GAO

United States Government Accountability Office

Center for Science, Technology, and Engineering

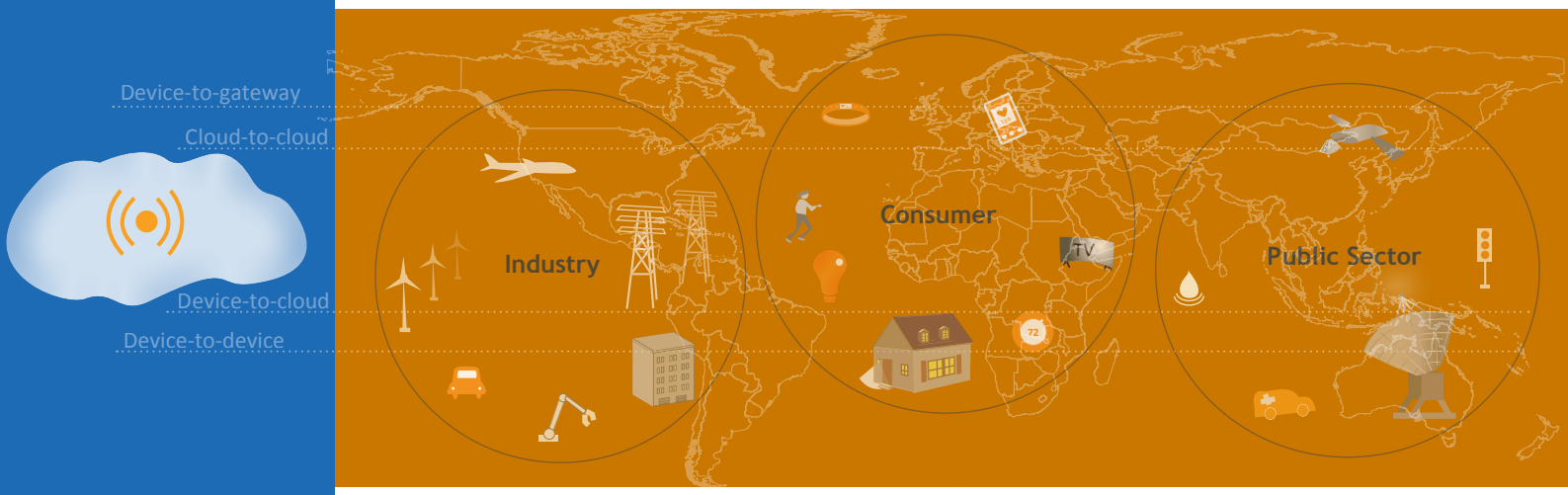
Report to Congressional Requesters

May 2017

TECHNOLOGY ASSESSMENT

Internet of Things

Status and implications of an increasingly connected world



GAO-17-75

The cover image is GAO's rendition of the diverse nature of the Internet of Things. The "things," or objects, in the Internet of Things range from wind mills, to lightbulbs, to traffic lights. These objects are grouped based on the primary user: ¬ consumer, industry, and public sector. The connection symbol in the cloud on the left hand side represents the network—typically the Internet—used to connect these objects, which are connected to the network using four different architectures (device-to-gateway, cloud-to-cloud, device-to-cloud, and device-to-device). The background of the world map portrays that the technologies used globally.

Highlights of GAO-17-75, a report to congressional requesters

May 2017

Why GAO did this study

The rapid, global proliferation of IoT devices has generated significant interest. In light of the current and potential effects of the IoT on consumers, businesses, and policy makers, GAO was asked to conduct a technology assessment of the IoT.

This report provides an introduction to the IoT and describes what is known about current and emerging IoT technologies, and the implications of their use.

To conduct this assessment, GAO reviewed key reports and scientific literature; convened two expert meetings with the assistance of the National Academies; and interviewed officials from two agencies to obtain their views on specific implications of the IoT.

Ten federal agencies and twelve experts reviewed the draft report and some provided technical comments, which were incorporated as appropriate.

View GAO-17-75. For more information, contact Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov or Mark Goldstein at (202) 512-6670 or goldsteinm@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

TECHNOLOGY ASSESSMENT

Internet of Things

Status and implications of an increasingly connected world

What GAO found

The Internet of Things (IoT) refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. These "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and respond automatically to improve industrial processes, public services, and the well-being of individual consumers. For example, a "connected" fitness tracker can monitor a user's vital statistics, and store the information on a smartphone. A "smart" tractor can use GPS-based driving guidance to maximize crop planting or harvesting.

Electronic processors and sensors have become smaller and less costly, which makes it easier to equip devices with IoT capabilities. This is fueling the global proliferation of connected devices, allowing new technologies to be embedded in millions of everyday products. The IoT's rapid emergence brings the promise of important new benefits, but also presents potential challenges such as the following:

- **Information security.** The IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet.

- **Privacy.** Smart devices that monitor public spaces may collect information about individuals without their knowledge or consent. For example, fitness trackers link the data they collect to online user accounts, which generally include personally identifiable information, such as names, email addresses, and dates of birth. Such information could be used in ways that the consumer did not anticipate. For example, that data could be sold to companies to target consumers with advertising or to determine insurance rates.

- **Safety.** Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners. For example, in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission.

- **Standards.** IoT devices and systems must be able to communicate easily. Technical standards to enable this communication will need to be developed and implemented effectively.

- **Economic issues.** While impacts such as positive growth for industries that can use the IoT to reduce costs and provide better services to customers are likely, economic disruptions are also possible, such as reducing the need for certain types of businesses and jobs that rely on individual interventions, including assembly line work or commercial vehicle deliveries.

Table of contents

Figures

Tables

Abbreviations

DIGIT	Developing Innovation and Growing the Internet of Things
DOT	Department of Transportation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FIP	Fair Information Practices
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GE	General Electric
IEEE	Institute of Electrical and Electronics Engineers
IFTTT	If This Then That
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
MEMS	Micro-electromechanical systems
NAS	National Academy of Sciences
NGMN	Next Generation Mobile Networks Alliance
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Cooperation and Development
PAN	Personal area network
SABRE	Semi-Automatic Business Research Environment
US-CERT	United States Computer Emergency Readiness Team

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 15, 2017

Congressional Requesters

The term "Internet of Things" (IoT) is generally defined as the concept of connecting and interacting through a network with a broad array of "smart" devices, such as fitness trackers, cameras, door locks, thermostats, vehicles, or jet engines.[1,2] Implemented around the world, the IoT is potentially affecting economies and societies in ways both great and small, from consumer products to industrial processes and public services. As the electronic processors and sensors that enable the IoT have become smaller and less costly, it has become easier to equip devices with computing and communications capabilities that dramatically enhance their usefulness and efficiency. A device that is IoT-enabled is often referred to as a "smart" or "connected" device, inasmuch as its connection to networks or the Internet offers additional capabilities and functionality.[3] The additional capabilities and functions can include enhanced smart device tracking and monitoring; new ways of gathering, analyzing, and correlating data generated by smart devices; and new service-related business opportunities based on data analysis. With the IoT, these devices can communicate on a larger scale and process information that has never been captured before and, in some cases, respond automatically to improve industrial processes, public services, and the well-being of individual consumers. For example, utilities may be able to use smart grid technologies to more efficiently manage the distribution of electricity service, while a single homeowner may be able to remotely shut a garage door inadvertently left open, from across the country.

As IoT technologies are embedded in a growing number of devices and applications, the number of connected devices is expected to increase. In 2013, the number of devices connected to the Internet globally was estimated to be over nine billion.[4] According to the McKinsey Global Institute, an estimated 25 to 50 billion devices will be connected to the Internet by 2025.[5] In 2015, the Organisation for Economic Cooperation and Development (OECD) estimated that a

[1] Although the IoT implies the Internet is the mode of communication, local networks can also transmit information collected by sensors. A June 2016 report from the National Institute of Standards and Technology (NIST) states the IoT has its 'things' tethered to the Internet, while the Network of Things has its 'things' tethered to any network. However, NIST uses the two terms interchangeably throughout the report. For the purposes of this technology assessment, the IoT refers to information collected and transferred both by the Internet and local networks.

[2] Networks are interconnected hardware components (such as routers, hubs, and cabling) and software protocols that allow devices to share data with each other.

[3] Smartphones, smart locks, smart thermostats, and smart cameras, are examples of "smart" devices discussed in this report. The terms "smart device" and "connected device" are used interchangeably throughout the report.

[4] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (2015). Joseph Bradley, Joel Barbier, and Doug Handler, *Embracing the Internet of Everything to capture your share of $14.4 trillion* (Cisco, 2013).

[5] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (June 2015).

family of four had an average of 10 devices connected to the Internet in their household and that this average will increase five-fold to 50 devices by 2022.[6]

The proliferation of connected devices and the way that new technologies are embedded in millions of everyday products presents challenges and implications for the use of the IoT. For example, in October 2016, one security incident involving IoT devices rose to national attention. A distributed denial of service attack targeted a company that manages Internet infrastructure. Due to this attack, several major websites were unavailable throughout the day.[7] The attack appeared to have used hundreds of thousands of IoT devices, such as Internet-connected cameras and baby monitors, directing them without the users' knowledge to overwhelm the targeted sites.

In light of the current and potential effects of the IoT on consumers, businesses, and policymakers, you asked us to conduct a technology assessment of the IoT. This report provides an introduction to the IoT and describes: (1) what is known about current and emerging IoT technologies, (2) how and for what purpose IoT technologies are being applied, and (3) potential implications of the use of IoT technologies.

To address these objectives, we reviewed key reports and scientific literature describing current and developing IoT technologies and their uses, concentrating on consumers, industry, and the public sector. We interviewed agency officials from the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC), researchers, and other industry experts. We participated in conferences on the latest uses and implications of the IoT to discuss and gather data and viewpoints from various perspectives. In addition, we collaborated with the National Academy of Sciences (NAS) to convene two meetings of experts, one focused on IoT technologies and the other focused on the implications of those technologies. The experts participating in the meetings specialized in various disciplines including computer science, security, privacy, law, economics, physics, and product development, and were from federal government agencies, academia, technology companies, and standards setting organizations that develop international standards. We continued to draw on the expertise of these individuals throughout our study.

We conducted our work from September 2015 to May 2017 in accordance with all sections of GAO's quality assurance framework relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis

[6] This estimate applies to an average family of four located in OECD countries. OECD, *OECD Digital Economy Outlook 2015* (Paris: OECD Publishing, 2015).

[7] Major websites affected by the attack include: Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times, among others. Nicole Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.", *The New York Times*, October 21st, 2016, accessed October 26th, 2016, http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

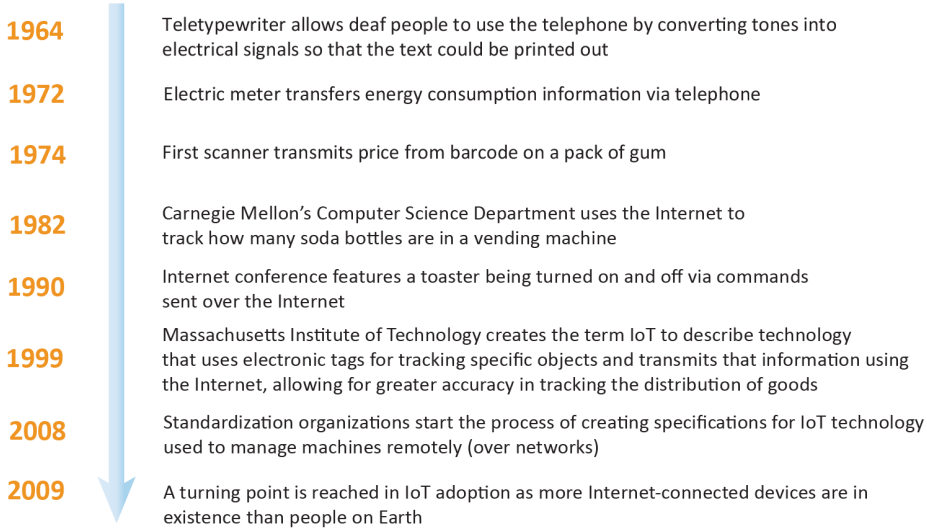
for our findings in this product. More details about the objectives, scope, and methodology can be found in appendix I.

1 Background

IoT devices sense and communicate information and, in some cases, act upon that information. Rather than relying on humans for direct input—for example, with a keyboard, a mouse, or a touchscreen—IoT devices can also capture information directly from the environment through sensors. By leveraging the interconnectedness of a network, the IoT device becomes "smart," meaning it can create, communicate, aggregate, analyze, or act on information, which can increase its value. The idea of connecting objects to a network is not new; however, recent advances in the underlying technologies for the IoT have allowed more objects to become interconnected. Figure 1 outlines milestones in the development of IoT devices.

As seen in figure 1, versions of connected objects have existed for decades. However, recent advances in the technologies that support IoT devices have accelerated their adoption. These technology advances include:

- **Miniaturized, inexpensive electronics**: The cost and size of electronics are decreasing, making it easier for the electronics to be embedded into objects, enabling them as IoT devices. Smartphones are one of the drivers behind these advances in electronics used



Source: GAO. | GAO-17-75

Figure 1: Milestones towards the development of IoT devices

in the IoT.[8] As the smartphone market has expanded to encompass billions of products, the electronics within smartphones—sensors, screens, and communication chips—are also manufactured in large quantities.[9] These electronics have become smaller to meet the requirements of smartphone developers, and less costly due to the quantities being produced. For example, the prices of sensors have steadily declined over the past decade. One type of sensor, called an accelerometer, which can be used to detect the acceleration of a device, cost an average of $2 in 2006; the average price declined to 40 cents in 2015.

- **Ubiquitous connectivity:** The expansion of networks and decreasing costs allow for easier connectivity. Easily accessible, pervasive networking allows for IoT devices to be connected almost anywhere. An example of how networks have expanded is with Wi-Fi.[10] The first computer with a Wi-Fi option was offered in 1999. In 2012, nearly two-thirds of households in the United States had Wi-Fi.[11] The adoption of smartphones has also accelerated connectivity, as smartphones can connect to multiple types of networks, such as Wi-Fi, cellular, and Bluetooth.[12,13]
- **Cloud computing:** Cloud computing allows for increased computer processing capabilities.[14] Since IoT devices can create a large amount of data, these devices can require large amounts of computing power to analyze the data. Cloud computing is one way to obtain this computing power. This means that the IoT device itself does not need to have the computation or storage capability, but can remotely access cloud computing instead. In addition, the cost of data storage has decreased to the point that cloud computing can store more data for longer periods of time, allowing for the accumulation of large amounts of data.[15]

[8] Smartphones combine the telecommunications functions of a mobile phone with the processing power of a computer, creating an Internet-connected mobile device capable of running a variety of software applications for productivity or leisure.

[9] Sensors collect information about the environment, such as temperatures or changes in motion.

[10] Wi-Fi is an example of a wireless computer network localized to a limited geographic area. A Wi-Fi network uses a set of broadband wireless networking standards, known as Institute of Electrical and Electronics Engineers (IEEE) 802.11x.

[11] Number of households using Wi-Fi from Strategy Analytics, *Connected Home Devices Service* (March 2012).

[12] Cellular is an example of a wireless network, such as 3G and 4G networks, used in mobile telecommunication. Mobile telecommunication technologies, including cell phones and systems, are classified by the generation they belong to. Third generation (3G) phones were developed in the late 1990s and 2000s to improve the data capability and speed. 3G phones were defined by the Third Generation Partnership Project. 4G is the fourth generation of wireless mobile telecommunications technology, succeeding 3G.

[13] Bluetooth is a communication protocol that enables short range wireless connection.

[14] According to NIST, cloud computing generally possesses five essential characteristics: (1) On-demand self-service, which allows consumers to acquire computing capabilities automatically and as needed; (2) Broad network access, which provides capabilities over a network accessed with standard devices (e.g., a mobile phone, tablet, laptop, and workstation); (3) Resource pooling, which refers to the ability of vendors with combined computing resources to serve multiple consumers at the same time; (4) Rapid elasticity, which refers to the ability to vary resources commensurate with demand; and (5) Measured services, which are incrementally valued, typically on a pay-per-use, or charge-per-use basis. Tim Grance and Peter Mell, *The NIST Definition of Cloud Computing*, accessed November 3rd, 2016, https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf.

[15] OECD, *OECD Digital Economy Outlook 2015* (Paris: OECD Publishing, 2015).

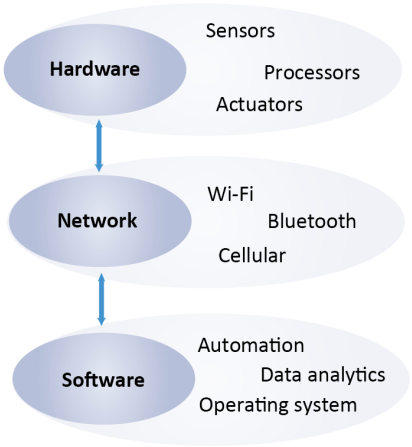
- **Data analytics:** Advances in data analytics have allowed for the efficient analysis of the rapidly increasing amounts of data created by IoT devices. New advanced analytical tools can be used to examine large amounts of data to uncover subtle or hidden patterns, correlations, and other insights. Advanced algorithms in computing systems enable the automation of functions that appear to require the ability to reason. For example, an algorithm may use data on weather, traffic, and road service capabilities to provide commuter alerts and suggest alternative routes. These advances in data analytics allow valuable information to be extracted from the data collected by IoT devices.

