Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

June 4, 2019

Internet of Things (IoT): An Introduction

The Internet of Things (IoT) is a system of interrelated devices that are connected to a network and/or to each other, 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 complex data analysis programs (analytics). IoT devices collect data using sensors and offer services to the user based on the analyses of the 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 smartphone.

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 a goal 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. In 2018, over 400 million IoMT devices were connected worldwide, according to the market data company Statista. At a personal health level, wearable IoT devices, such as fitness trackers and smart watches, can track a user's physical activities, basic vitals, and sleeping patterns. According to one estimate, over 40 million fitness trackers IoT were in use in the United States in 2017.

Smart Cities: IoT devices and systems in 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 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. Columbus, Ohio's winning proposal for the Department of Transportation's Smart City Challenge of 2016 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 product IoT devices used in homes and buildings are often grouped under the "smart home" category, including smart appliances, smart TV, 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.

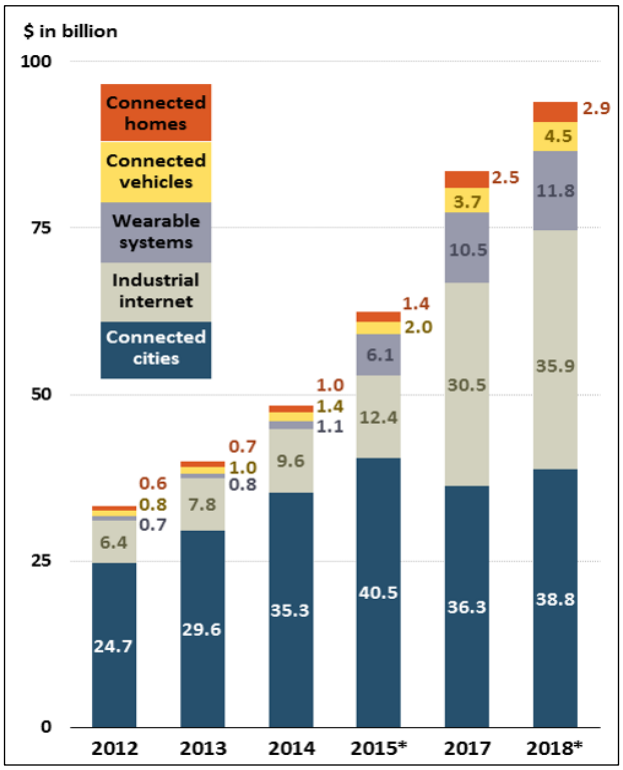
IoT Revenues

The IoT industry is a growing market both in the United States and globally. Statista estimated that there were over 700 million consumer IoT devices in use in 2017 in the United States and the 2018 U.S. IoT retail consumer market was worth almost $4 billion. **Figure 1** illustrates global IoT revenue from 2012 to 2018 (except 2016). Statista reported the total global IoT revenue in 2018 was about $93.9 billion. The connected smart cities category was the largest portion of 2018 global IoT revenue (41%). The IIoT had the biggest growth in terms of global revenue between 2017 and 2018 among the different categories and accounted for

38% of the 2018 total. The consulting firm McKinsey & Company projects IIoT systems to increase more than other IoT types by 2025. Consumer IoT devices, such as wearables and connected smart home devices, generated 16% (over $14 billion) of global revenue in 2018. Statista estimated the 2018 global smart home market size as over $30 billion with revenue of $2.9 billion. The connected smart vehicles category generated the remaining 5% ($4.5 billion) of global revenue in 2018.

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.

Figure 1. Internet of Things Subsystems Revenue Worldwide from 2012 to 2018 (Except 2016)



Source: CRS created based on data from Statista, "Revenue of Internet of Things Subsystems Revenue Worldwide from 2012-2018 (in billion U.S. dollars)," https://www.statista.com/statistics/503466/iot-subsystems-revenue-worldwide/.

Notes: 2016 data unavailable. Estimates signified by *.

Selected Policy Issues

Congress may take legislative and/or oversight actions related to the IoT. Congressional action may focus on regulation, digital privacy, and data security among other policy issues. These issues may also apply to several other emerging technologies.

Regulatory Issues: Emerging and converging technologies, such as the IoT, may not align wholly with federal agency oversight jurisdictions and legal and regulatory authorities. Congress may consider the federal regulatory role in an environment where technologies evolve quickly. 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 currently the case for many consumer IoT devices. Federal regulation of technologies such as the 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 digital privacy concerns, especially for consumers. 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 the IoT may be in direct opposition. Increased data collection and usage may yield innovation, technological progress, and improved utility. However, increased data collection and usage could also lead to erosion of privacy and data exploitation without consent.

Data Security Issues: Connected devices and systems such as IoT 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 each other and to the internet, the overall risk and impact of a compromise increase, along with the possibility of a cascading effect of a 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.

Currently, 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 and are targeted by malicious actors for exploitation.

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.

Suzy E. Park, Analyst in Science and Technology Policy

Disclaimer