robots; education and employment; environmental impact; liability.

- The **FCC rules for 5G wireless infrastructure**, set in September 2018, places time limits on processing applications for mounting antennas on public infrastructure and provides fee guidelines for charging providers. The expected effect is limitation of state and local control over the network infrastructure.\(^{11}\)

- A 2015 **FTC report**, “Internet of Things: Privacy & Security in a Connected World,” outlines the benefits and risks of IoT and offers recommendations for broad-based privacy legislation and improved data security practices.\(^{12}\)

- In November 2018, the **Aspen Cybersecurity Group** published a set of *IoT Security First Principles* as a step toward shaping an environment that “incentivizes products be secure-by-design and increases consumer transparency.”\(^{13}\)

- Governance structures, in the form of industry associations, NGOs, and manufacturer frameworks, facilitate communication and cooperation across sectors and organizations.

- The **World Bank** has released a report on the nascent state of IoT implementation in governments and expressed a need to invest in digital capacity and IoT infrastructure.\(^{14}\)

- **Internet of Things Privacy Forum** published a report delineating privacy risks in IoT, which includes warnings about diminishing transparency and challenges to gaining meaningful consent for data collection.\(^{15}\)

- **Alliance for IoT Innovation (AIOTI)** seeks to help the European Commission “prepare future IoT research and innovation, standardization and policy.”

- **Open Connectivity Foundation (AllJoyn Project)** advocates for “open standards to enable all the ‘things’ in the Internet of Things to work together.”

- **Industrial Internet Consortium (IIC)** seeks to establish a “reference architecture for the IoT that can be exploitable by major industrial groups, particularly in the manufacturing field.”

---


Policy Questions for Consideration

Security

• How can we incentivize designers and developers of IoT systems to dedicate a sufficient level of resources and care into the security of those systems? Economists would call this “internalizing the negative externalities.”

• Is there a minimum standard of security (e.g., upgradeability and maintainability) that government should enforce in all IoT systems?

• Could existing product liability and consumer protection laws be adapted for unforeseen or unintended uses of devices? How can relevant stakeholders share responsibility and hold each other accountable for safety risks?

Privacy

• How can we rethink the way we obtain free and informed consent from people in an environment where ubiquitous IoT devices are continually collecting data?

• Is there a minimum standard of privacy protection (e.g., data anonymization and encryption) that government should enforce in all IoT systems?

• How can data collection practices be made more transparent, and privacy policies be made more accessible and understandable?

• What are privacy principles that can inform regulation on law enforcement access to data? What is the right balance between respecting individual civil rights and improving public safety?