2 The IoT: A current model and emerging technologies

IoT devices consist of three common components and these components are supported by different technologies. Additionally, several common architecture models are used to describe how IoT devices connect to a network to collect, share, and communicate information. As the IoT evolves, different technologies are emerging to address specific IoT related capabilities.

2.1 Common components of the IoT

While IoT devices serve a wide array of purposes, they all consist of three common components: hardware, network connectivity (referred to as 'network'), and software. These components, and some examples of each, are shown in figure 2 and discussed below.



Source: GAO. | GAO-17-75

Figure 2: Components of an IoT device

2.1.1 Hardware

The hardware used in IoT devices consists of the embedded components—sensors, actuators, and processors, among others. Sensors collect information about the IoT devices' environment, such as temperatures or changes in motion. Actuators perform physical actions, such as unlocking a door. Processors serve as the "brains" of IoT devices, supporting the computing platform for the network and software components and interfacing with the sensors and actuators.

2.1.2 Network

The network component of an IoT device connects it to other devices and to network-accessible computer systems. Different IoT devices can connect via different digital communications methods, including wired or wireless methods. Wired devices typically connect to a network through an Ethernet connection via copper or fiber-optic cable. Wireless devices typically connect via the radio frequency spectrum. Bluetooth and Wi-Fi are commonly used short-range wireless connections, while cellular is used for long range wireless connections.[16] Wireless communications allow devices to remain

[16] Cellular networks are wireless telecommunications networks managed by service providers. These networks support smartphones which provide voice calling capabilities as well as Internet connectivity for smartphone-enabled applications, such as e-mail and Web browsing. These networks also support cellular data cards, or mobile broadband modems, which provide Internet connectivity to tablets and laptop computers.

connected to a network while mobile. Depending on the communication needs—such as transmission range, data transmission rate, and power—one or more network communications technologies can be incorporated into IoT devices.

Different types of networks operate over different ranges. For example, IoT devices can use a personal area network (PAN) to transmit data over a distance of about 10 meters (e.g., Bluetooth inside a room), a local area network to transmit data over an area of about 100 meters (e.g., Wi-Fi within a house), and a wide area network to transmit data over an even wider area, encompassing buildings or cities (e.g., cellular transmission). In addition to range needed, IoT devices may use different networks based on other factors such as available power.

IoT devices can be uniquely identified on their networks by being assigned "addresses." If an IoT device connects via the Internet, the Internet Protocol version 4 (IPv4) can be used. IPv4 provides approximately 4.3 billion unique Internet Protocol (IP) addresses, and is currently the most commonly used addressing system for the Internet. However, as the number of devices connecting to the Internet has grown with computer systems and IoT devices, all of the available addresses in the IPv4 scheme have been assigned. Some Internet users are transitioning to Internet Protocol version 6 (IPv6), which provides approximately 340 trillion trillion trillion (3.4×10^{38}) unique IP addresses. We have previously reported that IPv6 has superior scalability and identifiability features compared to IPv4 and allows each device—wired or wireless—to have a unique IP address independent of its current point of attachment to the Internet.[17] Since the number of IoT devices is projected to continue growing, IPv6 can address the need for more IP addresses to facilitate unique identification. However, challenges associated with several aspects of IPv6 adoption, including security management, implementation in current business applications, interfaces with business partners that are not IPv6 enabled, maintaining dual IPv6 and IPv4 environments, and the adoption of new standards, have delayed the transition from IPv4 to IPv6.

2.1.3 Software

Software in IoT devices performs a range of functions, from basic operations to complex analyses of collected data. For example, software of one IoT device may translate data from one format to another. Other software might analyze data to monitor the functionality of complex machines. Software for jet engines, for example, could collect the measurements from an engine's sensors and determine whether the engines require maintenance.

The software component may also include data analytics to find patterns, correlations, or outliers, among other information, in the collected data. Such information can inform users or determine and convey an action the IoT device needs to make. For example, IoT-enabled thermostats can use sensors to collect information about when consumers change the temperature in their homes, and

[17] For more information, see GAO, *Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain*, GAO-06-675 (Washington, D.C.: September 30th, 2006).

then use software to perform data analytics to automate the temperature change so that it mimics consumer usage patterns.

Although some software can be deployed within the IoT device itself, software performing complex data analysis is typically performed using cloud computing (also known as the cloud). Cloud computing applications are network-based and scalable. The cloud infrastructure may include servers, networks, and software. For the IoT, this means computing power does not have to physically reside on the device, or even at the same location as the device, allowing for devices to be placed in areas too remote or small to power and house a conventional computer.

2.2 Architectures: Connecting devices to collect, share, and use information

The components of the IoT—hardware, network, and software—must be connected for the device to be functional. An Internet Architecture Board guidance document released in 2015 presented four basic architecture models for networking smart objects, useful for all IoT devices: [18]

1. Device-to-device
2. Device-to-cloud
3. Device-to-gateway
4. Cloud-to-cloud

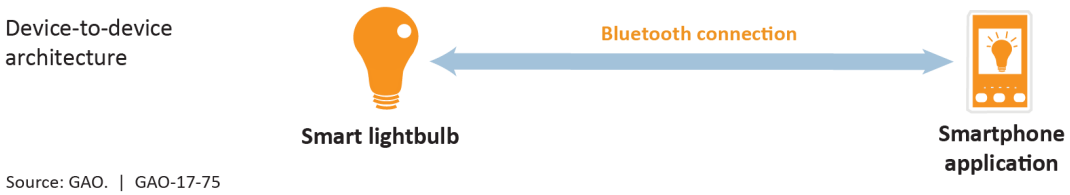
These models are the foundation for collecting, sharing, and using information from IoT systems.

2.2.1 Device-to-device architecture

IoT devices within the same network that generally connect using wireless PAN protocols, such as Bluetooth and Zigbee, are "device-to-device" architectures.[19] Home automation products like IoT-enabled smart lightbulbs use this architecture. For example, a user turns the smart lightbulb on or off over a network using a smartphone application. Figure 3 shows an example of home automation illustrating Bluetooth, as the wireless PAN, connecting a smart lightbulb with a smartphone application.

[18] H. Tschofenig, J. Arkko, D. Thaler, D. McPherson, *RFC 7452: Architectural Consideration in Smart Object Networking* (Internet Architecture Board, March 2015).

[19] Zigbee is a communication protocol that enables short range wireless connection to create a PAN. Unlike Bluetooth which uses the IEEE 802.15.1 specification standard, Zigbee uses the IEEE 802.15.4 standard to create a low power, secure short range network.



Source: GAO. | GAO-17-75

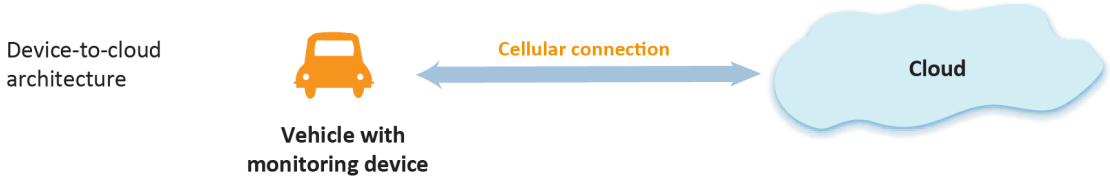
Figure 3: Example of a device-to-device architecture

2.2.2 Device-to-cloud architecture

In device-to-cloud architectures, IoT devices connect directly to the cloud, typically using a long range communications network, such as cellular. For example, IoT-enabled vehicle monitoring devices (such as those provided by car insurance companies to drivers) collect data on the vehicle, such as distances and speeds driven, and acceleration and braking rates. These data are then transmitted to the cloud, analyzed in the cloud, and used by insurance companies to create tailored insurance rates based on the driving data. Figure 4 depicts the connection between the car and the cloud using the cellular network.

2.2.3 Device-to-gateway architecture

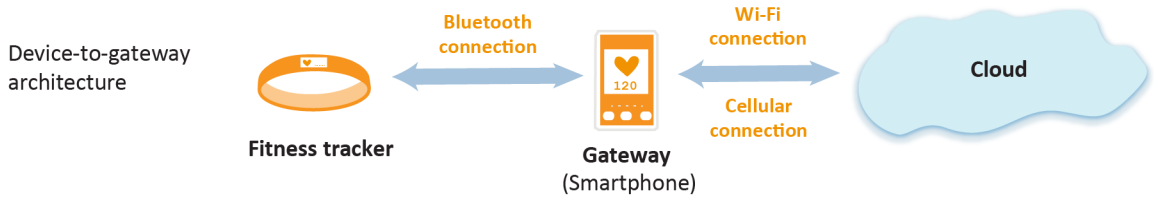
Device-to-gateway architectures transfer information from sensors to the cloud via a gateway device. Gateways are used to bridge different networks and communication technologies. For example, an IoT device could use a short-range communication technology to connect to the gateway, and then the gateway uses a long-range communication technology to connect to the cloud. The gateway may also provide security or act as a preliminary data aggregator, consolidating data from several devices. In addition, one expert told us a critical benefit of the device-to-gateway architecture is the ability to increase interoperability. As standards continue to evolve, gateways can interface with IoT devices using various



Source: GAO. | GAO-17-75

Figure 4: Example of a device-to-cloud architecture

standards. An example of an IoT device that uses the device-to-gateway architecture is an IoT-enabled fitness tracker, as depicted in figure 5. The fitness tracker creates data on physical activity, which is transferred over Bluetooth to a gateway device, in this example a smartphone.[20] The gateway collects the data and then communicates the data to the cloud through additional network connectivity, such as Wi-Fi or cellular connection.



Source: GAO. | GAO-17-75

Figure 5: Example of a device-to-gateway architecture

2.2.4 Cloud-to-cloud architecture

Cloud-to-cloud architecture, also known as back-end data sharing, enables third parties to access uploaded data from IoT devices. For example, smart buildings receiving data from smart thermostats and smart lightbulbs can send the data to a cloud via Wi-Fi (figure 6). The collected data are then aggregated in cloud 1, which may be owned by the building manager. The building manager could then share the data with the energy company, who stores it in its own cloud, cloud 2. If the energy company can access similar data from other building managers, the energy company can aggregate all these data to help predict energy demands by analyzing the amount of energy used according to different factors, such as time or weather.

These four basic architectures demonstrate underlying design strategies enabling connection to networks. IoT implementation of these architectures has traditionally relied on proprietary approaches, in which a vendor uses hardware, network, and software components that are custom designed, and may not be interoperable with other vendor systems. For example, in one smart home, vendor A's smart lightbulb may not work with vendor B's smart lock because they operate using different components. However, some vendors have developed specialized solutions to work with other vendors' IoT devices. One such solution is a website called IFTTT (If This Then That), which allows a user to automate tasks that can control IoT devices using "conditional triggers."[21] For example, using IFTTT

[20] The smartphone is considered a gateway, since the fitness tracker data has to pass through the smartphone to get to the cloud; the fitness tracker does not have a direct connection to the Internet. In the vehicle monitoring device example (figure 4), a smartphone is not required to be a gateway, since the device talks directly to the cloud over cellular. In the smart lightbulb example (figure 3), there is no cloud, as the lightbulb connects directly to the smartphone via Bluetooth.

[21] IFTTT, Do More with the Services You Love, accessed December 2, 2016, https://ifttt.com

as the conduit, a user can set a smart thermostat to activate when the user's car approaches their house (the conditional trigger in this example being the location sensor within the car). A 2015 Internet Society report noted that device interoperability and open standards are key considerations in the design and development of IoT systems. [22]

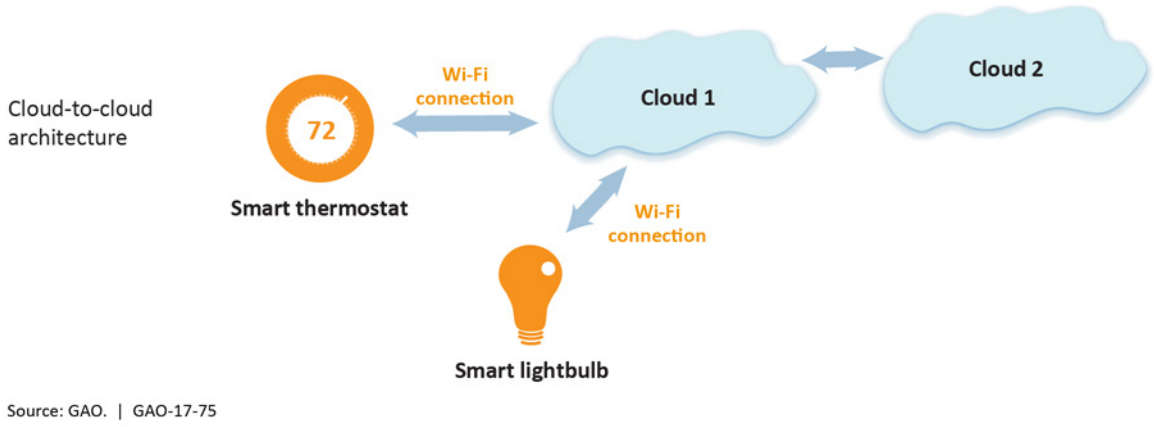


Figure 6: Example of a cloud-to-cloud architecture

[22] The Internet Society, *The Internet of Things: An Overview* (2015).

2.3 Developments in hardware, networks, software, and business opportunities

IoT component technologies are increasingly specialized. Manufacturers are tailoring designs specifically for IoT uses, whereas previously, IoT devices and systems were developed from various existing technologies. Additionally, while industry previously focused on using IoT data to improve manufacturing processes, it now focuses more on using the data to enhance service relationships.

2.3.1 Hardware: Designing for low power and limited space

Power consumption can be a constraint when designing IoT devices, as they require power to sense, analyze, and communicate information. Often, IoT devices may not have space for a large power source. IoT devices can also be placed in areas that are difficult to access, making it hard to replace a power source like a battery. One expert attending our meeting on IoT technologies stated there have been advances in energy sources and storage for IoT devices, but more progress is needed. The subject of IoT device power is becoming a significant area of research, with increased interest in how devices can harvest energy from the ambient environment.

Processors have also become more compact and more energy efficient. For example, one semiconductor company has designed a line of very small embedded processors for IoT devices. These processors are designed to provide high quality graphics for smart TVs while operating on low power. The company offers other processors that are physically small and can enable Internet connectivity with embedded networking. IoT devices such as fitness trackers use these processors.

2.3.2 Network: Connectivity emerging to support the IoT

Network connectivity needs are changing as new IoT technologies are being created. New types of networks and protocols are being developed to address evolving IoT hardware and software requirements. For example, Bluetooth was first introduced in 1999 to be used for short-range communications. The Bluetooth Low Energy protocol was developed to use about half the energy of Bluetooth. Another example of a new network technology is the emerging cellular technology known as the 5G network.[23] The 5G network is the next iteration of cellular technology and is expected to be rolled out by 2020, according to the Next Generation Mobile Networks Alliance (NGMN). NGMN considered the specific needs of IoT devices, among others, to design and build the 5G network. The 5G network is projected to have lower latency, better coverage, faster Internet connections, and to allow for more connections than the existing cellular network, all of which may enable more IoT devices to be connected.

2.3.3 Software developments in the IoT

Software developments projected to advance IoT development include: (1) analysis programs that can condense large volumes of IoT data into actionable information, (2)

[23] 5G refers to the fifth generation of mobile wireless technology.

software tailored for the IoT, and (3) "smart" programs that can augment or replace a human operator.

Aggregated data gathered from IoT devices can undergo sophisticated data analysis techniques, or analytics, to find patterns and to extract information and knowledge, enhancing decision-making.[24] For example, health care IoT devices—such as sensors that can be swallowed—gather and extract information about the patient's daily routine, which can improve the accuracy of clinical trials. Another analytics method is speech recognition, which can extract information from a wide variety of talking speeds, accents, and background noise. This method can be implemented to augment IoT devices, such as enabling voice control over smart televisions to change channels or adjust the volume. Data analysis can be used by businesses as well. For example, it can track and analyze consumer behavior or driving patterns, the latter of which can be used to determine driver risk and set insurance rates.

Analytics methods apply to large data sets that may be derived from sources other than the IoT. However, developments in the IoT have led to the release of software specific for IoT needs, such as operating systems. These operating systems are intended for use in low-power IoT devices and support device connectivity. Other IoT software may consist of custom elements for particular applications. For example, a participant at our expert meeting mentioned that, to handle updating IoT software on moving objects, they implemented remote, modular updating capabilities. Then, if the object goes out of range during an update, the update pauses and continues from where it left off when the object is back in range.

IoT software developments permitting automation may reduce the need for human operators in certain capacities. Such software relies on augmented intelligence and behavior to substitute for human judgement and actions, respectively. For example, IoT sensor data can be analyzed and then acted upon to reduce waste, energy costs, and the need for human intervention during industrial production. Power, for either the consumer home or in data centers, can be managed by employing software that balances home energy consumption patterns or computing loads.[25] Further, automation using the IoT may be implemented in complex systems, such as the self-driving car, which is predicted to be commercialized within 5-20 years. [26] Such systems require both hardware and software and are expected to react in real-time to unpredictable conditions, potentially without human input.

2.3.4 Changing business opportunities

Implementation of the IoT is shifting the focus of some industries from manufacturing to service-based relationship business. For example, General Electric (GE) has transformed its industrial line of business from the building and sale of lightbulbs and

[24] For further information on advanced data analytics, see GAO, *Data and Analytics Innovation: Emerging Opportunities and Challenges*, GAO-16-659SP (Washington, D.C.: September 20th, 2016).

[25] In the case of home automation, such data may be uploaded to a centralized location, such as a data cloud, for analysis.

