Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated February 12, 2020

The Internet of Things (IoT): An Overview

The Internet of Things (IoT) is a system of interrelated devices connected to a network and/or to one another, exchanging data without necessarily requiring human-to-machine interaction. In other words, IoT is a collection of electronic devices that can share information among themselves. Examples include smart factories, smart home devices, medical monitoring devices, wearable fitness trackers, smart city infrastructures, and vehicular telematics. Potential issues for Congress include regulation, digital privacy, and data security as discussed below.

IoT Characteristics

IoT devices are often called "smart" devices because they have sensors and can conduct complex data analytics. IoT devices collect data using sensors and offer services to the user based on the analyses of that data and according to user-defined parameters. For example, a smart refrigerator uses sensors (e.g., cameras) to inventory stored items and can alert the user when items run low based on image recognition analyses. Sophisticated IoT devices can "learn" by recognizing patterns in user preferences and historical use data. An IoT device can become "smarter" as its program adjusts to improve its prediction capability so as to enhance user experiences or utility.

IoT devices are connected to the internet: directly, through another IoT device, or both. Network connections are used for sharing information and interacting with users. The IoT creates linkages and connections between physical devices by incorporating software applications. IoT devices can enable users to access information or control devices from anywhere using a variety of internet-connected devices. For example, a smart doorbell and lock may allow a user to see and interact with the person at the door and unlock the door from anywhere using a mobile device or computer.

IoT Categories

IoT devices are used in different fields for a broad range of functions. This section describes select IoT categories of frequent congressional interest.

Industrial Internet of Things (IIoT): The manufacturing industry has begun to adopt commercial IoT applications. Referred to as industrial Internet of Things (IIoT), networked machines in a production facility can communicate and share information with the goals of improving efficiency, productivity, and performance. The application of IIoT can vary significantly, from detecting corrosion inside a refinery pipe to providing real-time production data. Currently in North America, there are more consumer IoT connections than IIoT connections, but this may change in the future. IIoT has the potential to transform a variety of industries, including manufacturing, chemicals, food and beverage, automotive, and steel. The incorporation of IIoT and analytics is viewed by experts as the Fourth Industrial Revolution, or 4IR.

Internet of Medical Things (IoMT): The healthcare field has begun incorporating IoT, creating the Internet of Medical Things (IoMT). These devices, such as heart monitors and pace makers, collect and send patient health statistics over various networks to healthcare providers for monitoring, analysis, and remote configuration. At a personal health level, wearable IoT devices, such as fitness trackers and smart watches, can track a user's physical activities, basic vital data, and sleeping patterns. According to a 2019 survey by Pew Research, about one-in-five Americans uses a smart watch or fitness tracker.

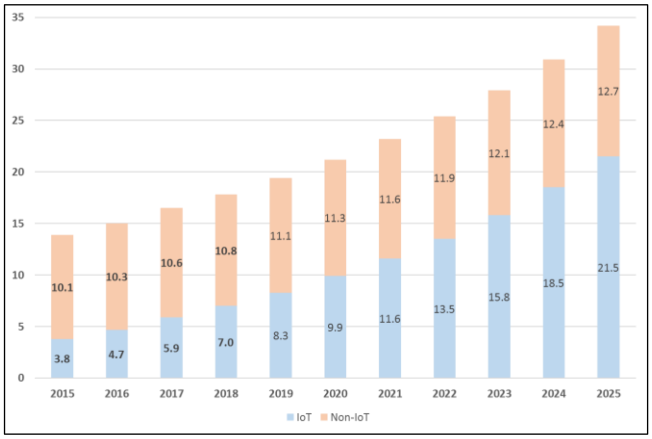
Smart Cities: IoT devices and systems in the utilities, transportation, and infrastructure sectors may be grouped under the category of "smart city." Utilities can use IoT to create "smart" grids and meters for electricity, water, and gas, where sensors collect and share customer usage data. This data is used to enable the central control system to optimize production and distribution to meet demand in real time. Cities can use transportation IoT for fare readers and status trackers or locaters that interface across all public transportation platforms. For example, Columbus, Ohio's winning proposal for the Department of Transportation's 2016 Smart City Challenge incorporated connected infrastructure that interacts with vehicles (including electric autonomous vehicles and shuttles), as well as a common payment and trip planning system across multiple transit systems.

Smart Homes: Consumer IoT devices used in homes and buildings are often grouped under the "smart home" category, including smart appliances, smart TVs, smart entertainment systems, smart thermostats, and network-connected light bulbs, outlets, door locks, door bells, and home security systems. These smart home IoT devices can be connected to a single network and controlled remotely over the internet via a mobile device or computer.