[26] Anderson, James M., Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras and Oluwatobi A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers* (Santa Monica, CA: RAND Corporation, 2016).

appliances to a manufacturing and services line of business that not only builds complex industrial machines, but also provides an ongoing maintenance service offering based on the performance data gathered from the IoT technologies built into the machines it manufactures.

GE installed sensors in its gas turbines and jet engines connecting them to the cloud and enabling the analysis of the resulting flow of operational data to identify ways to improve productivity and reliability. In 2013, GE produced an analytics platform using software to manage data produced by its industrial machines.[27] The cloud-based analytics platform provides a common architecture, combining intelligent machines, sensors, and advanced analytics to convert data from machines produced by GE into service and maintenance offerings for its corporate customers. Some of the services GE provides include condition-based maintenance, fuel consumption analysis, outage management, and controls and plant automation.

[27] In 2015, GE developed a cloud based service for its industrial customers.

3 Uses and benefits of the IoT for consumers, industry, and the public sector

IoT devices are used across multiple sectors and by various groups and individuals to inform future actions and decision-making.[28] The IoT can be used in almost any circumstance in which human activity or machine function can be enhanced by data collection or automation. We identified three primary users of the IoT: consumers, industry, and the public sector. Consumers can use IoT devices to collect personal information towards monitoring health and automating household functions, among other things. Industry can use IoT devices to optimize processes and generate cost savings. Communities and other public sector entities can use IoT devices to address concerns such as changes in the environment. There are many other uses of IoT devices. Examples of IoT devices can be found in appendix II.

3.1 Wearables

Wearable IoT devices, such as fitness trackers, smart watches, or smart glasses, collect personal data using sensors, analyze the data, and communicate information to the consumer. The most commonly recognizable examples of wearable IoT devices are fitness trackers, used to monitor physical activity, such as steps taken or heart rate, enabling consumers to track their physical activity over time. In 2015, the McKinsey Global Institute (McKinsey) Report on the IoT estimated that approximately 130 million people use fitness trackers worldwide.[29] Data from the fitness trackers are easily shared, allowing for feedback and reinforcement from others. An example of an IoT fitness tracker worn as a wristband is depicted in figure 7.

Source: Jawbone. | GAO-17-75

Figure 7: Example of a wearable IoT device

Other wearable IoT devices include clothing, such as IoT-enabled baby clothes that monitor respiration, temperature, and activity levels. IoT-enabled football helmets detect, and analyze impacts and notify medical staff, if needed. Smart glasses that use augmented reality are other examples of wearable IoT devices.[30] These glasses allow the user to see the physical world overlaid with digital material, with applications for surgeons, mechanics, engineers, and firefighters, among others.

[28] For the purposes of this report, we use the term sector to refer to an area of use or category of activity.

[29] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (2015).

[30] Augmented reality is created when the real world is viewed through a device, such as a smartphone camera, and a digital image is superimposed onto the real world view.

3.2 Smart homes and buildings

IoT devices can be deployed in both residential and commercial buildings to make resource and energy allocation more efficient and increase security, among other things. Such devices could include smart thermostats and refrigerators, connected security cameras and lighting sensors. McKinsey estimates that in 2025, IoT devices will, on average, reduce labor by 100 hours per year (or 17 percent) in a typical household by automating chores such as vacuum cleaning or lawn mowing. Household items connected to the Internet range from lightbulbs to alarm systems. For example, one company offers a "Smart Home Kit" that contains various sensors and modules that can turn household objects into Internet-connected objects, depicted in figure 8. These modules could be used to automate curtains or remotely control a pet feeder.

Smart thermostats are becoming increasingly popular because they can gather data on motion, temperature, humidity, and light, and analyze that data to automate the thermostat based on the habits of household members. By analyzing occupancy patterns, smart thermostats can conserve energy by turning the heating and cooling off when no one is home. These efficiencies can potentially reduce the energy demands of a building, thereby reducing heating and cooling bills. Some energy companies offer rebates to customers using smart thermostats who agree to let the energy company control the thermostat remotely during peak hours. Commercial buildings can have sensors attached to the windows, ceiling tiles, water tanks, and heating and cooling units. These sensors detect when an area is unoccupied and automatically adjust the heating, cooling, and lights to reduce energy use.

Source: littleBits. | GAO-17-75

Figure 8: Example of an IoT product for the home

IoT devices are used in both homes and offices for security. In offices, rather than have security personnel monitor camera footage, IoT-enabled security cameras can automatically detect possible intrusions and alert authorities. Smart locks connect door locks to the user's smartphone though Bluetooth or Wi-Fi, unlocking the door when the user, with their smartphone, approaches. The user can also email or text a digital key to allow others to enter the home, and can set provisions, such as only allowing access on certain days. Some smart locks can take photographs of people entering the house. Smart home security systems connect a variety of smart home devices—from door and window sensors, to garage door openers—to a central hub, across a wireless network, typically using Wi-Fi or Zigbee.

Experts that attended our meeting to discuss the IoT predict that consumers will adopt IoT devices, such as wearables and smart home automation, at an increasing rate as they become more affordable. One expert pointed to the advanced voice command processing technology as a factor that will be appealing to consumers since this technology creates an easy way—speaking naturally—for consumers to interact with devices.

3.3 Vehicles

IoT-enabled vehicles have the potential to benefit consumers, industry, and the public sector. Such vehicles can sense, analyze, and act on information, such as their location, suggested traffic routes, or impending safety hazards. Consumers also benefit from entertainment units in connected cars that can stream music or provide real time navigation.[31] Through an IoT-enabled data communications system, automobile companies can remotely update the vehicle's software, saving drivers a trip to a dealership. Tesla addressed a recall on a defective charger through an over-the-air software update, similar to how smartphones receive software updates.

Future IoT devices may allow vehicles to connect to each other as well as to transportation management systems. According to the U.S. Department of Transportation (DOT), vehicle-to-vehicle communication, where internal computing systems share data about the vehicle's status with nearby vehicles, has the potential to enhance safety by reducing the number of accidents on the road that occur as a result of human error.[32] Figure 9 depicts the connections created with vehicle-to-vehicle communication. The figure shows three vehicles approaching an intersection, where the vehicles are communicating information to each other using vehicle-to-vehicle communication. Additionally, IoT devices can be installed in vehicles to transmit data to and from transportation management systems. For example, in London, data are collected

[31] An IoT-enabled automobile is also known as a "connected car." A connected car is a car that is typically equipped with Internet access, usually via satellite or cellular communications. Connected cars can also refer to vehicles containing vehicle-to-vehicle and vehicle-to-infrastructure technologies. Vehicle-to-vehicle technologies transmit data between vehicles, and vehicle-to-infrastructure technologies transmit data between vehicles and road infrastructure.

[32] GAO has previously reported on vehicle to vehicle and vehicle to infrastructure communication, see GAO, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist*, GAO-14-13 (Washington, D.C.: Nov 1, 2013) and GAO, *Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Benefits, but Deployment Challenges Exist* , GAO-15-775 (Washington, D.C.: Sep 15, 2015).

from vehicles and sent to the system which controls traffic lights, in real time, in order to reduce congestion within the city. Looking ahead, automobile manufacturers are working towards using IoT technologies to produce fully automated, self-driving vehicles.

Source: GAO. | GAO-17-75

Figure 9: Visual representation of vehicle-to-vehicle communication

3.4 Manufacturing

IoT devices can benefit industry if they are added to machines and supplies used to produce goods—the manufacturing process. These machines and supplies can produce data that are analyzed to monitor process performance, which can improve efficiency and product quality. For example, chemical plants use sensors to measure ingredient mixtures, pressure, and temperature. Chemical plants can then adjust these factors automatically to optimize the process to reliably produce a quality product. Similarly, pulp and paper manufacturers use IoT devices to remotely monitor and control temperature, changing the shape and intensity of the flame in the kiln. These technologies can reduce risk and increase efficiency in the manufacturing process by addressing issues before they become costly.

McKinsey predicts savings will come from increasing the efficiency of factories and from analyzing data collected by sensors to refine equipment and processes.

IoT devices can enhance predictive maintenance for equipment in the manufacturing sector. Predictive maintenance uses data analytics on the information collected by IoT devices to predict potential vulnerabilities. Also, maintenance can be scheduled precisely when needed, based on the collected data. The volume of data IoT devices collect, along with the ability to aggregate the data to perform analytics, enables predictive maintenance. Predictive maintenance has allowed some companies to move to a new business model where the manufacturer not only owns, but also maintains the product. In return, the customer is guaranteed the product will be operational for a specified amount of time.

For example, in the airlines industry, certain airlines no longer purchase jet engines. Instead, they rent the engines, paying for the duration of use. The engine manufacturer, rather than airlines, is responsible for engine maintenance and upkeep. The engine manufacturer can use environmental and performance data collected by embedded sensors to identify if the jet engines require maintenance. Using such data, one manufacturer identified that hot and humid climates cause engines to heat up and lose efficiency. With this information, the manufacturer implemented preventative maintenance, in this case by washing the engines more frequently, to improve performance. The airline benefits from reduced airplane downtime, and the engine manufacturer benefits from a steady income

stream based on the service relationship and fewer major maintenance calls.

3.5 Supply chain

A supply chain is a set of organizations, people, activities, information, and resources that create or move a product or service from suppliers to customers. To enhance supply chains, IoT devices are embedded in products for inventory management systems. This benefits industry by identifying bottlenecks, reducing inefficiencies, and as a result, reducing costs. IoT devices have been used in supply chain management since the 1990's—the term "Internet of Things" was originally used to reference Radio Frequency Identification tags, a technology primarily used in the supply chain.[33] According to Tata Consulting, a majority of consumer packaged goods companies use IoT devices to monitor production and distribution of their products.[34] For example, Coca-Cola embeds sensors both in its products and vending machines to remotely detect when a machine is not operating properly. Such integration of IoT devices has allowed companies to address distribution bottlenecks and improve supply management to reduce labor and capital costs. IoT devices can also enable manufacturers to determine exactly how much product is at a location, giving them information they need to improve their restocking program. The shipping process uses IoT devices to measure environmental data, such as temperature, humidity, and pressure, which is then combined with location data to provide a complete picture of the shipping process. These IoT devices can help ensure consistency when transporting sensitive items, such as a pet, a transplant organ, or humidity sensitive artwork. However, according to one participant at our expert meeting, some industries involved in the supply chain, such as shipping and railroads, have low profit margins, and thus may not invest in IoT technologies. Another expert in our meeting said that more case studies using IoT devices will facilitate the industry's adoption of the technologies, as case studies help show a proven path forward.

3.6 Agriculture

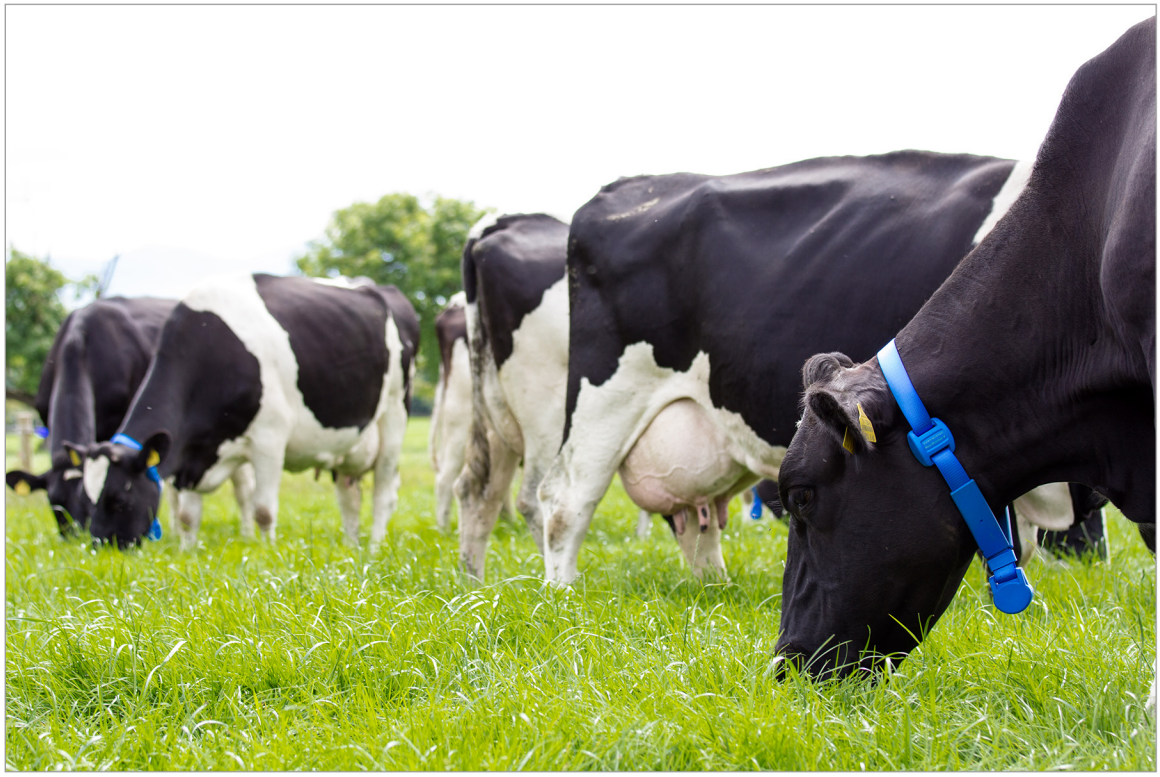
Some farming companies in the agricultural industry are using IoT devices to maximize efficiency while minimizing costs associated with production and labor. This involves using sensors to track different facets of the agricultural process. The IoT data inform the company of potential issues while IoT devices enact changes modifying the agricultural process in real time. For example, in the field, sensors take measurements of chemical levels, soil moisture, and air quality. These data are analyzed to determine which fields need more water or fertilizer, which improves the quality of the crops. IoT devices also can be used to track similar data in greenhouses, such as temperature and humidity, and transmit that data to farmers via wireless networks. The data are then analyzed, and farmers can set alerts if data reach certain values. Based on data, the farmers can adjust the temperature and humidity in the greenhouses as needed. In another example, an agricultural equipment and vehicle manufacturer offers a device that replaces a steering wheel on a tractor to automate the

[33] Radio Frequency Identification technology consists of active or passive electronic tags that are attached to equipment and supplies that are shipped from one location to another.

[34] Tata Consultancy Services, *Internet of Things: The Complete Imaginative Force* (2015).

steering of the tractor within an inch of accuracy using the Global Positioning System. This can increase the crop yield by reducing operator mistakes, such as double planting rows or skipping over parts of the field.

Farmers and ranchers can also use IoT devices to support the care of livestock and other animals. Electronic identification readers implanted in livestock track movements and eating patterns, providing the farmer with insight into the location of livestock and any deviation from an animal's normal eating habits. Other devices, such as the cow monitoring device depicted in figure 10, can track information used by ranchers to determine when the cows are in their optimal breeding cycle, improving the chance of pregnancy. Other devices can detect early signs of health issues, such as disease. For example, one South Korean telecom company that focuses on the IoT has piloted an eel farm management system which senses environmental metrics, such as water temperature and oxygen levels. Eel farmers are alerted remotely of any changes, and can correct the change before any animals are injured.



Source: Dairymaster MooMonitor+. | GAO-17-75

Figure 10: Example of an IoT device used in agriculture

3.7 Health care

IoT devices are used in health care, both for home health monitoring and in hospitals, with benefits to consumers and industry. Health care IoT devices collect data to improve patient quality of life and safety by enabling patients to self-manage and monitor their health.[35] Furthermore, IoT devices can be used together for patients with chronic conditions, such as diabetes. For example, a fitness tracker will generate detailed data on the patient's activity levels. A home monitor will collect data on the patient's blood glucose levels. IoT-enabled pill bottles can collect data on when and how often the patient is taking medication. Aggregating data provide a more complete picture of the patient's health by identifying trends and problems that may require intervention by patients and health care providers. Using IoT devices that transmit health data collected at home to a medical facility can be particularly beneficial to individuals living in rural areas. For example, patients with an implanted heart device can transmit data from their heart device to specialized equipment in their home. The equipment then transmits these data to the patient's health care provider for review to identify any health-related issues.

Some hospitals rely on IoT devices to monitor and track patients and equipment. For example, a sensor mat under a hospital bed can track patient movement as well as heart and respiration rates. These data are analyzed to monitor movement in and out of bed, to adjust the patient's position while in bed to reduce pressure, and to view trends in heart and respiration rates. Wi-Fi connected badges worn by patients are used in hospitals and long term care homes to track patients' locations. Health care providers can view a patient's location on a monitor, as well as receive alerts if the patient enters a restricted area. This type of monitoring increases patient visibility, mitigates injuries from falls, and monitors a patient's activity. Similarly, hospital equipment, from wheelchairs to vital carts, can be tagged with Wi-Fi devices to provide real-time location and availability information. This reduces the time health care providers spend searching for equipment and prevents theft by creating an alarm if the equipment is taken off premises.

3.8 Energy

The energy industry uses IoT devices in multiple ways. Energy companies report using IoT devices to track product flow, from development to distribution.[36] For example, an oil and gas company can use IoT devices to measure multiple data points along a drill line. Information from the devices is used to adjust the speed and pressure of the drill bit when drilling, resulting in an optimization of the process that reduces costs.[37] Smart grids rely heavily on IoT devices to facilitate communication between the energy grid and

[35] According to the Office of the National Coordinator for Health Information Technology, *Issue Brief: Patient-Generated Health* Data *and Health IT* (2013).

[36] Tata Consultancy Services, *Internet of Things: The Complete Imaginative Force* (2015).

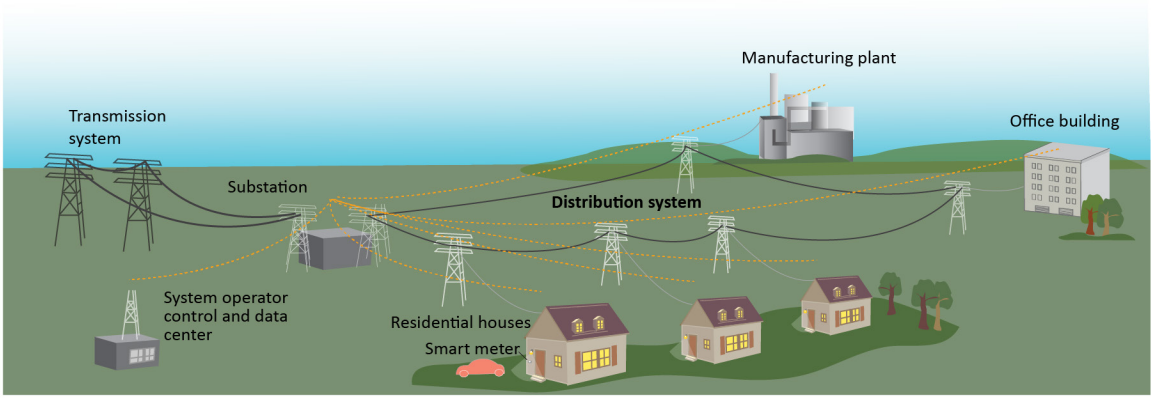
[37] Chris Murphy, *Internet of Things: What's Holding us Back* (Information Week, May 2014), accessed July 6th 2016, http://www.informationweek.com/strategic-cio/it-strategy/internet-of-things-whats-holding-us-back/d/d-id/1235043?print=yes.

the building consuming energy.[38] Figure 11: shows different components of a smart grid.

One component of the smart grid is a smart meter, which displays the energy usage of a consumer's home, enabling the consumer to monitor their energy consumption and identify opportunities for energy savings. Smart grids also allow for the delivery of energy, such as solar or wind power, installed at homes or businesses, back to the grid. Smart grids can enable electricity suppliers to offer "smart pricing," which rewards consumers for reducing energy consumption when demand is high. Some programs provide incentives to consumers to pre-program their smart thermostat to make adjustments if energy prices rise, such as reducing the use of air conditioning by raising thermostat settings.

3.9 Environment

IoT devices can monitor the environment, including air quality, to benefit the public sector and industry. In Chattanooga, TN, city officials are developing sensors to be distributed around the city to collect information about air quality—specifically pollen content—to provide real-time data to residents. Other products allow consumers to gather data on air quality from outside their home and submit the collected data online. The results can be used to inform people, especially those who experience health effects from poor air quality. In addition, there are systems that track water quality. For example, a water quality project started by researchers at the University of California,



Source: GAO. | GAO-17-75

Figure 11: Components of a smart grid.

[38] Smart grids include communication and information technology used throughout electric power transmission and distribution systems in order to automate action with the aim of improving the electric reliability and efficiency. GAO has several products on the smart grid, including *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention,* GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

Berkeley, collects real-time data, such as pollution levels, flow movement, and temperature, via mobile sensors floating in local waterways. The sensors communicate the data to researchers, who can create maps that portray the flow of water and different water characteristics, such as temperature and salinity levels, to track water contamination levels and identify levee breaches. IoT devices have also helped monitor the environment for potential natural disasters. The Wireless Sensor Network System for the Detection and Early Warning of Landslides, developed by scientists in India, is comprised of sensors that collect data wirelessly from the local terrain. It can send out alerts if the data indicates a potential landslide. Similarly, connected drones can collect and share data, including photos and video, in locations and environments that are particularly difficult or dangerous for people to visit, enabling better monitoring of disaster areas, among other things.[39]

The intersection of IoT technologies and environmental monitoring may also offer benefits to businesses. For example, an IoT system has been developed to track optimal conditions in vineyards. By collecting data about the environment, this system can communicate wirelessly with farmers, reducing their time in the field while providing data that can affect the yield, taste, and quality of their products.

3.10 Smart communities

The public sector in both the United States and overseas is adopting IoT devices in Smart Cities and Smart Communities to improve livability, management, and service delivery of the community.[40,41] For example, IoT technologies can provide real time data about the status of the community, making it easier to monitor and improve public services. In Barcelona, Spain, sensors are used to determine if public waste bins are full, streamlining waste collection by sending crews only to full bins. In Nashville, Tennessee, public buses are outfitted with sensors that collect and report real-time location data so that citizens know whether the bus is on time. Smart street lighting—lighting that allows for two-way communication—is used in Dublin, Ireland to report operational status and control the lights. The lights can also be dimmed or brightened depending on the weather, traffic, or emergency services.

Although the current IoT solutions for Smart Communities tend to be specific to a single function, future promise lies in combining data from sources in different functions to solve problems. For example, data from IoT sensors deployed to aid in the transportation sector, such as parking sensors and traffic video cameras, and for environmental monitoring, such as air quality monitors, can be used to achieve larger community goals like health and safety. For example, the Copenhagen Solutions Lab collects real time information across different sectors in order to create transportation solutions and reduce

[39] Drones are also referred to as unmanned aerial systems.

[40] Livability encompasses the factors that contribute to quality of life, such as economic prosperity, social stability, equity, as well as educational, cultural, entertainment and recreational opportunities.

[41] There are multiple different definitions of Smart Cities and Smart Communities. This report highlights the use of IoT devices within the Smart City or Smart Community context and uses the terms interchangeably.

carbon emissions. In New York City, the Center for Urban Science and Progress combines data from air pollution with traffic data and hospitalization rates for asthma to better establish correlations between air quality and traffic.

3.11 IoT device use across multiple sectors

The proliferation of IoT devices will likely increase the use of IoT devices and systems that span multiple sectors. For instance, a city's department of transportation could use data collected from traffic cameras, sensors on roads, in cars, buses and parking meters, combining the collected data with weather reports to optimize traffic flow.

Combining IoT data with other data streams has the potential to provide benefits on a larger scale. One expert from our meeting pointed to health initiatives that benefit from the rise of fitness trackers. Data from wearables is combined with genetic, clinical, and survey data to create a giant data set. From there, variables such as genetics, daily activities, and the environment can be used to help predict health outcomes. The research can inform health care providers about effective treatments for certain conditions, as health care providers will have access to data on previously successful approaches. Figure 12 shows a future landscape of the IoT, where various devices in different settings transmit and share data.

Source: GAO. | GAO-17-75

Figure 12: Potential interconnections in an IoT-enabled environment

4 Potential implications of the use of the IoT

Even though the IoT creates many benefits, it is important to acknowledge implications that may arise with its broader adoption. Such implications could shape how IoT technologies are used, potentially hindering the spread of the IoT, or reducing the potential benefits. These implications include challenges to the development of the IoT, such as ensuring information security, privacy, user safety, and device reliability. In addition, governmental oversight, effective management of the electromagnetic spectrum, and global coordination all affect device capabilities and interoperability, including the development and use of standards. Economic impacts on the market and employment, as well as societal effects, are also likely to result from the adoption and use of the IoT.

4.1 Information security challenges

Adoption of the IoT across different sectors has amplified the challenge of designing and implementing effective information security controls by bringing the potential effects of poor security into everyday situations in homes, factories, and communities. The rapid and pervasive adoption of IoT devices, the lack of attention in designing them to be secure, and the predominant use of cloud computing to provide connectivity with these devices pose unique information security challenges that may limit broader adoption of the IoT.

4.1.1 Maintaining security with extensive IoT connectivity

The growing ubiquity and pervasive connectivity of IoT devices and networks may pose significant security risks. Unauthorized individuals and organizations may gain access to these devices and use them for potentially malicious purposes, including fraud or sabotage. As cyber threats grow increasingly sophisticated, the need to manage and bolster the cybersecurity of IoT products and services is also magnified.

GAO has previously reported that cyber threats to Internet-based systems are evolving and growing.[42] Without proper safeguards, these systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The threat is substantial and increasing for many reasons, including the ease with which intruders can obtain and use hacking tools and technologies.

Threat actors make use of a variety of techniques or attacks that may compromise information or adversely affect devices, software, networks, an organization's operations, an industry, or the Internet itself. Table 1 provides examples of cyber-attacks that could affect IoT devices and networks.

[42] GAO, Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems, GAO-15-573T (Washington D.C.: April 22, 2015).

Types of attack	Description
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports. | GAO-17-75

Table 1: Examples of cyber-attacks that could affect IoT devices

While there are many industry-specific standards and best practices that address information security, standards and best practices specific to IoT technologies are still in development or not widely adopted. For example, the National Institute of Standards and Technology (NIST) has issued extensive information security guidance to federal agencies, including a catalog of security and privacy controls to be used to protect information and systems. In addition, the Center for Internet Security has issued guidelines on critical security controls an organization can implement to defend their networks and systems from a variety of internal and external threats.[43] Further, the Institute of Electrical and Electronics Engineers (IEEE) has developed information security standards that address specific areas such as encryption, storage, and hard copy devices.

[43] The Center for Internet Security, *CIS Critical Security Controls for Effective Cyber Defense*, Version 6.0 (Arlington, Virginia: Oct. 15, 2015).

Designing and incorporating security controls into IoT devices from the initial design to the operational environment during development may curtail vulnerabilities. Widespread concerns have been raised about the lack of security controls in many IoT devices, which is in part because many vehicles, equipment, and other increasingly IoT-enabled devices were built without anticipating threats associated with Internet connectivity or the requisite security controls. Experts from our meeting agreed that information security presents significant challenges for the IoT environment and it is a topic that should be addressed from the initial development of these devices.

As the number of deployed IoT devices grows, the risk of exploitation also grows. Any device that is connected to the Internet is at risk of being attacked if it does not have adequate access controls. For example, as The Internet Society has suggested, an unprotected television that is infected with malware might send out thousands of harmful emails using the owner's home Wi-Fi Internet connection.[44]

In addition, many IoT devices are configured with identical or near identical software and firmware, which can magnify the impact of successfully exploiting a technical vulnerability common to all of them. For example, security vulnerabilities that are identified for one type of IoT device might extend to all other IoT devices that use that same underlying firmware or share the same design characteristics. This significantly increases the potential for successful attacks.

While experts agree that the growing number of IoT interconnections presents significant security challenges, they do not agree on how to address the issue. The Federal Trade Commission (FTC) staff has recommended that companies prioritize and build security into their devices from the outset, conduct security risk assessments as part of the design process, test security measures before products are launched, and consider encryption for the storage and transmission of sensitive information. Several experts suggested applying access controls to IoT devices, such as role-based access controls that can be used to limit the privileges of device components and applications. Thus, if an intruder successfully gains access to a specific device, they should have limited access to other parts of the system. Nevertheless, establishing limits on access controls presents its own challenges for suppliers, because the functionality and flexibility of their devices could be affected if access controls are too restrictive.

NIST recommends that organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls.[45] NIST also points out that organizations typically do not have control over the external networks (e.g. the Internet) with which their devices directly connect, and suggests that they apply boundary protection devices, such as firewalls and routers, to mediate between the devices and the external networks. Such advice can also apply to IoT devices that are connected

[44] The Internet Society, *The Internet of Things: An Overview* (Reston, VA: October 2015).

[45] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

through the Internet to their manufacturer or their cloud service provider.

4.1.2 Designing IoT devices with software update capabilities

NIST recommends that organizations take steps to ensure that the security controls implemented on their systems are up to date. This includes identifying and correcting information security flaws and installing software patches and other security updates in a timely manner, among other things.[46]

However, many IoT devices are designed without a software upgrade capability or with a cumbersome upgrade process, potentially leaving them vulnerable as cyber-attacks evolve. Security researchers evaluating automotive cybersecurity determined that attackers could gain significant control over important vehicle functions remotely, such as the engine, brakes, and steering performance, by exploiting wireless communication vulnerabilities. If an owner does not upgrade the vehicle's software, the vehicle may be susceptible to an attacker gaining access to key functions.

Further, the United States Computer Emergency Readiness Team (US-CERT) has warned that IoT devices have been used to create large-scale botnets—networks of devices infected with self-propagating malware—that can execute crippling distributed denial-of-service attacks. These attacks can severely disrupt an organization's communications or cause significant financial harm. For example, in September 2016, a well-known security blog was targeted by a massive denial-of-service attack by the Mirai botnet, which uses a short list of common default usernames and passwords to scan the Internet for vulnerable devices to infect. Because many IoT devices are unsecured or weakly secured, this list allowed the botnet to access hundreds of thousands of devices. The attack involved over 380,000 IoT devices, including network-enabled cameras and digital video recorders in homes and offices. The same type of attack occurred in October 2016 that targeted a company whose servers monitor and reroute Internet traffic, leaving major websites unavailable to people across the United States. In order to prevent this type of attack, US-CERT suggests that users should change default passwords and update IoT devices with security patches as soon as they become available. This type of prevention can be difficult for IoT devices designed without a capability to upgrade software or ones that have to be manually updated.

In addition, many IoT devices may be deployed with an anticipated service life many years longer than typically associated with high-tech equipment, making it unlikely that security updates will continue through that entire service life. Further, some devices might outlive the companies that created them, complicating updates and repairs, which may also increase the likelihood that the devices' security mechanisms will not be adequate over their full lifespan.

In a recent study, AT&T suggests that a basic security requirement for every network-connected device should be to have the capability for authorized operators to update the device's software using a highly

[46] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, MD.: April 2013).

automated process.[47] The FTC staff has suggested that companies should be forthright in their representations about providing ongoing security updates and software patches and that disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-connected devices.[48]

4.1.3 Use of cloud computing

NIST has outlined the considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.[49] It offers guidelines for companies to consider when using cloud services, such as carefully planning the security and privacy aspects of cloud computing solutions before engaging them and ensuring the environment meets organizational security and privacy requirements for cloud computing.

Cloud computing is a major underlying platform for the IoT, as it is an ideal technology for operating across a range of different systems, services, and devices. Some advantages of working in the cloud are the ability for large-scale data aggregation and analysis, continuous availability, and the potential for rapid scaling of computing resources.

However, many of the features that make cloud computing attractive can also pose security challenges. One major challenge is the loss of control of the computing environment that supports the device. Using the cloud as a platform requires a transfer of information and system components to the cloud provider that would otherwise be under the company's direct control. This situation makes the company dependent on the cloud provider to carry out key security functions, such as continuous monitoring and incident response. Loss of control over both the physical and logical aspects of the system diminishes the company's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security that are in the best interest of the organization. Under such conditions, companies face an increased potential for mismanagement of their computing environment, including not implementing proper security controls to protect the data they are collecting.

Cloud computing could also increase the risk that data may be accessed by an excessive amount of personnel for unauthorized purposes. Moving to a cloud computing environment expands the number of entities that have access to the data, including the cloud provider's staff and subcontractors and potentially other customers using the cloud provider's service, thereby increasing risk.

Lastly, the complexity of cloud computing environments also poses increased risks. A cloud computing environment often includes many components, such as applications,

[47] AT&T, *Cybersecurity Insights, vol. 2: The CEO's Guide to Securing the Internet of Things* (2015), accessed January 6, 2017, https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf.

[48] Federal Trade Commission Staff Report, *Internet of Things: Privacy & Security in a Connected World* (Washington, D.C.: January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[49] NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-146 (Gaithersburg, Md.: December 2011).

virtual machines, data storage, and supporting middleware, all of which may be provided by different vendors. Security in a cloud computing environment depends on secure interactions among each of these components.

Using cloud computing as a platform for IoT devices offers potential increased benefits, including faster deployment of computing resources, less need to buy hardware or to build data centers, and more robust collaboration capabilities. These characteristics are suitable given the massive scale of the IoT and the large amount of data IoT devices collect. However, experts in our meeting pointed out that the inherent security issues associated with the cloud have not been fully resolved. Consequently, IoT devices relying on the cloud could remain vulnerable until such issues are addressed.

4.2 Privacy challenges

Privacy considerations, which are related to but distinct from security concerns, are critical to the growth and ultimate success of the IoT. Developers of IoT devices and systems face a number of challenges in ensuring that their products respect consumers' privacy and do not inappropriately collect or misuse their personal information. These challenges include developing suitable methods for notifying consumers about how their data are used, obtaining consent for such use, and limiting the collection and use of personal information to authorized purposes.

4.2.1 Fair Information Practices

The Fair Information Practices (FIPs) are a widely accepted set of principles for protecting the privacy and security of personal information that were first proposed in 1973 by a U.S. government advisory committee.[50] The Organisation for Economic Co-operation and Development (OECD), an international organization, developed a revised version of the FIPs in 1980 that has been widely adopted (see table 2).[51]

[50] See U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

[51] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.

Source: OECD. | GAO-17-75

Table 2: The Fair Information Practices

These principles, with some variation, have been used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States. The FIPs provide a useful framework of principles for balancing the need for privacy with other interests.

IoT devices can involve extensive collection and analysis of detailed personal information, making it critically important that the privacy of that information is protected. With respect to IoT devices, concerns have been raised about notifying individuals how their information may be used and allowing them to choose whether to allow its collection; ensuring that once information is collected it will not be retained and used for unrelated purposes, and preventing unauthorized monitoring of individuals by aggregating information about them from multiple IoT data sources.