Global IoT Device Adoption

The market research firm IoT Analytics predicts the number of active IoT devices will grow from 9.9 billion in 2019 to 21.5 billion in 2025. While non-IoT device connections will also continue to increase, IoT devices will be about two-thirds of those connections by 2025, up from about one-third in 2019 (**Figure 1**).

Figure 1. Global Number of Connected Devices ($ Billions)



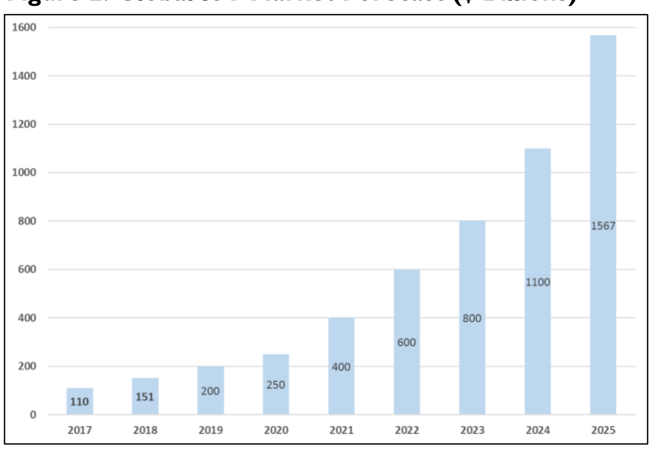
Source: Internet Analytics, August 8, 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

Notes: IoT devices do not include mobile devices, laptops, tablets, nor other computing devices. They are represented as Non-IoT devices. The figures do not include devices no longer in use. Non-bolded figures are estimates.

IoT Market Growth

The development, application, and usage of IoT will likely continue to grow with the deployment of fifth-generation (5G) cellular networks and technologies. These allow a larger number of devices to be connected simultaneously to a network and communicate with minimal delays, supporting not only consumer but industrial use of IoT devices and systems. The global IoT is expected to grow approximately 37% from 2017 to $1,567B by 2025 (**Figure 2**).

Figure 2. Global IoT Market Forecast ($ Billions)



Source: Internet Analytics, August 8, 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

Notes: Non-bolded figures are estimates.

Selected Policy Issues

Congress may take IoT-related legislative and/or oversight actions. Issues could include regulation, digital privacy, and data security among other policy issues.

Regulatory Issues: Emerging and converging technologies, such as IoT, may not align wholly with federal agency oversight jurisdictions. New technologies may be left unregulated, partially regulated, or more fully regulated under a newly developed framework. They could also be left to self-regulate by the industry, which is the case for many consumer IoT devices. Federal regulation of IoT may entail policies for deconfliction, harmonization, and/or expansion of agency jurisdictions.

Digital Privacy Issues: The IoT facilitates increased collection and consumption of data, posing potential privacy concerns. A piece or aggregation of the collected information could be used to identify, locate, track, or monitor an individual without the person's knowledge. The revealed patterns in their activities may also be exploited. The dilemma lies in that digital privacy and the advancement of smart technologies like IoT may be in direct opposition. Increased data collection and usage may yield innovation, technological progress, and improved utility, but could also lead to the erosion of privacy and data exploitation without consent.

Data Security Issues: Connected devices and systems offer the possibility of ubiquitous access, which equates to more possible entry points for both authorized and unauthorized users. As more devices become connected to one another and to the internet, the risk and impact of a compromise increase, along with the possibility of a cascading cyberattack. Data security is a tradeoff to consider between convenience and vulnerability.

The IoT links cybersecurity and physical security. For example, when smart doors and locks are remotely controlled by a malicious actor through cyberattack, the physical security of that building also becomes compromised. The damage may not be limited to loss of digital content or information. Loss of data physically stored in the compromised location as well as personal security could be jeopardized.

Many IoT devices do not employ strong encryption at the device or user interface level. Not implementing strong encryption may be intentional due to associated benefits—it usually reduces cost, increases battery life of devices, minimizes memory requirements, reduces device size, and is easier to use or implement. However, a system may become easier to break into if IoT devices are the most vulnerable points of a system.

Congress may choose to define the role of the federal government in overseeing digital privacy and data security through legislation that comprehensively addresses IoT issues or that revises specific authorities of federal agencies. In considering options, Congress may face three potential policy decisions: (1) whether data privacy and data security should be addressed together or separately in different laws, (2) whether various types of personal data should be treated equally or differently, and (3) which agencies should be responsible for implementing such laws.

Patricia Moloney Figliola, Specialist in Internet and Telecommunications Policy

Disclaimer