4.2.2 Notifying users and obtaining their consent

In accordance with the FIPs, users should be notified whenever their personal information is collected and retained, and they should be given the opportunity to choose whether to allow such collection. The openness principle states that the public should be informed about the privacy policies and practices of an organization that is collecting personal information and should have ready means of

learning about the specific ways in which their personal information will be used. Further, the collection limitation principle states that organizations should collect no more than the specific personal information needed for their stated purpose, that they should obtain that information by lawful and fair means, and, where appropriate, with the knowledge or consent of the affected individuals. These principles help ensure privacy by informing individuals and empowering them to approve the collection of their personal information and to understand exactly how it is to be retained and used.

In many cases, IoT devices collect information through sensors that are embedded in everyday items, ranging from thermostats to automobiles, that may have at best a very limited ability to convey information about privacy policies and practices or to seek an individual's consent to collect their personal information. While devices such as computers and smartphones can notify their users and obtain consent through information presented on a screen, many IoT devices have no screen or other interface to communicate with the user. For example, IoT-enabled baby monitors use sensors to monitor a baby's breathing, sleeping temperature, body position, activity level, and whether they are awake or asleep. This information may be collected and stored on the device or in an Internet-based system maintained by the device's manufacturer, but the monitor itself provides no notice or consent for this function. Even if a device has a screen, that screen may be too small to explain privacy policies and practices and obtain consent.

Further, IoT devices may collect data at times when an individual is not be able to read a notice or offer consent, such as when driving an automobile, or when the individual is simply not aware that information is being collected. For example, IoT-enabled televisions and video game consoles may have voice recognition or vision features that collect information about users and transmit that data to their providers. An initial user may have consented to data collection, but others who come in contact with the devices may not know that their personal information is being collected and cannot choose to decline the collection.[52] An example of IoT use that may collect personal information without a user's knowledge is Smart Cities, which continuously collect, aggregate, and use data about and for residents. Smart Cities collect information on various aspects of life, including health and wellness, energy efficiency, building automation, transportation, and public safety. These kinds of IoT technologies may provide benefits to individuals and the city as a result of their use, but pose a privacy problem for those who are unaware of the presence of the devices or not provided notice of what is being collected and when it is being collected. Smart City managers should ensure that they initiate efforts to provide adequate notice and choice to the public to help ensure that, the public knows when their personal information is being collected and what it will be used for.

Industry experts agree that providing notice and choice to users in a highly connected IoT environment is difficult, and there is no consensus on how to resolve the problem.

[52] In February, 2017, VIZIO, a large manufacturer and seller of internet connected smart televisions, had to pay $2.2 million to FTC and the State of New Jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent. See https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

The Online Trust Alliance suggested that companies use an associated platform, such as a mobile device or computer, to provide notice and choice when an IoT device is being installed or configured.[53] Other suggestions included offering notice and choice at point of sale, through tutorials offered on the Internet, or through codes on the device that, when scanned, would take the consumer to a website with information about privacy policies and practices and would allow consumers to choose whether to allow their data to be collected. However, because these methods require consumers to take extra steps to learn about privacy and make privacy choices, they may not effectively reach many of the individuals whose personal information is being collected. As a result, providing adequate notice and consent remains a challenge for many IoT devices and applications.

4.2.3 Limiting the collection of personal information by IoT devices

According to the FIPs, organizations should specify the purpose of any collection of personal information they undertake and ensure that the data they collect are only used for that purpose, not something unrelated. Further, the data should not be used in the future for a new or supplemental purpose without first obtaining the consent of the affected individuals. Adherence to these principles can provide reassurance to individuals that these organizations maintain a degree of control over how their personal information is used.

However, given the extensive potential of IoT devices to collect data, companies may be reluctant to refrain from collecting and retaining as much information as their IoT devices are capable of capturing. For companies, the collected data can be used for a variety of purposes that appear to be beneficial and profitable, regardless of the original intent that an individual may have had in purchasing or interacting with an IoT device or network of such devices. For example, fitness trackers can capture a variety of information about an individual's physical activity and biometric traits, including when and how much a person exercises, the duration of their sleep, and variations in their heart rate throughout the day. Fitness trackers, like many other IoT devices, link the data they collect to online user accounts, which generally include personally identifiable information, such as names, email addresses, and dates of birth.

Such information could be used in ways that the consumer did not anticipate or was not given the option to approve. For example, data could be sold to companies looking to target consumers with advertising or combined with other information to determine insurance eligibility or rates. The FTC staff conducted a study of 12 different health and fitness apps and found the apps sent data they collected from consumers to 76 different third-party entities. These data included names, email addresses, exercise habits, diets, medical symptom searches, location, gender, and more. Additionally, the Director of National Intelligence warned that foreign intelligence services may begin using the IoT for identification, surveillance, monitoring, location tracking, and targeting

[53] Online Trust Alliance, *OTA IoT* Trust *Framework* (Bellevue, WA: September 2016).

for recruitment, or to gain access to networks or user credentials.[54]

Given the increased use and presence of IoT devices and the ease with which data about individuals can be aggregated from multiple sources, companies and governments will likely be able to track an individual's activities and habits, in great detail, over their entire lifetime. IoT devices can collect information about people with an unprecedented degree of specificity and intimacy. Aggregation and correlation of these data can create detailed profiles of individuals that could increase the potential for identity theft, discrimination, and other harms. The benefits of advanced data analytics need to be balanced with an individual's right to privacy. This dilemma is ongoing and given the issues with notice and consent already discussed will not be solved in near future without consumer, industry, and public sector involvement and cooperation.

It is possible to imagine many ways in which seemingly trivial everyday information could be aggregated to create the potential for harm to individuals if misused. For example, the Internet Society has suggested that an individual may use an IoT-enabled toothbrush that captures and transmits data about that person's tooth-brushing habits.[55] If the same person's refrigerator reports the inventory of the foods he eats and his fitness-tracking device reports his physical activity, the combination of these data could provide a detailed profile of the person's health. The resulting portfolio of health-related data, which outlines dental hygiene habits, food consumption, and activity levels—complete with time stamps and geolocation data—could be used to determine the users' health risks. The sophistication of the aggregation could create situations that expose the user to physical, criminal, financial, or reputational harm.

To the extent that companies collect, maintain, and share data for business purposes, experts have suggested that methods exist to protect that information, such as maintaining the data in de-identified form. De-identification is the process of removing personal identifiers from a data set in an attempt to prevent a person's unique identity from being connected with the information. Many experts agree that effective de-identification could help to minimize privacy concerns related to data aggregation and tracking, as it reduces the likelihood that the data would be connected to a specific person. However, questions also have been raised about whether existing methods of de-identification effectively prevent data from being re-identified.[56] As a result, the protection of privacy for aggregated personal information will likely remain a challenge.

4.3 Safety concerns

As IoT devices expand into transportation and health care, among other sectors, user safety concerns increase. According to one expert from our meeting, connected cars can help

[54] Office of the Director of National Intelligence. *Worldwide Threat Assessment of the US Intelligence Community*. (Washington, D.C.: February 25, 2016).

[55] The Internet Society, *The Internet of Things: An Overview* (Reston, VA: October 2015).

[56] Cynthia Dwork, "Differential Privacy," in *Automata, Languages and Programming,* 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II. (Berlin: Springer, 2006), 1-12.

improve safety, but are susceptible to other risks, including hacking. One example reported by the media is the hacking of a connected car—a Jeep Cherokee—in July 2015. Hackers were able to cut the brakes as well as disable the transmission of the car via remote access through the entertainment system, causing the car to slow down on the highway and endangering the driver, as well as others, on the road.[57] Most recently, a Tesla Model S sedan on autopilot was reported to have crashed into a tractor-trailer in May 2016, resulting in a fatality for the driver. According to Tesla, "Neither the autopilot nor the driver noticed the white side of the tractor trailer against a brightly lit sky, so the brake was not applied."[58,59]

Safety is also a concern with IoT medical devices in the health care industry.[60] For example, one expert at our meeting described an instance with a ventilator where the manufacturer decided to make the firmware update available online. However, the website had been hacked and the firmware update had malware attached to it. This expert stated that when the ventilator devices are infected, they are no longer able to deliver patient care, putting the patient's health at risk. Another expert from our meeting told us that there is no security on implantable medical devices, making them easily hackable. The expert explained the rationale for not having security on the devices is that the hacking risk is balanced by the risk of the device being inaccessible to medical professionals. According to the expert, there have been no security breaches to a medical device to date. However, former Vice President Dick Cheney modified his heart defibrillator to disable the wireless feature due to concerns that his device could be hacked remotely.

Reliability and maintainability of IoT devices are also concerns. As objects embedded with IoT technologies often have extended service lives, maintainability and upgradability may be difficult. One expert from our meeting pointed out that buildings are expected to last more than 50 years, and IoT devices in the buildings typically last 20 years before being retrofitted. However, the expert pointed out, the IoT technologies are maturing much faster than the systems in which they are embedded. Additionally, many IoT devices rely on the cloud, and if the manufacturer stops supporting cloud services the device cannot function. This recently happened with Nest's hub Revolv, where Nest shut down the cloud services used by Revolv, causing the hub to no longer work.[61] To help address these concerns, one expert discussed the idea of designing graceful degradation into devices, where the system retains some

[57] Andy Greenberg. *Hackers Remotely Kill a Jeep on the Highway – With Me in* It (Wired, July 2015), accessed July 19th 2016, www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[58] The Tesla Team. *A Tragic Loss* (Tesla, June 30th 2016), accessed December 16th 2016, https://www.tesla.com/blog/tragic-loss.

[59] For more information, see NHTSA investigation PE 16-007, Jan. 19th 2017, accessed Mar. 6th 2017, https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF.

[60] GAO has previously reported on security threats in medical devices, see GAO, *Medical Devices FDA Should Expand Its Consideration of Information Security for Certain Types of Devices,* GAO-12-816 (Washington, D.C.: August 31, 2012).

[61] FTC File No. 162-3119. The FTC staff investigated the incident to determine if Nest violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, and, in July 2016, recommended no enforcement. The decision was based on a number of factors including Nest offering full refunds after the shutdown was announced.

level of function even after being disconnected from a network or power.

Finally, as IoT systems become more complex (e.g., smart homes embedded with an increasing number of IoT devices), the consumer may not have the skills to troubleshoot and maintain the system. According to the course "Internet of Things: Roadmap to a Connected World" offered by MIT Professional Education, a typical technology user troubleshoots an IoT device by powering off and then back on. However, the issue of diagnostics should be considered, as IoT devices are used in increasing different ways. For example, when replacing a valve, a plumber may first need to initialize the sensor in that valve, which can require IT skills.

4.4 Governmental oversight

There is no single U.S. federal agency that has overall regulatory responsibility for the IoT. Various agencies oversee or regulate aspects of the IoT, such as certain devices or management of certain kinds of data. However, some issues, such as privacy and security, are crosscutting, and sector-specific oversight efforts in these areas could overlap.

Federal agencies that have sector-specific oversight roles or mission-related responsibilities involving the IoT include the Federal Aviation Administration, which is involved in regulation and other activities relating to unmanned aerial vehicles or drones, and the National Highway Traffic Safety Administration (NHTSA) within the DOT, which regulates the requirements for motor vehicles, including autonomous vehicles and vehicle-to-vehicle communications technology.[62]

One expert at our meeting noted that IoT technologies can face regulatory competition when a device spans sectors and falls into many agencies' jurisdiction. For example, certain mobile health applications may be regulated by the Food and Drug Administration (FDA) for their effectiveness as potential medical devices, while other offices within the Department of Health and Human Services oversee the privacy of health data collected by the application and protected under the Health Insurance Portability and Accountability Act of 1996. The FTC investigates false or misleading claims about the applications' safety or performance, and the Department of Justice addresses the law-enforcement aspects, including cyberattacks, unlawful exfiltration of data from devices and/or networks, and the investigation and prosecution of other computer and intellectual property crimes.[63]

In addition to the federal government's role in overseeing aspects of the IoT, states may also regulate the use of IoT devices. For example, some states have enacted legislation that allows the use of autonomous vehicles (unmanned or driverless vehicles) within their

[62] GAO, *Unmanned Aerial Systems: FAA Continues Progress toward Integration into the National Airspace*, GAO-15-610 (Washington, D.C.: Aug 17, 2015).

[63] The FTC, in conjunction with the Department of Health and Human Services' Office of National Coordinator for Health Information Technology, the Office for Civil Rights and the Food and Drug Administration, created a web-based tool that developers of health-related mobile apps can use to understand what federal laws and regulations might apply to their apps. See https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool .

state.[64] The states and auto industry are working with NHTSA and DOT to ensure that testing of autonomous vehicles is conducted safely.

The question of whether to regulate IoT devices or data and who should regulate them (sector specific agencies or some overall oversight agency) is an issue that has arisen in both the Executive and Legislative branches of the federal government. The National Telecommunications and Information Administration (NTIA) within the Department of Commerce began conducting a review of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things in April 2016.[65] NTIA sought, and is still seeking, broad input from all interested stakeholders through requests for comments and workshops, and released a Green Paper in January 2017 that analyzes the comments it had received thus far.[66] Also, the Developing Innovation and Growing the Internet of Things Act (DIGIT Act), with versions introduced in both the House of Representatives and Senate, would require the Department of Commerce to convene a working group of federal stakeholders to provide recommendations to Congress on the proliferation of the IoT.[67]

4.5 Managing the IoT electromagnetic spectrum

Experts we spoke with agreed that there will be an enormous need for spectrum capacity as IoT device usage grows. They identified two major spectrum-related challenges and knowledge gaps associated with the IoT: (1) managing interference and (2) developing spectrum management strategies. Additional IoT spectrum challenges and gaps include addressing inaccessible devices and the deployment of the next-generation wireless network, called 5G.

The radio-frequency spectrum is the part of the natural spectrum of electromagnetic radiation lying between the frequencies of 3

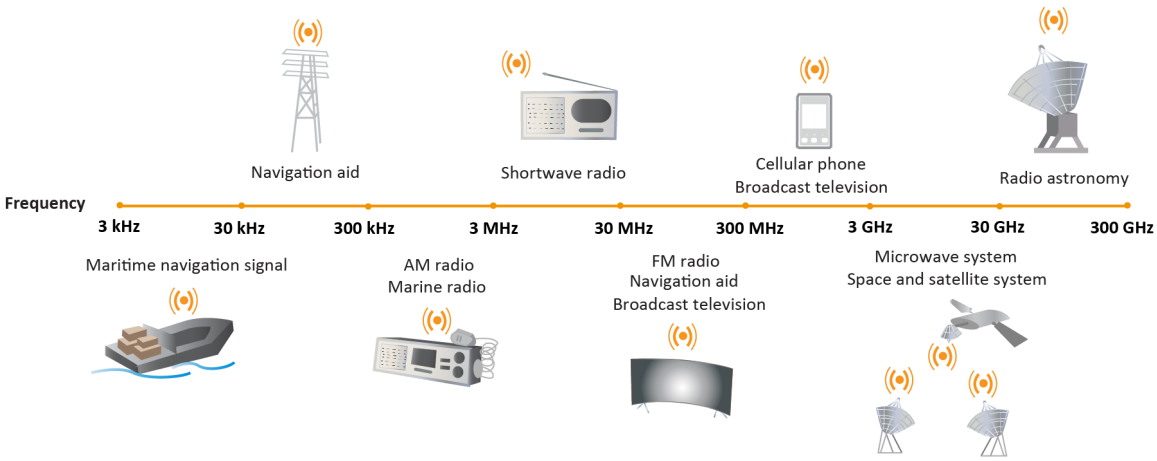
[64] An autonomous vehicle or highly automated vehicle is defined by NHTSA as using a combination of hardware and software (both remote and on-board) that performs a driving function, with or without a human actively monitoring the driving environment. They are automated vehicle systems that are capable of monitoring the driving environment; such as an automated system that can both actually conduct some parts of the driving task and monitor the driving environment *in some instances*, but the human driver must be ready to take back control when the automated system requests, as well as an automated system that can perform all driving tasks, under all conditions that a human driver could perform them. NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution In Roadway Safety*. (Sept. 2016). https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016. Last accessed October 12, 2016.

[65] 81 Fed. Reg. 19956 (Apr. 6, 2016).

[66] The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things* (January 2017), at https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf. NTIA published a new request for public comment seeking additional input from all interested stakeholders on issues proposed in its Green Paper. 82 Fed. Reg. 4313 (Jan. 13, 2017). Comments were due March 13, 2017.

[67] S. 88, 115th Cong. (2017); H.R. 686, 115th Cong. (2017).

kHz and 300 GHz.[68] It is the medium for wireless communications and supports a vast array of commercial and governmental services (figure 13).



Source: GAO. | GAO-17-75

Figure 13: Examples of allocated spectrum uses

Historically, concern about interference, or crowding among users, has been a driving force in spectrum management. Interference occurs when two communication signals are at or close to the same frequencies in the same vicinity, which may lead to degradation of device operation or service. FCC staff said that relatively few interference complaints arise from devices that are operating properly and are compliant with regulations. They also said that most current devices are generally shielded and polite. An expert in spectrum research told us that for consumer goods, interference is less likely to be an issue because most IoT devices only transmit for short durations and transmit locally (less than 10 feet). If the range of the devices is confined to a specific region, then many devices can transmit on the same spectrum in a large enough area for each device to have its own region. Similarly, devices that transmit rarely can take turns transmitting over the same spectrum. These strategies allow for spectrum sharing, whereby multiple authorized users can access the same spectrum with their devices (figure 14).

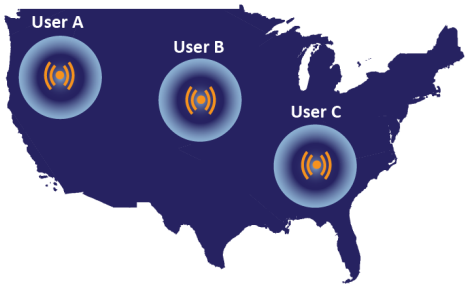
FCC staff stated that interference management is becoming more challenging given the rapid expansion in wireless services and devices. Unexpected sources of interference may pose a challenge to IoT devices. For example, microwave ovens leak waves that can interfere with Wi-Fi access points. Further, experts in spectrum research told us that for certain large-scale IoT deployments—such as in smart cities, connected cars, or applications where large amounts of video data are being transferred—spectrum needs can be a major issue. Finally, an expert in our meeting mentioned that having overly restrictive rules to manage interference may suppress

[68] Spectrum is typically measured in cycles per second, or hertz. Standard abbreviations for measuring frequencies include kHz (kilohertz: thousands hertz), MHz (megahertz: millions of hertz), and GHz (gigahertz: billions of hertz). See Moore, Linda, K. *Framing Spectrum Policy: Legislative Initiatives.* R44433 (Congressional Research Service, August, 2016).

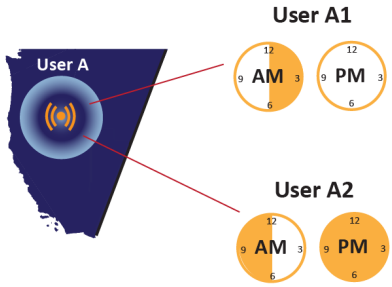
customization of spectrum-using devices when companies “lock-down” their devices to accommodate such rules.

Different IoT devices will have different spectrum requirements, and knowledge gaps remain in how to advance technologies to better share spectrum and how to fully benefit from the existing spectrum when managed by multiple sources. Similarly, there is no requirement for spectrum dedicated specifically for IoT devices. FCC staff told us that because the future spectrum market is

Geographic sharing occurs when multiple users access the same frequencies in different geographic areas which are sufficiently separated to avoid interference.



Sharing spectrum in time occurs when multiple users access the same frequencies at different times to avoid interference. When a primary spectrum user is not using its spectrum, it could allow access to a secondary user - even if users are in close proximity.



Source: GAO. | GAO-17-75

Figure 14: Illustration and examples of spectrum sharing

hard to predict, they need to be adaptive, and that there is no one-size-fits-all management approach. However, spectrum governance is important. One spectrum research expert told us that spectrum management cannot be left to the free market. This expert likened spectrum oversight to traffic laws, indicating that some standards, rules, and requirements are needed for the system to work well. This expert also suggested that the government should play a role in areas where markets do poorly. Similarly, a participant in our expert meeting told us that because spectrum is a scarce natural resource that is in dispute, the government has a critical role in being an arbiter for allocation.

Over the long-term, as spectrum needs and communication technologies evolve, IoT devices may have antiquated spectrum and communications requirements. One expert from our meeting spoke about an IoT device embedded in infrastructure and designed for 20 years of operations being inaccessible for updates or modifications.[69] Since the IoT device was developed using spectrum rules at a given time, it may become obsolete if the spectrum rules change after being embedded, making communication to the device impossible using established methods. FCC staff we spoke to suggested and encouraged the use of unlicensed spectrum to avoid obsolescence.[70] They told us that if a company were to use licensed spectrum for such purposes, the company would risk that

[69] Experts also indicated that it is critical to consider two-way communication capabilities for inaccessible devices. They told us that being able to update IoT software remotely can help address security and communication challenges.

[70] Licensing assigns a specific portion of spectrum to a specific entity such as a wireless company. In some frequency bands, users do not need to obtain a license to use the spectrum. In such cases, an unlimited number of unlicensed users can share frequencies on a non-interference basis.

conditions may change and the requirement for using licensed spectrum may become obsolete or irrelevant. Use of unlicensed spectrum may also confer other advantages such as lowered costs for manufacturers and consumers, according to an OECD report on the IoT.[71] However, unlicensed spectrum may merit monitoring for interference resulting from increased demand for such spectrum from IoT applications.

The mobile telecommunications industry is developing a new generation of cellular network communications technology, known as 5G, to address the challenges of spectrum interference in unlicensed spectrum, among other things. However, the deployment of new spectrum for the 5G network may pose challenges.[72] No officially recognized definition of 5G exists, but FCC documentation notes that the International Telecommunication Union (ITU) plans to develop requirements by 2017. This fifth-generation technology is intended to address the growth of the IoT, including improved support of machine-to-machine communication, and allowing for higher numbers of mobile broadband users and connected devices, among other things. The United States is participating in work being done by the ITU but is not waiting for the outcome of ITU studies. Instead, according to FCC staff we interviewed, the U.S. approach is to make spectrum available and then rely on private sector-led processes to produce technical standards.[73] This approach may lead to U.S. goods unable to initially integrate with ITU standards and policies, thereby requiring customization of products for each market being entered. There is a knowledge gap currently in the United States regarding 5G implementation and distribution; in particular there are no current 5G technology transfer policies which can create uncertainty in the industry.

4.6 Global initiatives

Many countries have IoT-related national initiatives designed to further IoT development and encourage IoT use around the world. Some of these national initiatives include support for IoT research centers, support programs focusing on improving Internet and broadband access to help foster connectivity, or specific guidance on spectrum use by IoT devices. For example, the South Korean Ministry of Science, Information Communications Technology, and Future Planning released a roadmap for the IoT in November 2014 to guide government actions in developing cybersecurity standards and best practices.

Global standards can facilitate IoT adoption. One expert told us that in the future, successful solutions will depend on implementation of global standards rather than national or regional solutions. Another expert mentioned some urgency to this matter, noting that according to a 2014 National Security Telecommunications Advisory Committee (NSTAC) report on the

[71] OECD, *The Internet of Things: Seizing the Benefits and Addressing the Challenges* (2016).

[72] FCC documentation suggests that part of the focus of 5G development is on frequencies at 24 GHz and above, which includes parts of the spectrum called "millimeter-wave frequencies."

[73] In July 2016, FCC took steps to facilitate mobile broadband and next generation wireless technologies in spectrum above 24 GHz, see https://www.fcc.gov/document/spectrum-frontiers-ro-and-fnprm.

IoT, there is a limited window of about three to five years for countries to influence global standards. The NSTAC report also states that the IoT "requires the development of governance and policy structures much more quickly than the norm" and that "good governance will require international engagement."[74]

Certain countries subsidize IoT development. In terms of policy, participants at our experts meeting told us some countries in Asia have national policies to promote the IoT, including South Korea and China. In South Korea, Japan, and China, there are concentrated research centers to support IoT innovation. Some countries subsidize development of parts of the IoT environment, which may be an area of concern for the United States to avoid an uneven playing field.

Other countries, such as the United Kingdom, have a top-down approach whereby the government establishes regulations that companies must follow. For example, one expert in our meeting said that IoT device manufacturers have not requested dedicated spectrum for IoT devices, and that the FCC has not established dedicated spectrum for IoT devices in the United States. However, an expert in our meeting told us that in the United Kingdom, the spectrum regulatory agency Ofcom has provided spectrum guidance for the IoT, confirming some spectrum specifically for IoT device use. In South Korea, there is a dedicated organization—the Telecommunications Strategy Council—which oversees laws and regulations related to the IoT and collaborates with other ministries to improve relevant regulations. Another expert in spectrum research told us that a more centralized model of spectrum management can more readily focus resources where needed and take a long-term approach, but takes risk that competition could be suppressed.

Experts told us that having a uniform regulation that applies throughout the European Union may make it easier for collaboration within the European Union. For example, The European Union adopted the General Data Protection Regulation (GDPR) in spring 2016, which seeks to simplify data protection for individuals by providing a single set of rules that apply to all European Union member states. It is scheduled to be implemented over the next two years.[75] The financial penalties for violating the GDPR are very high on issues such as obtaining consent, data breaches, and right of data erasure. There are initiatives such as the H2020 Privacy Flag, which is intended to address legal gaps between European Union and other systems.

There are also other implications with doing business in the European Union. For example, a participant in our expert meeting wondered whether one can use U.S.-produced devices within the European Union, and noted that there are issues with international IoT data transfer. Another expert mentioned that there may be issues with data generated from

[74] President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things.* (Washington, D.C.: 2014).

[75] Regulation (E.U.) 2016/679. The proposed new E.U. data protection regime extends the scope of the E.U. data protection law to all foreign companies processing data of E.U. residents. It provides for a harmonization of the data protection regulations throughout the E.U., thereby making it easier for non-European companies to comply with these regulations.

airplanes that fly internationally.[76] To address such issues, experts told us that certain U.S. companies are developing regional data centers in the European Union, and likely vice versa.

4.7 IoT interoperability

Interoperability is the ability of one system to work with or use the parts or equipment of another system. The promise of interoperability is the seamless integration of multiple products from different manufacturers coexisting and sharing data and interfaces, resulting in additional value and operating benefits. However, challenges persist—including consensus on standards—in achieving this level of interoperability.

Full interoperability—the ability of any device to connect and exchange information with other devices—would enable global and cross-industry exchanges of data from IoT devices. However, enabling an environment where any IoT device would be able to connect and exchange information with any other device may be challenging. In practice, interoperability is complex. The adoption of common standards that specify these communication details, are central to the conversation around interoperability and the IoT.

Manufacturers who would like to create IoT products are often met with constraints, such as costs, lead times, or technical performance that make interoperability difficult. Additional challenges occur when manufacturers want new products to be interoperable with legacy products. As a result, manufacturers are faced with design trade-offs between maintaining compatibility with legacy systems by using the legacy standard and using a different standard that may achieve greater interoperability with other devices.

Some manufacturers may design IoT devices to use proprietary protocols or specifications that limit interoperability with other brands to establish a market advantage. Proprietary vendor standards may increase functionality and consistency with that vendor's products, but can complicate integration by other companies. At the same time, proprietary protocols or specifications may create opportunities for companies looking to manufacture and sell "bridge" capabilities that allow that vendor's proprietary products to have some interoperability with open standards.

4.8 Standards for the development and use of the IoT

Currently, there is no single universally recognized set of standards or definitions for the IoT, nor a commonly accepted definition among various standards organizations. Due to the complex nature of the IoT, there are standards that address different aspects of the IoT, especially in communications and networking. According to the IEEE Standards Association, there are more than 350 IEEE standards that can apply to the IoT, and more than 110 IEEE IoT-related standards that are in development.[77] Since there are so many standards, one potential issue is standards

[76] Airplane data not containing personally identifiable information might not be subject to the GDPR.

[77] Institute of Electrical and Electronic Engineers Standards Association, *Internet of Things (IoT) Ecosystem Study* (New York, NY: IEEE, 2015).

incompatibility where a device designed to one standard may not be interoperable with a device designed to a different standard. As a result, many different frameworks have evolved to encompass a set of standards to support interoperability in different use cases.

IoT standards and frameworks are context dependent—encompassing multiple actors (including hardware/device manufacturers, software platform providers, and cloud providers) across distinct sectors such as health, connected homes, wearables, and manufacturing. There are several public and private collaborations that are in the process of establishing IoT standards.

For example, the IEEE Standards Association Panel's project IEEE P2413 "Standards for an Architectural Framework for the Internet of Things" aims to create a blueprint on how IoT devices used in different sectors can interact with each other. In addition, NIST created a "Framework for Cyber-Physical Systems" to guide designing, building and verifying cyber-physical systems—a concept related to the IoT. The ITU formed the ITU-T Study Group 20 to create international standards for IoT technologies, including IoT applications in smart communities.

While established standards development organizations are working on creating IoT standards, new groups have emerged with their own frameworks or sets of standards. For example, the Industrial Internet Consortium, which includes AT&T, IBM, Cisco, GE, and Intel, as well as academic and federal government entities, was formed in 2014 to influence global standards and develop frameworks for interoperability, among other things.

The Thread Group released a framework to be used to ensure all IoT home devices connect seamlessly. The framework covers networking, power usage, and security, among other things. The Thread Group has over 80 members, including Samsung, Philips, and Nest. Likewise, the AllSeen Alliance developed the AllJoyn protocol, an open source software framework that supports interoperability between devices within a Wi-Fi network.

Private industry also has standardization initiatives that include coordination of standards. Individual companies have vested interests in leading the adoption of particular standards and some may be active in multiple standardization efforts. Examples of companies creating frameworks for their own implementation include:

- Apple's HomeKit is a framework for use of devices in the home that can be integrated with other devices that use Apple's software. The framework has specifications for hardware used in IoT devices as well as guidelines for interfaces and software.
- Google's Brillo is an operating system designed to be used in the smart home domain and is supported by specific hardware. Google's Weave is a communication protocol that allows device to device, device to Internet and device to smartphone communications.

Designing products to proven standard specifications can lower risk. 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. However, some areas lack proven standards. Manufacturers need to assess the technical design risk of their products using various standards. For example, there are no widely accepted communication standards for IoT devices that use low data rates, consume low power and require a long range of communication.

According to the IEEE, gaps persist even as different organizations and companies create their own standards. IEEE notes that some standard bodies do not have a global reach, thus standards bodies need to collaborate and coordinate efforts.[78] Additionally, there is no common definition of the IoT among the different standards organizations. Establishing one common definition of the IoT would simplify the coordination among standards bodies.

4.9 Economic ramifications

The IoT has the potential to offer increased economic benefits globally, but it also poses negative implications that need to be addressed. Embedding sensors in IoT devices allows their owners to control their sensor utilization more effectively and efficiently, creating value for their consumers, both in the public and private sectors. Innovators have the potential for enhancing their competitive position by using their assets more efficiently, reducing their costs, and reaching more customers. Improved competitiveness for some, however, can mean losses for others. For example, there is a potential for disruptions affecting certain segments of the labor force such as drivers of some types of vehicles and assembly line workers.

4.9.1 The potential economic impact of the IoT

Estimating the economic impact of new technologies on the economy is difficult, and that is certainly true for the IoT, whose applications are likely to be widespread and span various economic sectors. However, there have been past experiences with some technologies that shed light on the potential economic impacts of the IoT. For example, the SABRE system computerized airline reservations for American Airlines in the mid-1960's and was subsequently expanded as an offering from IBM to the rest of the airline industry some years later.[79] SABRE allowed the industry to better track the status of the seats on aircraft, deliver the information efficiently to booking agents and the airlines, and price seats in a way that increased their utilization. This enhanced management of the industry's physical assets—seats in this case—allowed airlines to reduce the number of empty seats on their flights. Greater utilization of air travel capacity, the availability of more information for both sellers and buyers, and increasing competition in the industry have all contributed to more affordable travel for more people, growing the size of the industry.

Today, IoT has carried the digitization of objects a great deal farther, promising wider reach and more far-reaching economic

[78] Institute of Electrical and Electronic Engineers Standards Association, *Internet of Things (IoT) Ecosystem Study* (New York, NY: IEEE, 2015).

[79] Semi-Automatic Business Research Environment (SABRE), as originally titled. Https://www-03.ibm.com/ibm/history/ibm100/us/en/icons/sabre, last accessed Sept. 22, 2016. Current title is Sabre.

benefits. IoT technology now embeds sensors and actuators into physical objects and integrates them directly into computing systems, making it more effective than the kind of digitization employed in the original SABRE system.

The increase in the growth of the IoT may be attributed to the lowering of manufacturing costs as IoT technologies, including semiconductors, sensors, and actuators, are embedded into physical objects and integrated directly into systems. For example, the cost per-transistor in semiconductors fell by 50 percent between 2012 and 2015, while the cost of micro-electromechanical systems (MEMS) sensors fell by 30 to 70 percent between 2010 and 2015. Today, a growing number of objects in various industries are being equipped with semiconductors and embedded sensors and actuators; thereby greatly increasing the potential impact of the IoT on more sectors of the economy.

4.9.2 Additional possibilities for growth of the IoT

Some indicators show that that IoT will have a profound impact on all aspects of consumer life, industry, and the public sector. However, despite this overall positive effect on global economies, this growth has many influences and will not be easy to quantify.

While the Internet has already brought radical changes to some industries, like the news and music industries, other industries have, so far, not been similarly affected. Other industries lacked the ability to manage and transmit information about their products and services as efficiently in the past, but now are benefitting from the IoT phenomenon. The IoT now enables industries to digitally tag and manage the objects that they produce to more effectively provide information about them in the markets in which they operate. Furthermore, industries can tag physical objects in their work processes and manage and control them in ways that can greatly enhance efficiency and reduce costs. Examples of such industries that are now benefiting from the IoT phenomenon include farming, mining, manufacturing, and transportation and logistics. The IoT is also entering the lives of consumers directly, in products such as wearable fitness trackers and smart home appliances. These changes all translate into efficiency enhancements or added value that some experts claim can be measured as increases in economic welfare.

Innovative examples of productivity-enhancing applications of the IoT abound at the firm level, and they illustrate the economic promise that the technologies hold. One example comes from the mining industry starting in 2010, when a Canadian company contracted with a networking company to connect its offices, miners, equipment, heavy machinery, and other assets in a network across continents. This system allows the company to monitor and control operations with the promise of increasing capacity utilization, reducing operational costs and downtime, and improving mine safety and environmental conditions. Interconnectivity and monitoring help reduce idle time for machinery and mineworkers, improve scheduling of machinery maintenance, and reduce communication and energy costs. It has allowed some operations—such as fixing broken machinery—to be conducted with the help of experts working from central locations and in real time, avoiding expensive downtime and time-consuming travel for technicians. According to a Cisco Systems

study, the IoT system increased mine productivity four-fold, far exceeding the company's targeted improvement of 30 percent.[80] This example is illustrative both of the competitive advantage that an individual company can have through the innovative use of the IoT, as well as how the IoT can enhance economic efficiency.

The accumulation of benefits at the level of the individual organization translates into economic benefits on the industry- and economy-wide levels. The IoT's overall impact on economic growth is subject to uncertainties. It is difficult to forecast the economic impact of the IoT on specific sectors of the economy, let alone the economy as a whole. One sectoral study examines the impact of the IoT on the commercial real estate market in the United States.[81] This 2015 study starts with the premise that sensors, beacons, and smartphones can be used to "instrument" objects that were previously too complex or costly to track and manage. According to this 2015 study, only about two-thirds of the 12 billion square feet of commercial real estate space in the United States is utilized. The study analyzed the impact of an IoT system "using sensors, coupled with understanding of utilization, [in order to] create liquid marketplaces of real estate by enabling real-time discoverability, usability and payment." Assuming a 50 percent adoption of the system, the study concluded that utilization would increase by nearly 40 percent from current levels, which could result in benefits to consumers due to lower rental rates.

Different innovative business models are emerging to take advantage of the economic promise of the IoT. Some businesses continue with a traditional production based business, while others are shifting to a service-based business model. Some businesses focus on developing and producing IoT devices, such as wearable personal health monitors; other businesses focus on creating platforms for more efficient transactions between owners of assets and potential buyers. Yet other companies focus on offering IoT services as a product, designing intelligent networks for individuals and organizations in the private and public sectors.

There is also a growth market for the manufacturers of devices that enable IoT applications. According to an industry study, the market for MEMS, sensors that are heavily used in the IoT, is expected to grow from $10 billion in 2014 to $13 billion in 2020.[82] Their products are used by manufacturers of other devices, such as Fitbit, a manufacturer of fitness trackers that have witnessed phenomenal growth in recent years. The growth in MEMS sensors is driven by growth in the manufacture of various devices used in other applications. In addition to consumer devices like fitness trackers, MEMS are also used in industries such as automotive, data processing, industrial,

[80] CISCO. Internet of Everything Case Study: Mining Firm Quadruples Production with Internet of Everything, (October, 2014).

[81] See Veena Pureswaran and Robin Lougee, *The Economy of Things: Extracting new value from the Internet of Things*, IBM Institute for Business Value (Somers, NY: 2015).

[82] Jérémie Bouchaud, Director and Sr. Principal Analyst MEMS & Sensors, IHS Markit, on the sensor market estimated revenue. Correspondence with GAO Sept. 22, 2016. IHS Markit is a [London-based] company that specializes in market data and analysis for capital intensive industries. These estimates have been corroborated by other market firm estimates of the potential growth of wireless sensor networks.

medical electronics, military and civil aerospace, and wired communications.

A number of companies use a service-based business model based on the use of the Internet and telecommunications technologies to connect customers with owners of physical assets, using platforms that greatly enhance the utilization of these assets. Ride-sharing companies like Uber and Lyft, for example, use online platforms to connect customers with vehicle owners. Airbnb uses a similar business model to connect real estate owners with customers in the hospitality industry. These companies are also a part of the sharing economy. This model is likely to keep growing with new, innovative companies emerging in various areas.

4.9.3 The effect of the IoT on jobs

The OECD reported that economic opportunities emanating from the IoT may be accompanied by disruptions that could affect some businesses and job categories negatively.[83] Businesses that utilize the IoT effectively may have competitive advantage over those businesses that do not. While the IoT is likely to open new employment opportunities and improve work conditions for some workers, other workers could experience negative impacts, including job losses. However, there is no consensus on what the long-term impacts of the IoT will be on employment.

Some disruptive impacts of the IoT have already attracted considerable public attention. For example, ride-sharing companies, which have benefited greatly from the IoT, are likely taking away market share from traditional taxi companies, and cab drivers in many cities around the world have protested, sometimes violently, for fear over their jobs. Driverless vehicles have, in fact, already been deployed in some applications. For example, one mining company operates 69 driverless trucks in its mines. These are huge vehicles that collectively haul millions of tons of material each month. Generally, driverless vehicles are controlled from a remote location by technically skilled employees working in a state-of-the-art operations center hundreds of miles away. Eventually, this mining company aims to remotely control their operations from the pits all the way to the port. Driverless vehicles have also been deployed in military applications, such as minesweeping, and in warehousing and logistics.

Drivers of all kinds of vehicles may eventually face pressure as the penetration of driverless vehicles increases. Earlier this year, six convoys of two or three driverless trucks each, traveled from locations in Sweden, Germany, and Belgium to the Dutch port of Rotterdam. While experts do not see mass adoption of driverless trucks for some time—possibly decades—some maintain that their advent is likely and economically beneficial, despite the disruptions that their initial implementation may cause. A study by Morgan Stanley envisions mass adoption of driverless vehicles, including trucks, within

[83] OECD, *The Internet of Things: Seizing the Benefits and Addressing the Challenges* (Paris: 2016).

the next 20 years.[84] The President of Lyft ride sharing company said in September 2016 that he expects a majority of Lyft cars will be driverless within 5 years (by 2021).

The IoT is likely to have repercussions for other types of workers. Robotics has displaced workers in various sectors, and progress in IoT technologies will increase the threat to some types of jobs. Electronic tagging of objects in the workplace, combined with the use of robots, can result in enhanced efficiency and cost savings in various industries, and part of the savings will be in labor costs. For example, one major China-based supplier for Samsung and Apple announced plans to replace tens of thousands of workers with robots. Some longshoremen worry that their positions may be obsolete as more major seaports adopt robots to handle cargo, thereby threatening their jobs.

As in the case of technological change throughout history, the IoT will likely not only make some jobs obsolete, but also improve the quality of work of some workers, and create new kinds of employment. Tedious, repetitive tasks for some workers will be replaced with more creative work opportunities. New skills will be needed for some workers to conduct operations that were previously conducted by relatively unskilled workers. The IoT is likely to increase demand for information technology workers in fields such as software, hardware, and robotics design; Internet privacy/security; data analysis; and cloud computing. Workers with skills in these areas have already replaced workers displaced by the introduction of IoT-based technologies. One such example is the hiring of highly skilled workers to manage certain mine operations after the introduction of autonomous vehicles displaced the drivers of the old mining trucks.

There is some disagreement among economists who have studied the impact of technology on employment. Optimists point to historic breakthroughs in technology, such as the development of steam power and electricity, which resulted in the creation of employment opportunities while, at the same time, rendered other types of work obsolete. Less optimistic observers point to technological advances that have improved productivity, but did not produce proportional economic and employment growth in developed economies. Also on the optimistic side, two experts at our meeting said that there are hundreds of thousands of unfilled jobs because there is a shortage of people with the new set of skills to manage the IoT and cloud services. These experts, along with several other experts at our meeting stated that there are likely to be net gains in employment due to the IoT.

As in other areas of advanced technology, education and training will figure very prominently in addressing employment challenges. Historically, new technologies result in job creation and job loss. There may be a need for a highly skilled, problem-solving, creative workforce to foster the innovation and development of IoT technologies. Conversely, those areas of the

[84] Shanker, Ravi, et al., *Autonomous Cars: Self-Driving the New Auto Industry Paradigm*, Morgan Stanley Research Global, (November 6, 2013). The study posits a "Utopian" scenario where driverless trucks are fully embraced, probably no earlier than 20 years hence. The study estimates that driverless trucks will then result in annual savings to the transportation industry of $168 billion. They also estimate other benefits, such as a significant decrease in accidents and associated health care costs. The study authors qualify their savings and other benefits analysis as a "thought exercise, rather than a definitive" one.

labor force that have manual, routine, and procedural based jobs may be negatively impacted as those jobs are replaced by technological innovation. Colleges, universities, and vocational schools will play an important part in mitigating these challenges to the labor force.

4.9.4 The IoT influence on market power

Some economic advisors have noted the potential for effects on a market that limits future economic benefits of the IoT to others. One participant at our expert meeting observed that large technology or service providers can leverage their resources and scale to "influence technology ecosystems and technical standards" to create barriers for competition, harming consumers and potential competitors. Another participant at our expert meeting noted that some countries have placed institutional barriers that may limit competition among companies that supply IoT goods and services.

4.10 Other considerations

4.10.1 Digital divide

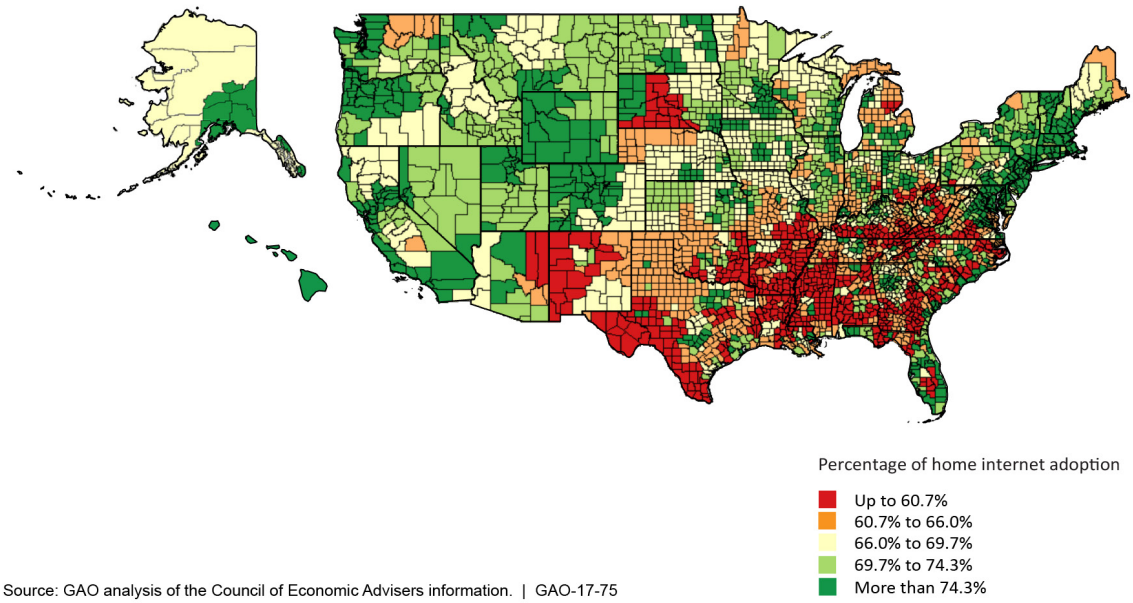
Access to IoT applications may improve quality of life for its users.[85] However, there does not appear to be equitable access to the IoT. The gap between groups that use technology and those that do not—called the digital divide—favors those with reliable access to high-speed networks.[86,87]

The map in figure 15 highlights the digital divide between urban and rural locations. For example, the large areas of dark green represent the top quintile of Internet adoption in the Northeast corridor from Boston to Washington, D.C., around Chicago and its suburbs, and along the California coast from San Diego to the San Francisco Bay. Counties in the rural South and portions of the Southwest have Internet adoption rates in the lowest quintile in the United States.

[85] According to the Rand Corporation in *Europe's policy options for a dynamic and trustworthy development of the Internet of Things* (Santa Monica, CA: 2013).

[86] The Federal Communications Commission reports that 19 million Americans (6 percent) do not have access to fixed broadband – with a majority of those Americans (14.5 million) being in rural areas. Federal Communications Commission, *Eighth Broadband Progress Report* (Washington, D.C.: 2012).

[87] Fewer than 50 percent of households in the bottom income quintile use the Internet at home, according to the Council of Economic Advisers, *Issue Brief: The Digital Divide and Economic Benefits of Broadband Access* (March 2016).



Source: GAO analysis of the Council of Economic Advisers information. | GAO-17-75

Figure 15: Internet adoption in United States by county in 2013

While the map in figure 15 suggests an urban-rural divide, it also reveals several rural areas with relatively high rates of Internet adoption. Examples include much of the Northern Great Plains and several counties in Montana, Wyoming, North Dakota, Colorado and Utah. This suggests that even though geography has an impact on access, other factors also influence Internet adoption.

In many cases, the IoT serves as an extension of the Internet and having access to the Internet is often a necessity to use IoT devices and services. Therefore, existing inequality may be exacerbated by the growth in the IoT. The NTIA surveyed Americans about their use of the IoT in July 2015.[88] At the time, only one percent of Americans used a wearable IoT device. IoT users tended to have the same characteristics as those that also had greater access to the Internet. Americans using IoT technologies had generally attained higher education levels, earned more income, and were more likely to use a smartphone than the average American. Table 3 shows the statistics from the NTIA.

[88] Per the NTIA, Questions on use of IoT were part of the Computer and Internet Use Supplement to the Census Bureau's Current Population Survey.

Demographic	Wearable Device Users	All Americans
Family income < $25,000	8 percent	20 percent
Family income $100,000+	40 percent	24 percent
Lack a High School Diploma (15+)	5 percent	15 percent
Are College Graduates (15+)	52 percent	29 percent
Have a Disability (15+)	6 percent	12 percent
Live in a Metropolitan Area	93 percent	86 percent

Source: National Telecommunications and Information Administration. | GAO-17-75

Table 3: Wearable device users and all Americans: selected demographics (July 2015)

Table 3 shows that although the IoT is often discussed as being equally available to all, it is unevenly distributed, similar to the existing digital divide. According to a RAND Corporation report, designing intuitive interfaces and providing education of the IoT may increase equitable use and shared benefits of the IoT.[89]

Experts at our meeting raised concerns regarding inequitable access to IoT technologies. One expert cited recent data from an app deployed by the City of Boston. The app used a smartphone's location sensor to locate potholes in the city, and the data received were skewed towards wealthier areas of the city where more residents drove with a smartphone.[90] Another expert explained that certain geographic areas may lack the broadband and cellular infrastructure needed to access the IoT. Privacy concerns were also raised, as one expert explained that fee-based services, which provide enhanced digital privacy, may not be a viable option to those with lower incomes.

4.10.2 Electronic waste

As use of the IoT increases, so will electronic waste. Experts at our meeting told us that extremely high production rates of IoT devices have the potential to create massive amounts of hazardous waste when these devices are eventually discarded. As costs for these devices drop, disposing and replacing the devices may become financially easier than repairing them. Furthermore, IoT technologies are often embedded in devices and are not externally visible. Consumers may be unaware that IoT devices contain electronic components and, in disposing of these devices, they are contributing to electronic waste.

Experts also raised concerns that the United States currently relies on developing countries to accept our electronic waste, but that may change in the future. As electronic waste grows, disposal of IoT devices may be challenging due to the harmful effects

[89] Rand Corporation, *Europe's policy options for a dynamic and trustworthy development of the Internet of Things* (Santa Monica, CA: 2013).

[90] FTC, *Big Data, A Tool for Inclusion or Exclusion? Understanding the Issues* (Jan 2016).

associated with the unsafe handling and disposal of these products.[91] Another expert noted that IoT waste may impact lower income communities in the United States, as history has shown the waste is often discarded in these communities. One expert suggested focusing on sustainable engineering in IoT devices to help reduce the amount of electronic waste. This expert suggested government could contribute to promoting sustainable engineering in its research agenda.

[91] Mercy Wanjau, Principal Legal Officer at the Communications Commission of Kenya, already noted in 2011, (see ITU News, No. 9, 2011) that "e-waste is one of the fastest growing waste streams."

5 Summary

The IoT is being adopted globally across multiple sectors, including the public sector, agriculture, health care, manufacturing, and energy, among others. IoT technologies have evolved from a tool for simple communication and tracking via networks to include service-based business offerings that rely on data analytics. Adoption will likely accelerate as IoT devices become more affordable and offer increasing benefits. However, significant challenges accompany the wider adoption of IoT technologies. For example, devices that collect health information on patients may be vulnerable to hacking. With the rapid global expansion of IoT, security and privacy measures become increasingly important to curtail its misuse. Although there is no single U.S. federal agency that has overall regulatory responsibility for the IoT, various agencies oversee or regulate aspects of the IoT, such as specific sectors, types of devices, or data. Generally, industries use the IoT to reduce costs through efficiencies, among other things, while addressing the challenges of enhancing interoperability of IoT devices, and maintaining security and privacy. Estimating the economic impact of the IoT is complicated due to the large number of widespread applications that span various economic sectors and related environmental impacts. Economic opportunities resulting from the IoT may be accompanied by disruptions that pose challenges to certain businesses and job categories.

Agency and expert comments

We provided a draft of this report to 10 federal agencies for review and comment. They were the Department of Commerce (NIST and NTIA), Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Justice, Department of Transportation, Federal Communications Commission, Federal Trade Commission, National Science Foundation, and the Office of Science and Technology Policy. Although we made no recommendations in this technology assessment report, the agencies were asked for feedback on the draft in its entirety. None of the entities provided a written response. However, they did provide technical comments and we incorporated the comments as appropriate.

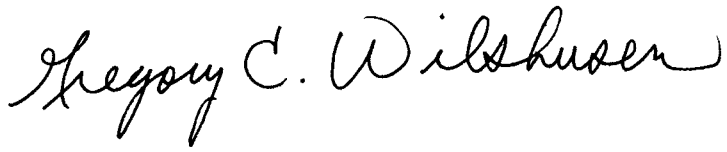
We invited 27 participants from our 2 meetings of experts to review our draft report. We asked them to review the draft with respect to factual accuracy, scientific and technical quality, and for errors of omission. Of the 14 participants who responded, 12 provided technical comments. Many of the comments were suggestions to add more details, to use different terms, and to include additional specific examples, while others were strictly editorial. We incorporated the technical comments as appropriate throughout the report. One meeting expert expressed concern about the tone of our economic assessment, and suggested adding potential positive effects of the IoT on certain data analyst jobs. We made changes to our economic assessment that we believe address this concern.

We are sending copies of this report to the appropriate congressional committees, relevant federal agencies, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov or Mark Goldstein at (202) 512-6670 or goldsteinm@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Nabajyoti Barkakati
Director, Center for Technology and Engineering

Mark Goldstein
Director, Physical Infrastructure Issues



Gregory C. Wilshusen
Director, Information Security Issues

List of Requesters

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Brian Schatz
Ranking Member
Subcommittee on Communications, Technology, Innovation, and the Internet
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Cory Booker
United States Senate

The Honorable Deb Fischer
United States Senate

The Honorable Cory Gardner
United States Senate

Appendix I: Objectives, scope, and methodology

GAO was asked by Congressional requestors to conduct a technology assessment of the Internet of Things (IoT). This report describes the IoT and examines: (1) what is known about current and emerging IoT technologies, (2) how and for what purpose IoT technologies are being applied, and (3) potential implications of the use of IoT technologies.

Our initial research found there are several other technical terms used to describe the same or similar concepts to the IoT. Table 4 describes some of these concepts.

Concept Name	Description
Cyber Physical Systems	Smart systems of interacting networks of physical and computation components.
Internet of Everything	Expansion of the IoT to encompass networks of people, process, data, and things, where billions of connections increase both opportunities for innovation and vulnerabilities.
Network of Things	A broader class of connected 'things', which could be either virtual or physical, that are connected to any network, including but not limited to the Internet.
Web of Things	A concept where people, places, and ideas are represented virtually.

Source: GAO. | GAO-17-75

Table 4: Concepts similar to the IoT

For the purposes of this technology assessment, we use the term IoT to refer to the concept of connecting a wide array of objects that can sense and communicate information to a network.

To determine what is known about current and emerging IoT technologies, we reviewed various reports; documents; and scientific literature including government reports; conference papers; articles published in peer-reviewed journals or written by nonprofit organizations, think tanks, and industry; and relevant books describing current and developing IoT technologies and their uses. We concentrated on consumers, industry, and the public sector.

We attended multiple technical conferences to gather data and learn about the latest IoT technologies and advancements in the industries implementing the IoT. These include Internet of Things: Innovation and Growth 2015 in San Francisco, CA; the 3rd Annual Internet of Things Global Summit 2015 in Washington, DC; the Global Cities Team Challenge Kickoff at the National Institute of Standards and Technology in Gaithersburg, MD; and the Internet of Things World Conference in San Francisco, CA.

We convened a meeting of experts to gather data and various viewpoints regarding the technical aspects of the IoT, including emerging IoT technologies; interoperability; technical standards; and ancillary technical components of the IoT, such as spectrum management, device software, and network architecture. The experts participating in the meeting specialized in various disciplines,

including computer science, electrical engineering, embedded systems architecture, networked systems, and technology standards. They were from the federal government, academia, technology companies, and international standards-making bodies. We continued to draw on the expertise of these individuals throughout our study. The detailed methodology on the selection of experts for the meeting is discussed later in this appendix.

To identify how IoT technologies are being applied, we reviewed literature and attended conferences to determine the end users and the usage areas or sectors of the IoT. To determine the end users of the IoT, we reviewed the literature and identified users who either consume IoT technologies or benefit from its implementation. We identified three broad categories: consumers, industry, and the public sector. To identify the sectors serving these user categories, we reviewed literature sources using the criteria of frequency of mention. Within the consumer user category, the sectors that were mentioned most often were wearables, smart homes/building, and vehicles. Within the industry user category, the sectors that were mentioned most often were smart home/building, manufacturing, agriculture, supply chain, energy, and health care. Within the public sector user category, the sectors that were mentioned most often were communities and the environment. To learn the extent of IoT technologies use, we interviewed subject matter experts, such as representatives from communities implementing the IoT.

To determine potential implications of the IoT, we conducted interviews. For implications on spectrum management, we interviewed experts in academia as well as representatives from the Federal Communications Commission. To better understand the implications to regulations, we interviewed staff from the Federal Trade Commission. For the remaining implications, we reviewed relevant literature and attended conferences. Our review was not exhaustive of all programs, agencies, or sectors.

Additionally, to address the second and third objectives, we convened a second meeting of experts to gather data and various viewpoints on the uses and implications of IoT technologies in consumer, industrial, and public sector applications. This included discussions on policies to ensure device security and user privacy; economic impacts of the IoT on business models and desirable workforce skills; examining access to the IoT; and international frameworks and regulatory structures. The experts participating in the second meeting specialized in various disciplines including information security, economics, engineering, privacy, computer science, data analytics, physics, communications, media, chemistry, transportation, cloud computing, software development, telecommunications, database management, and technology policy. The experts were from federal government agencies, academia, and technology companies.

Because the IoT consists of emerging and evolving technologies, we convened the meetings to supplement our understanding of the technology. We collaborated with the National Academy of Sciences (NAS) staff to convene the two expert meetings at the Keck Center in Washington D.C. Additionally, we collaborated with NAS staff to select experts from federal government agencies, academia,

technology companies, and international standards-making bodies, with expertise covering significant areas of our review. The first meeting was held on April 12, 2016 and focused on the technical aspects of the IoT. The second meeting was held on May 24-25, 2016 and focused on the uses and implications of the IoT. NAS staff asked members of the Computer Science and Telecommunications Board and a current Academies study committee on cyber-physical systems to identify relevant experts. Biographical information for this pool of potential experts was reviewed and experts were selected based on sub-topics of the two meetings.

The experts we selected were surveyed to identify any circumstances that could be viewed by others as affecting their objectivity. Twenty-seven experts were considered to be objective, and the group as a whole was determined to be balanced with representations of a wide range of significant viewpoints on the agenda topics. Additionally, a Professor from Massachusetts Institute of Technology provided a presentation for the first NAS meeting. See appendix III for a list of these experts and their affiliations.

The meetings were recorded and transcribed to accurately capture the experts' statements. After the meetings, we analyzed the transcription to help inform the structure and design of our study. We continued to seek advice from these experts to clarify and expand upon what we had learned. Consistent with our quality assurance framework, we provided the experts with a draft of our report and solicited their feedback, which we incorporated as appropriate.

We conducted our work from September 2015 to May 2017 in accordance with all sections of GAO's quality assurance framework relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for our findings in this product.

Appendix II: IoT use examples

Sector	IoT Technologies Description	Examples	User
Wearables	Smart technology worn on various parts of the body or embedded into attire.	• Clothing for babies that monitor their respiration, temperature, and activity level. • Football helmets that detect impacts and notify medical staff. • Bands worn around the lower back that notify the wearer when it detects slouching. • Wearable fitness trackers that count steps and measure pulse and heart rate.	Consumer
Homes and buildings	Networked electronic home equipment, primarily for monitoring, comfort, convenience, as well as assisted living. Office buildings use the technology to control lights, temperature, and to track space utilization.	• Smart Thermostats gather data on motion, temperature, humidity and light and combine that with data analysis to automate the control of the temperature based on the users' habits. Also these thermostats can connect to the energy utility company, and the utility can remotely control energy usage during periods of high energy demand. • Smart lights and motion detectors have sensors and can turn lights on and off when motion or activity is detected. • Refrigerator that is equipped with an internal camera that enables a user to remotely view the contents of the refrigerator. • Lawn sprinkler system that automatically turns off when it senses rain.	Consumer Industry
Vehicles	Technology used for, among other things, safety, such as automatic braking, predict maintenance and enhance performance. Vehicles can also be used as a platform for other sensors.	• Railroads are using sensors on both trains and the tracks to create more accurate scheduling as well as predict maintenance. • Many automobiles now have collision detection and automatic braking systems to help avoid accidents. • Vehicle traffic sensors and cameras collect data on the speed, heading, braking and other information, which is then transmitted via short range radio to other nearby vehicles.	Consumer Industry Public Sector

Sector	IoT Technologies Description	Examples	User
		• Automobile manufacturers are able to upgrade software in cars remotely.	
Manufacturing	Using sensors to control and monitor the manufacturing process as well as to predict system maintenance.	• Jet engines are outfitted with different sensors in order to detect performance and failure conditions that enable better predictions for maintenance and reduce downtime. • Chemical plants use sensors to measure ingredient mixtures, pressure, and temperature, and then design controls to automatically adjust conditions or modify ingredients. • Pulp and paper manufacturers use sensors to manage temperature, changing the shape and intensity of the flame in the kiln.	Industry
Agriculture	Optimize operations and decrease costs using such technology as field sensors or animal tracking chips.	• IoT devices on animals can detect early signs of health issues. • Monitoring systems on cows to sense optimal breeding times. • Farmers use data from sensors on equipment and plants, combining it with satellite images and weather tracking for higher productivity and more efficient use of resources. • Greenhouses use the IoT to gather data on the temperature, humidity, and soil.	Industry
Energy	Technologies used to automate actions to improve the electric grid's reliability and efficiency.	• Smart meters used to provide customers with a visual display of energy usage. • Sensors in turbines for wind energy to adjust blade angles on windmills.	Industry
Supply Chain	Embedding sensors on products for inventory management in order to cut cost and reduce inefficiencies.	• Inventory is tagged to provide real time location information. • Trucking companies use weather data, traffic patterns to optimize routes. • Soft drink distributors use sensors on products and in vending machines for inventory management.	Industry
Health care	Medical devices and technology used in health care settings to	• Patients with congestive heart failure wear sensors to monitor weight, blood pressure,	Consumer

Sector	IoT Technologies Description	Examples	User
	generate data used to improve health outcomes.	and heart rate for early detection of problems. • IoT devices, both wearables and context-aware, can be used in home to detect if a patient falls. • Smart hospital beds automatically adjust to patients movements.	Industry
Environment	Used to monitor weather, air and water pollution as well as natural disaster monitoring for earlier detection of natural disasters such as wildfires and landslides.	• Pollen sensors can create a map to show where pollen is worse for people with allergies. • Air quality sensors that collect data on pollution. • Waterway sensors that manage water resources and collect information on flow, temperature and pollution. • Cameras and sensors are combined to detect forest fires. • Drones used in disaster management to collect information and imagery where people are not able to enter.	Public Sector
Communities	A community in which IoT-related technologies have been deployed or are being developed to improve the livability, management, or service delivery of the community.	• Law enforcement uses sonic sensors to pinpoint gunshots. • Busses have sensors that report real time location information. • Barcelona uses sensor networks in traffic management, trash collection, public safety policing, road management, road maintenance, and snow removal. • Sensors embedded in parking spots to notify drivers of open parking spots. • Trash can sensors alert waste management when the cans are full.	Public Sector

Source: GAO. | GAO-17-75

Appendix III: Expert participation

We collaborated with the National Academy of Sciences to convene two meetings of experts to inform our work. The experts who participated in our study are listed below.

Ms. Kendall Burman

Cybersecurity and Data Privacy Counsel
Mayer Brown, LLP

Dr. Robert Cohen

Economist and Senior Fellow
Economic Strategy Institute

Dr. Shoumen Palit Austin Datta

Vice President, Industrial Internet Consortium
Research Affiliate, School of Engineering
Massachusetts Institute of Technology

Mr. Mark Eichorn

Assistant Director, Division of Privacy and Identity Protection
Federal Trade Commission

Dr. Nick Feamster

Professor of Computer Science
Acting Director, Center for Information Technology Policy
Princeton University

Dr. Batya Friedman

Professor of Information
University of Washington

Dr. Kevin Fu

Associate Professor of Electrical Engineering and Computer Science
University of Michigan

Dr. Chris Greer

Director, Smart Grid and Cyber-Physical Systems Program Office
National Institute of Standards and Technology

Dr. Haitham Hassanieh

Assistant Professor of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Dr. Verena Kantere

Associate Professor, Centre Universitaire d' Informatique
University of Geneva

Mr. Mark Kraeling

Product Manager and System Architect
General Electric Transportation

Dr. Santosh Kumar

Professor of Computer Science
University of Memphis

Dr. David Lary

Professor of Physics
University of Texas at Dallas

Mr. Kenneth Leonard

Director, Intelligent Transportation Systems Joint Program Office
U.S. Department of Transportation

Dr. Ratul Mahajan

Principal Researcher, Microsoft Research
Affiliate Professor
University of Washington

Mr. Brian Markwalter

Senior Vice President of Research and Standards
Consumer Technology Association

Dr. Margaret Martonosi

Hugh Trumbell Adams ’35 Professor of Computer Science
Princeton University

Dr. Lee McKnight

Professor of Entrepreneurship and Innovation
Syracuse University

Ms. Emily McReynolds

Program Director, Tech Policy Lab
University of Washington

Mr. Wesley Mukai

Chief Technology Officer
GE Transportation Digital Solutions

Mr. Dennis Roberson

Vice Provost and Research Professor
Illinois Institute of Technology

Ms. Karen Rose

Senior Director, Strategy and Analysis
Internet Society

Mr. Sudhi Sinha

Vice President of Product Development
Johnson Controls

Dr. Daniel Spulber

Professor of International Business and Strategy
Northwestern University

Dr. S. Shyam Sundar

Professor
Penn State University

Dr. David Wollman

Deputy Director, Smart Grid and Cyber-Physical Systems Program Office
National Institute of Standards and Technology

Mr. Sébastien Ziegler

President
IoT Forum

Appendix IV: GAO contact and staff acknowledgments

GAO contact

Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Mark Goldstein, (202) 512-6670 or goldsteinm@gao.gov

Gregory Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff acknowledgements

In addition to the contacts named above, Edward Alexander, Jr., Pille Anvelt, Ana Ivelisse Avilés, Jennifer Beddor, Angela Bell, Amy Bowser, Marisol Cruz, Gary DePalo, John de Ferrari, Philip Farah, Dani Greene, Hayden Huang, Michael Kaeser, Gretchen Snoey, Elaine Vaurio, and Susan Zimmerman made key contributions to this report.

Eli Albagli, Tommy Baril, Robert Breitbeil, Bruce Cain, Brett Caloia, Timothy Carr, Joseph Cook, Leia Dickerson, Karen Doran, David Dornisch, Lawrence Evans, Jr., Shirley Jones, Joseph Kirschbaum, Christopher Murray, John Neumann, Penny Pickett, Sarah Resavy, Oliver Richard, Stephen Sanford, Andrew Stavisky, Eugene Stevens, Walter Vance, John Yee, and Carolyn Yocom also made contributions to this report.

Related GAO products

Health Care: Telehealth and Remote Patient Monitoring Use in Medicare and Selected Federal Programs. GAO-17-365. Washington, D.C.: April 14, 2017.

Open Innovation: Practices to Engage Citizens and Effectively Implement Federal Initiatives. GAO-17-14. Washington, D.C.: October 13, 2016.

Highlights of a Forum: Data and analytics innovation: Emerging opportunities and challenges. GAO-16-659SP. Washington, D.C.: September 20, 2016.

Long-term Care Workforce: Better information needed on nursing assistants, home health aides, and other direct care workers. GAO-16-718. Washington, D.C.: September 15, 2016.

Information Technology Reform: Agencies need to increase their use of incremental development practices. GAO-16-469. Washington, D.C.: August 16, 2016.

Intelligent Transportation Systems: Urban and rural transit providers reported benefits but face deployment challenges. GAO-16-638. Washington, D.C.: June 21, 2016.

Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. GAO-16-350. Washington, D.C.: March 24, 2016.

Critical Infrastructure Protection: Cybersecurity of the nation's electricity grid requires continued attention. GAO-16-174T. Washington, D.C.: October 21, 2015.

Unmanned Aerial Systems: FAA continues progress toward integration into the national airspace. GAO-15-610. Washington, D.C.: August 17, 2015.

Telecommunications: Agencies need better controls to achieve significant savings on mobile devices and services. GAO-15-431. Washington, D.C.: May 21, 2015.

Cybersecurity: Actions needed to address challenges facing federal systems. GAO-15-573T. Washington, D.C.: April 22, 2015.

Mobile Devices: Federal agencies' steps to improve mobile access to government information and services. GAO-15-69. Washington, D.C.: December 22, 2014.

Intelligent Transportation Systems: Vehicle-to-vehicle technologies expected to offer safety benefits, but a variety of deployment challenges exist. GAO-14-13. Washington, D.C.: November 1, 2013.

Spectrum Management: Incentives, opportunities, and testing needed to enhance spectrum sharing. GAO-13-7. Washington, D.C.: November 14, 2012.

Medical Devices: FDA should expand its consideration of information security for certain types of devices. GAO-12-816. Washington, D.C.: September 27, 2012.

Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy. GAO-12-903. Washington, D.C.: September 11, 2012

Cybersecurity: Challenges in securing the electricity grid. GAO-12-926T. Washington, D.C.: July 17, 2012.

Cybersecurity: Threats impacting the nation. GAO-12-666T. Washington, D.C.: April 24, 2012.

Electricity Grid Modernization: Progress being made on cybersecurity guidelines, but key challenges remain to be addressed. GAO-11-117. Washington, D.C.: January 2, 2011.

Electronic Government: Challenges to the adoption of smart card technology. GAO-03-1108T. Washington, D.C.: September 9, 2003.

For previously issued GAO Technology Assessments, go to http://www.gao.gov/technology_assessment/key_reports .

(100312)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu