The Internet of Things: Frequently Asked Questions

Eric A. Fischer
Senior Specialist in Science and Technology

October 13, 2015

Congressional Research Service
7-5700
www.crs.gov
R44227

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

"Internet of Things" (IoT) refers to networks of objects that communicate with other objects and with computers through the Internet. "Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems.

In other words, the IoT potentially includes huge numbers and kinds of interconnected objects. It is often considered the next major stage in the evolution of cyberspace. Some observers believe it might even lead to a world where cyberspace and human space would seem to effectively merge, with unpredictable but potentially momentous societal and cultural impacts.

Two features makes objects part of the IoT—a unique identifier and Internet connectivity. Such "smart" objects each have a unique Internet Protocol (IP) address to identify the object sending and receiving information. Smart objects can form systems that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes and potentially transforming them into integrated systems.

Those systems can potentially impact homes and communities, factories and cities, and every sector of the economy, both domestically and globally. Although the full extent and nature of the IoT's impacts remain uncertain, economic analyses predict that it will contribute trillions of dollars to economic growth over the next decade. Sectors that may be particularly affected include agriculture, energy, government, health care, manufacturing, and transportation.

The IoT can contribute to more integrated and functional infrastructure, especially in "smart cities," with projected improvements in transportation, utilities, and other municipal services. The Obama Administration announced a smart-cities initiative in September 2015.

There is no single federal agency that has overall responsibility for the IoT. Agencies may find IoT applications useful in helping them fulfill their missions. Each is responsible for the functioning and security of its own IoT, although some technologies, such as drones, may fall under the jurisdiction of other agencies as well. Various agencies also have relevant regulatory, sector-specific, and other mission-related responsibilities, such as the Departments of Commerce, Energy, and Transportation, the Federal Communications Commission, and the Federal Trade Commission.

Security and privacy are often cited as major issues for the IoT, given the perceived difficulties of providing adequate cybersecurity for it, the increasing role of smart objects in controlling components of infrastructure, and the enormous increase in potential points of attack posed by the proliferation of such objects. The IoT may also pose increased risks to privacy, with cyberattacks potentially resulting in exfiltration of identifying or other sensitive information about an individual. With an increasing number of IoT objects in use, privacy concerns also include questions about the ownership, processing, and use of the data they generate.

Several other issues might affect the continued development and implementation of the IoT. Among them are

- the lack of consensus standards for the IoT, especially with respect to connectivity;
- the transition to a new Internet Protocol (IPv6) that can handle the exponential increase in the number of IP addresses that the IoT will require;

- methods for updating the software used by IoT objects in response to security and other needs;
- energy management for IoT objects, especially those not connected to the electric grid; and
- the role of the federal government, including investment, regulation of applications, access to wireless communications, and the impact of federal rules regarding "net neutrality."

No bills specifically on the IoT have been introduced in the 114th Congress, although S.Res. 110 was agreed to in March 2015, and H.Res. 195 was introduced in April. Both call for a U.S. IoT strategy, a focus on a consensus-based approach to IoT development, commitment to federal use of the IoT, and its application in addressing challenging societal issues. House and Senate hearings have been held on the IoT, and several congressional caucuses may consider associated issues. Moreover, bills affecting privacy, cybersecurity, and other aspects of communication could affect IoT applications.

Contents

What Is the Internet of Things (IoT)? 1
How Does the IoT Work? 2
What Impacts Will the IoT Have? 4
- Economic Growth 4
- Economic Sectors 4
  - Agriculture 4
  - Energy 5
  - Health Care 6
  - Manufacturing 6
  - Transportation 6
  - Infrastructure and Smart Cities 7
- Social and Cultural Impacts 8

What Is the Current Federal Role? 8
What Issues Might Affect the Development and Implementation of the IoT? 11
- Technical Issues 11
  - Internet Addresses 11
  - High-Speed Internet 13
  - Wireless Communications 13
  - Standards 13
  - Other Technical Issues 14
- Cybersecurity 14
- Safety 15
- Privacy 16
- Other Policy Issues 17
  - Federal Role 17
  - Spectrum Access 18
  - Net Neutrality 18

What Actions Has Congress Taken? 19
- Legislation 19
  - Bills 19
  - Resolutions 19
- Hearings 19
- Caucuses 20

Where Can I Find Additional Resources on This Topic? 20

Contacts

Author Contact Information 20
Acknowledgments 20

The Internet of Things (IoT) is a complex, often poorly understood phenomenon. The term is more than a decade old, but interest has grown considerably over the last few years as applications have increased.[1] The impacts of the IoT on the economy and society more generally are expected by many to grow substantially. This report was developed to assist Congress in responding to some commonly asked questions about it:

- "What Is the Internet of Things (IoT)?"
- "How Does the IoT Work?"
- "What Impacts Will the IoT Have?"
- "What Is the Current Federal Role?"
- "What Issues Might Affect the Development and Implementation of the IoT?"
- "What Actions Has Congress Taken?"
- "Where Can I Find Additional Resources on This Topic?"

What Is the Internet of Things (IoT)?

When people talk about the Internet, they are usually referring to the electronic network that permits computers around the world to communicate with each other. What, then, is the IoT? There is no universally agreed-upon definition,[2] but generally, the term is used to describe networks of objects that are not themselves computers but that have embedded components that connect to the Internet. "Things" may include, for example, smart meters, fitness trackers, personal vehicles, home appliances, medical devices, and even clothing used by individual consumers. They may also include embedded devices in roadways and in other components of infrastructure such as electric grids, manufacturing plants and other buildings, farms, and virtually any other object, element, or system for which remote communications, control, or data collection and processing might be useful.

While fixed and mobile computing devices such as desktop computers, smartphones, and tablets are generally not considered to be IoT objects, smartphones in particular have features such as motion and position sensors that blur the distinctions.[3] Some smartphone applications, for example, enable them to be used in fitness tracking and other health monitoring.

In other words, the IoT potentially includes huge numbers and kinds of interconnected objects. In practice, IoT refers not to a simple or uniform network of objects but rather to a complex collection of objects and networks. Specific dimensions of the IoT may be referred to by terms such as smart grid, connected cities, and Industrial Internet.[4] Other terms may also be used in the

[1] Postscapes, "A Brief History of the Internet of Things," 2015, http://postscapes.com/internet-of-things-history.

[2] See, for example, Roberto Minerva, Abyi Biru, and Domenico Rotondi, "Towards a Definition of the Internet of Things (IoT)" (IEEE Internet Initiative, May 27, 2015), http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

[3] Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (Mercatus Center (George Mason University), November 19, 2014, http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without.

[4] See, for example, Goldman Sachs Global Investment Research, "Our Thinking—What Is the Internet of Things?," *Goldman Sachs*, September 2014, http://www.goldmansachs.com/our-thinking/pages/iot-infographic.html. Some observers even use Industrial Internet as a synonym for the IoT, although it more commonly applies to manufacturing and other industrial activities. See, for example, World Economic Forum, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services" (World Economic Forum, January 2015), http://www.weforum.org/reports/industrial-internet-things-unleashing-potential-connected-products-and-services; Industrial Internet Consortium, (continued...)

context of IoT to denote related concepts such as cyber-physical systems[5] and the Internet of Everything.[6]

The IoT is often considered the next major stage in the evolution of cyberspace.[7] The first electronic computers were developed in the 1940s, but forty years passed before connecting computers through wired devices began to spread in the 1980s. The first decade of the twenty-first century saw the next stage, marked by the rapid spread of smartphones and other mobile devices that use wireless communications,[8] as well as social media, big-data analytics, and cloud computing.[9] Building on those advances, connections between two or more machines (M2M) and between machines and people are expected by many observers to lead to huge growth in the IoT by 2020.[10]

How Does the IoT Work?

The IoT is not separate from the Internet, but rather, a potentially huge extension and expansion of it. The "things" that form the basis of the IoT are objects. They could be virtually anything—streetlights, thermostats, electric meters,[11] fitness trackers, factory equipment, automobiles, unmanned aircraft systems (UASs or drones),[12] or even cows or sheep in a field.[13] What makes an

(...continued)

"Home," 2015, http://www.industrialinternetconsortium.org/index.htm.

[5] National Institute of Standards and Technology, "Cyber-Physical Systems," May 22, 2015, http://www.nist.gov/cps/index.cfm. NIST defines cyber-physical systems as "co-engineered interacting networks of physical and computational components." It is a somewhat broader concept than the IoT, in that such systems need not be connected to the Internet to function.

[6] Cisco, "The Internet of Everything," 2013, http://perma.cc/Y4LQ-633J?type=live. This concept is similar to that of the IoT but emphasizes its ubiquity, leading some observers to argue that it is more comprehensive (Dorothy Shamonsky, "Internet of Things vs. Internet of Everything: Does the Distinction Matter to User Experience Designers?," *ICS Insight Blog*, July 13, 2015, http://www.ics.com/blog/internet-things-vs-internet-everything-does-distinction-matter-user-experience-designers). For purposes of this report, they are treated as synonymous.

[7] The term *cyberspace* usually refers to the worldwide collection of connected ICT components, the information that is stored in and flows through those components, and the ways that information is structured and processed. Its evolution has been characterized in many different ways, but IoT's emergence is a common theme. See, for example, Janna Anderson and Lee Rainie, "The Internet of Things Will Thrive by 2025," *Pew Research Center*, May 14, 2014, http://www.pewinternet.org/2014/05/14/internet-of-things/; Simona Jankowski et al., "The Internet of Things: Making Sense of the Next Mega-Trend" (Goldman Sachs Global Investment Research, September 3, 2014), http://www.goldmansachs.com/our-thinking/pages/internet-of-things/iot-report.pdf; The White House, "Cyberspace Policy Review," May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf..

[8] Pew Research Internet Project, "Device Ownership over Time," January 2014, http://www.pewinternet.org/data-trend/mobile/device-ownership/.

[9] Nicholas D. Evans, "SMAC and the Evolution of IT," *Computerworld*, December 9, 2013, http://www.computerworld.com/article/2475696/it-transformation/smac-and-the-evolution-of-it.html. SMAC stands for social media, mobile devices, analytics (big data), and cloud computing.

[10] Gartner, Inc., "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015" (press release, November 11, 2014), http://www.gartner.com/newsroom/id/2905717; Leon Spencer, "Internet of Things Market to Hit $7.1 Trillion by 2020: IDC," June 5, 2014, http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/.

[11] See CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by Brandon J. Murrill, Edward C. Liu, and Richard M. Thompson II.

[12] See CRS Report R44192, *Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry*, by Bill Canis.

[13] Tove B. Danovich, "Internet-Connected Sheep and the New Roaming Wireless," *The Atlantic*, February 9, 2015, http://www.theatlantic.com/technology/archive/2015/02/internet-connected-sheep-and-the-new-roaming-wireless/385274/; David Evans, "Introducing the Wireless Cow," *The Agenda*, July 2015, http://www.politico.com/agenda/(continued...)

object part of the IoT is embedded or attached computer chips or similar components that give the object both a unique identifier and Internet connectivity. Objects with such components are often called "smart"—such as smart meters and smart cars.

Internet connectivity allows a smart object to communicate with computers and with other smart objects. Connections of smart objects to the Internet can be wired, such as through Ethernet cables, or wireless, such as via a Wi-Fi or cellular network.

To enable precise communications, each IoT object must be uniquely identifiable. That is accomplished through an Internet Protocol (IP) address, a number assigned to each Internet-connected device, whether a desktop computer, a mobile phone, a printer, or an IoT object.[14] Those IP addresses ensure that the device or object sending or receiving information is correctly identified.

What kinds of information do IoT objects communicate? The answer depends on the nature of the object, and it can be simple or complex. For example, a smart thermometer might have only one sensor, used to communicate ambient temperature to a remote weather-monitoring center. A wireless medical device might, in contrast, use various sensors to communicate a person's body temperature, pulse, blood pressure, and other variables to a medical service provider via a computer or mobile phone.

Smart objects can also be involved in command networks. For example, industrial control systems can adjust manufacturing processes based on input from both other IoT objects and human operators. Network connectivity can permit such operations to be performed in "real time"—that is, almost instantaneously.

Smart objects can form systems that communicate information and commands among themselves, usually in concert with computers they connect to. This kind of communication enables the use of smart systems in homes, vehicles, factories, and even entire cities.

Smart systems allow for automated and remote control of many processes. A smart home can permit remote control of lighting, security, HVAC (heating, ventilating, and air conditioning), and appliances. In a smart city, an intelligent transportation system (ITS) may permit vehicles to communicate with other vehicles and roadways to determine the fastest route to a destination, avoiding traffic jams, and traffic signals can be adjusted based on congestion information received from cameras and other sensors.[15] Buildings might automatically adjust electric usage, based on information sent from remote thermometers and other sensors.[16] An Industrial Internet application can permit companies to monitor production systems and adjust processes, remotely control and synchronize machinery operations, track inventory and supply chains, and perform other tasks.[17]

(...continued)

story/2015/06/internet-of-things-growth-challenges-000098.

[14] Internet Assigned Numbers Authority (IANA), "Number Resources," 2015, https://www.iana.org/numbers.

[15] Department of Transportation, "Intelligent Transportation Systems (ITS)," 2015, http://www.its.dot.gov/index.htm; Bruce Katz, "Why the U.S. Government Should Embrace Smart Cities" (Brookings Institution, July 26, 2011), http://www.brookings.edu/research/opinions/2011/07/26-cities-katz.

[16] Richard Barker and Amy Liu, "Smart Buildings the Next Step for Seattle," *Brookings Institution*, July 28, 2014, http://www.brookings.edu/blogs/the-avenue/posts/2014/07/28-smart-buildings-seattle-barker-liu; Bob Violino, "Smart Cities Are Here Today—and Getting Smarter," *Computerworld*, February 12, 2014, http://www.computerworld.com/article/2487526/emerging-technology-smart-cities-are-here-today-and-getting-smarter.html.

[17] See, for example, Industrial Internet Consortium, "Home."

IoT connections and communications can be created across a broad range of objects and networks and can transform previously independent processes into integrated systems. These integrated systems can potentially have substantial effects on homes and communities, factories and cities, and every sector of the economy, both domestically and globally.

What Impacts Will the IoT Have?

The IoT may significantly affect many aspects of the economy and society, although the full extent and nature of its eventual impacts remains uncertain. Many observers predict that the growth of the IoT will bring positive benefits through enhanced integration, efficiency, and productivity across many sectors of the U.S. and global economies.[18] Among those commonly mentioned are agriculture, energy, health care, manufacturing, and transportation. Significant impacts may also be felt more broadly on economic growth, infrastructure and cities, and individual consumers. However, both policy and technical challenges, including security and privacy issues, might inhibit the growth and impact of IoT innovations.

Economic Growth

Several economic analyses have predicted that the IoT will contribute significantly to economic growth over the next decade, but the predictions vary substantially in magnitude. The current global IoT market has been valued at about $2 trillion, with estimates of its predicted value over the next five to ten years varying from $4 trillion to $11 trillion.[19] Such variability demonstrates the difficulty of making economic forecasts in the face of various uncertainties, including a lack of consensus among researchers about exactly what the IoT is and how it will develop.[20]

Economic Sectors

Agriculture

The IoT can be leveraged by the agriculture industry through precision agriculture, with the goal of optimizing production and efficiency while reducing costs and environmental impacts. For farming operations, it involves analysis of detailed, often real-time data on weather, soil and air quality, water supply, pest populations, crop maturity, and other factors such as the cost and availability of equipment and labor.[21] Field sensors test soil moisture and chemical balance,

[18] See, for example, National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things," November 19, 2014, http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf..

[19] Denise Lund et al., "Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand," May 2014; Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020" December 12, 2013, http://www.gartner.com/newsroom/id/2636073; James Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype" (McKinsey Global Institute, June 2015), http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights/Business Technology/Unlocking the potential of the Internet of Things/Unlocking_the_potential_of_the_Internet_of_Things_Full_report.ashx; Verizon, "State of the Market: The Internet of Things 2015," February 20, 2015, http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf.

[20] Anderson and Rainie, "The Internet of Things Will Thrive by 2025."

[21] Jasper Janangir Mohammed, "Surprise: Agriculture Is Doing More with IoT Innovation than Most Other Industries," *VentureBeat*, December 7, 2014, http://venturebeat.com/2014/12/07/surprise-agriculture-is-doing-more-with-iot-innovation-than-most-other-industries/; IBM Research, "Precision Agriculture," 2015, http://www.research.ibm.com/
(continued...)

which can be coupled with location technologies to enable precise irrigation and fertilization.[22] Drones and satellites can be used to take detailed images of fields, giving farmers information about crop yield, nutrient deficiencies, and weed locations.[23] For ranching and animal operations, radio frequency identification (RFID) chips and electronic identification readers (EID) help monitor animal movements, feeding patterns, and breeding capabilities, while maintaining detailed records on individual animals.[24]

Energy

Within the energy sector, the IoT may impact both production and delivery, for example through facilitating monitoring of oil wellheads and pipelines.[25] When IoT components are embedded into parts of the electrical grid, the resulting infrastructure is commonly referred to as the "smart grid."[26] This use of IoT enables greater control by utilities over the flow of electricity and can enhance the efficiency of grid operations.[27] It can also expedite the integration of microgenerators into the grid.[28]

Smart-grid technology can also provide consumers with greater knowledge and control of their energy usage through the use of smart meters in the home or office.[29] Connection of smart meters to a building's HVAC, lighting, and other systems can result in "smart buildings" that integrate the operation of those systems.[30] Smart buildings use sensors and other data to automatically adjust room temperatures, lighting, and overall energy usage, resulting in greater efficiency and lower energy cost.[31] Information from adjacent buildings may be further integrated to provide additional efficiencies in a neighborhood or larger division in a city.

(...continued)

articles/precision_agriculture.shtml.

[22] Agnes Szolnoki and Andras Nabradi, "Economic, Practical Impacts of Precision Farming—With Especial Regard to Harvesting," *Applied Studies in Agribusiness and Commerce* 8, no. 2–3 (2014): 141–46, http://ageconsearch.umn.edu//handle/202892.

[23] Matthew J. Grassi, "Imagery: Which Way Is Right for Me?," *PrecisionAg*, August 6, 2015, http://www.precisionag.com/data/imagery/imagery-which-way-is-right-for-me/.

[24] See, for example, Adrianne Jeffries, "Internet of Cows: Technology Could Help Track Disease, but Ranchers Are Resistant," *The Verge*, May 13, 2013, http://www.theverge.com/2013/5/10/4316658/internet-of-cows-technology-offers-ways-to-track-livestock-but; The State of Victoria, "On-Farm Benefits of Sheep Electronic Identification (EID)," *Agriculture*, 2015, http://agriculture.vic.gov.au/agriculture/farm-management/national-livestock-identification-system/nlis-sheep-and-goats/on-farm-benefits-of-sheep-electronic-identification.

[25] Verizon, "State of the Market: The Internet of Things 2015."

[26] Department of Energy, "The Smart Grid," 2015, http://www.smartgrid.gov/the_smart_grid#smart_grid.

[27] CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[28] Jean Kumagai, "The Rise of the Personal Power Plant," *IEEE Spectrum*, May 28, 2014, http://spectrum.ieee.org/energy/the-smarter-grid/the-rise-of-the-personal-power-plant.

[29] CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by Brandon J. Murrill, Edward C. Liu, and Richard M. Thompson II.

[30] Institute for Building Efficiency, "What Is a Smart Building?," April 2011, http://www.institutebe.com/smart-grid-smart-building/What-is-a-Smart-Building.aspx.

[31] IBM, "Smarter Buildings," 2015, http://www.ibm.com/smarterplanet/us/en/green_buildings/overview/.

Health Care

The IoT has many applications in the health care field,[32] in both health monitoring and treatment, including telemedicine and telehealth.[33] Applications may involve the use of medical technology and the Internet to provide long-distance health care and education.[34] Medical devices—which can be wearable or nonwearable, or even implantable, injectable, or ingestible[35]—can permit remote tracking of a patient's vital signs, chronic conditions, or other indicators of health and wellness.[36] Wireless medical devices may be used not only in hospital settings but also in remote monitoring and care, freeing patients from sustained or recurring hospital visits.[37] Some experts have stated that advances in healthcare IoT applications will be important for providing affordable, quality care to the aging U.S. population.[38]

Manufacturing

Integration of IoT technologies into manufacturing and supply chain logistics is predicted to have a transformative effect on the sector.[39] The biggest impact may be realized in optimization of operations, making manufacturing processes more efficient.[40] Efficiencies can be achieved by connecting components of factories to optimize production, but also by connecting components of inventory and shipping for supply chain optimization.[41] Another application is predictive maintenance, which uses sensors to monitor machinery and factory infrastructure for damage. Resulting data can enable maintenance crews to replace parts before potentially dangerous and/or costly malfunctions occur.[42]

Transportation

Transportation systems are becoming increasingly connected. New motor vehicles are equipped with features such as global positioning systems (GPS) and in-vehicle entertainment, as well as

[32] The use of IoT in medicine is sometimes referred to as "connected" or "digital" health. See, for example, Food and Drug Administration, "Digital Health," September 22, 2015, http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm20035974.htm.

[33] American Telemedicine Association, "What Is Telemedicine?" 2015, http://www.americantelemed.org/about-telemedicine/what-is-telemedicine.

[34] Health Resources and Services Administration, "Telehealth," *Department of Health and Human Services*, 2015, http://www.hrsa.gov/ruralhealth/about/telehealth/telehealth.html.

[35] Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype."

[36] Jerome Couturier et al., "How Can the Internet of Things Help to Overcome Current Healthcare Challenges," *Digiworld Economic Journal*, no. 87 (Q 2012): 67–81, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304133.

[37] See, for example, Food and Drug Administration, "Wireless Medical Devices," September 22, 2015, http://www.fda.gov/MedicalDevices/DigitalHealth/WirelessMedicalDevices/default.htm.

[38] See testimony from Senate Special Committee on Aging, *Roundtable: Harnessing the Power of Telehealth: Promises and Challenges?*, 2014, http://www.aging.senate.gov/hearings/roundtable-harnessing-the-power-of-telehealth-promises-and-challenges; House Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet, *Internet of Things*, 2015, http://judiciary.house.gov/index.cfm/2015/7/hearing-internet-of-things.

[39] Lopez Research, "Building Smarter Manufacturing with the Internet of Things (IoT)," January 2014, http://www.cisco.com/web/solutions/trends/iot/iot_in_manufacturing_january.pdf; James Macaulay, Lauren Buckalew, and Gina Chung, "Internet of Things in Logistics" (DHL Trend Research and Cisco Consulting Services, 2015), http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf.

[40] Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype."

[41] Macaulay, Buckalew, and Chung, "Internet of Things in Logistics."

[42] Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype."

advanced driver assistance systems (ADAS), which utilize sensors in the vehicle to assist the driver, for example with parking and emergency braking.[43] Further connection of vehicle systems enables fully autonomous or self-driving automobiles, which are predicted to be commercialized in the next 5-20 years.[44]

Additionally, IoT technologies can allow vehicles within and across modes—including cars, buses, trains, airplanes, and unmanned aerial vehicles (drones)—to "talk" to one another and to components of the IoT infrastructure, creating intelligent transportation systems (ITS). Potential benefits of ITS may include increased safety and collision avoidance, optimized traffic flows, and energy savings, among others.[45]

Infrastructure and Smart Cities

The capabilities of the smart grid, smart buildings, and ITS combined with IoT components in other public utilities—such as roadways, sewage and water transport and treatment, public transportation, and waste removal—can contribute to more integrated and functional infrastructure, especially in cities.[46] For example, traffic authorities can use cameras and embedded sensors to manage traffic flow and help reduce congestion.[47] IoT components embedded in street lights or other infrastructure elements can provide functions such as advanced lighting control, environmental monitoring, and even assistance for drivers in finding parking spaces.[48] Smart garbage cans can signal waste removal teams when they are full, streamlining the routes that garbage trucks take.[49]

This integration of infrastructure and service components is increasingly referred to as smart cities, or other terms such as connected, digital, or intelligent cities or communities. A number of cities in the United States and elsewhere have developed smart-city initiatives.[50]

---

[43] Intel, "Technology and Computing Requirements for Self-Driving Cars," June 2014, http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/automotive-autonomous-driving-vision-paper.pdf.

[44] James M. Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers* (Santa Monica, CA: Rand Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf.

[45] Intelligent Transportation Systems (ITS) and Joint Program Office (JPO), "ITS 2015-2019 Strategic Plan" (Department of Transportation, February 19, 2015), http://www.its.dot.gov/strategicplan.pdf.

[46] Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype"; Matthew Cuddy et al., "The Smart/Connected City and Its Implications for Connected Transportation" (Department of Transportation, October 14, 2014), http://www.its.dot.gov/itspac/Dec2014/Smart_Connected_City_FINAL_111314.pdf.

[47] Katz, "Why the U.S. Government Should Embrace Smart Cities."

[48] GE Lighting, "GE Announces Programs for Intelligent Cities on Both U.S. Coasts as It Pilots New Connected LED Solution" (Press Release, April 15, 2015), http://pressroom.gelighting.com/news/ge-announces-programs-for-intelligent-cities-on-both-u-s-coasts-as-it-pilots-new-connected-led-solution#.VcuyzfnYjnh.

[49] See Andrea Zanella et al., "Internet of Things for Smart Cities," *IEEE Internet of Things Journal* 1, no. 1 (February 2014): 22–32, doi:10.1109/JIOT.2014.2306328.

[50] See, for example, Brookings Institution, "Getting Smarter About Smart Cities," April 18, 2014, http://www.brookings.edu/~/media/research/files/papers/2014/04/smart-cities/bmpp_smartcities.pdf; City of Scottsdale, "myScottsdale," 2015, http://www.scottsdaleaz.gov/service-request/myScottsdale; City of Dubuque, "DBQ IQ Water Management," 2015, http://www.cityofdubuque.org/1786/DBQ-IQ; Cleantech San Diego, "Smart Cities San Diego," 2015, http://cleantechsandiego.org/smart-city-san-diego/; Boyd Cohen, "The 10 Smartest Cities In North America," *Fast Company*, November 14, 2013, http://www.fastcoexist.com/3021592/the-10-smartest-cities-in-north-america; GE Lighting, "GE Announces Programs for Intelligent Cities"; Smart Cities Council, "Vision," 2015, http://smartcitiescouncil.com/category-vision; Violino, "Smart Cities Are Here Today—and Getting Smarter."

As with IoT and other popular technology terms, there is no established consensus definition or set of criteria for characterizing what a smart city is. Specific characterizations vary widely, but in general they involve the use of IoT and related technologies to improve energy, transportation, governance, and other municipal services for specified goals such as sustainability or improved quality of life.[51] The related technologies include

- *social media* (such as Facebook and Twitter),
- *mobile computing* (such as smartphones and wearable devices),
- *data analytics* (big data—the processing and use of very large data sets; and open data—databases that are publicly accessible), and
- *cloud computing* (the delivery of computing services from a remote location, analogous to the way utilities such as electricity are provided).[52]

Together, these are sometimes called SMAC.[53]

Social and Cultural Impacts

The IoT may create webs of connections that will fundamentally transform the way people and things interact with each other. The emerging cyberspace platform created by the IoT and SMAC has been described as potentially making cities "like 'computers' in open air," where citizens engage with the city "in a real-time and ongoing loop of information."[54]

Some observers have proposed that the growth of IoT will result in a hyperconnected world in which the seamless integration of objects and people will cause the Internet to disappear as a separate phenomenon.[55] In such a world, cyberspace and human space would seem to effectively merge into a single environment, with unpredictable but potentially substantial societal and cultural impacts.

What Is the Current Federal Role?

There is no single federal agency that has overall responsibility for the IoT, just as there is no one agency with overall responsibility for cyberspace. Federal agencies may find the IoT useful in

[51] See, for example, Brookings Institution, "Getting Smarter About Smart Cities"; Hafedh Chourabi et al., "Understanding Smart Cities: An Integrative Framework" (45th Hawaii International Conference on System Sciences, IEEE, 2012), 2289–97, doi:10.1109/HICSS.2012.615; Frost and Sullivan, "Strategic Opportunity Analysis of the Global Smart City Market," August 2013, http://twimgs.com/audiencedevelopment/JC/LANDINGPAGES/GOV/YEAR_2014/020314/4Define.pdf; GSMA and A.T. Kearney, "GSMA Mobile Economy 2013," July 19, 2013, http://www.gsmamobileeconomy.com/GSMA%20Mobile%20Economy%202013.pdf; Smart Cities Council, "Definitions and Overviews," 2015, http://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews.

[52] See CRS Report R42887, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, by Patricia Moloney Figliola and Eric A. Fischer.

[53] See, for example, Evans, "SMAC and the Evolution of IT."

[54] Carlo Ratti of the Massachusetts Institute of Technology, as quoted in Violino, "Smart Cities Are Here Today—and Getting Smarter."

[55] See, for example, Hayley Tsukayama, "What Eric Schmidt Meant When He Said 'the Internet Will Disappear,'" *The Washington Post*, January 23, 2015, https://www.washingtonpost.com/blogs/the-switch/wp/2015/01/23/what-eric-schmidt-meant-when-he-said-the-internet-will-disappear/.

helping them fulfill their missions through a variety of applications such as those discussed in this report and elsewhere.[56] Each agency is responsible under various laws and regulations for the functioning and security of its own IoT, although some technologies, such as drones, may also fall under some aspects of the jurisdiction of other agencies.

Various agencies have regulatory, sector-specific, and other mission-related responsibilities that involve aspects of IoT. For example, entities that use wireless communications for their IoT devices will be subject to allocation rules for the portions of the electromagnetic spectrum that they use.

- The **Federal Communications Commission** (FCC) allocates and assigns spectrum for nonfederal entities.[57]
- In the **Department of Commerce,** the **National Telecommunications and Information Administration** (NTIA) fulfills that function for federal entities,[58] and the **National Institute of Standards and Technology** (NIST) creates standards, develops new technologies, and provides best practices for the Internet and Internet-enabled devices.[59]
- The **Federal Trade Commission** (FTC) regulates and enforces consumer protection policies, including for privacy and security of consumer IoT devices.[60]
- The **Department of Homeland Security** (DHS) is responsible for coordinating security for the 16 critical infrastructure sectors.[61] Many of those sectors use industrial control systems (ICS), which are often connected to the Internet, and the DHS National Cybersecurity and Communications Integration Center (NCCIC) has an ICS Cyber Emergency Response Team (ICS-CERT) to help critical-infrastructure entities address ICS cybersecurity issues.[62]
- The **Food and Drug Administration** (FDA) also has responsibilities with respect to the cybersecurity of Internet-connected medical devices.[63]
- The **Department of Justice** (DOJ) addresses law-enforcement aspects of IoT, including cyberattacks, unlawful exfiltration of data from devices and/or

[56] See, for example, Joseph Bradley et al., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity," White Paper (Cisco, 2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf.

[57] CRS Report RL32589, *The Federal Communications Commission: Current Structure and Its Role in the Changing Telecommunications Landscape*, by Patricia Moloney Figliola; CRS Report R43256, *Spectrum Policy: Provisions in the 2012 Spectrum Act*, by Linda K. Moore.

[58] CRS Report R43866, *The National Telecommunications and Information Administration (NTIA): An Overview of Programs and Funding*, by Linda K. Moore.

[59] See, for example, National Institute of Standards and Technology, "Cyber-Physical Systems."

[60] See, for example, FTC Staff, "Internet of Things: Privacy and Security in a Connected World" (Federal Trade Commission, January 2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[61] For descriptions of these sectors, see The White House, "Critical Infrastructure Security and Resilience" (Presidential Policy Directive 21, February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. The directive also identifies sector-specific agencies for each of the identified sectors.

[62] Department of Homeland Security, "About the National Cybersecurity and Communications Integration Center," April 27, 2015, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

[63] See, for example, Food and Drug Administration, "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication," June 13, 2013, http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

networks, and investigation and prosecution of other computer and intellectual property crimes.[64]

- Relevant activities at the **Department of Energy** (DOE) include those associated with developing high-performance and green buildings, and other energy-related programs, including those related to smart electrical grids.[65]
- The **Department of Transportation** (DOT) has established an Intelligent Transportation Systems Joint Program Office (ITS JPO) to coordinate various programs and activities throughout DOT relating to the development and deployment of connected vehicles and systems, involving all modes of surface transportation.[66] DOT mode-specific agencies also engage in ITS activities.[67] The **Federal Aviation Administration** (FAA) is involved in regulation and other activities relating to unmanned aerial vehicles (UAVs)[68] and commercial systems (UAS).[69]
- The **Department of Defense** was a pioneer in the development of much of the foundational technology for the IoT. Most of its IoT deployment has related to its combat mission, both directly and for logistical and other support.[70]

In addition to the activities described above, several agencies are engaged in research and development (R&D) related to the IoT.

- Like NIST, the **National Science Foundation** (NSF) engages in cyber-physical systems research and other activities that cut across various IoT applications.[71]
- The Networking and Information Technology Research and Development Program (NITRD), under the **Office of Science and Technology Policy** (OSTP) coordinates Federal agency R&D in networking and information technology. The NITRD Cyber Physical Systems Senior Steering Group "coordinates programs, budgets and policy recommendations" for IoT R&D.[72] Other agencies involved

[64] See, for example, Department of Justice, "FY 2015 Budget Request: Cybersecurity," February 28, 2014, http://www.justice.gov/sites/default/files/jmd/legacy/2014/08/18/cyber-security.pdf.

[65] See, for example, CRS Report R40147, *Issues in Green Building and the Federal Response: An Introduction*, by Eric A. Fischer; CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[66] See, for example, Brian Cronin and Kevin Dopart, "Connected Vehicles—Improving Safety, Mobility, and the Environment" (U.S. Department of Transportation, April 9, 2014), http://www.its.dot.gov/presentations/pdf/NASA_Briefingv3.2.pdf; Intelligent Transportation Systems (ITS) and Joint Program Office (JPO), "ITS 2015-2019 Strategic Plan."; CRS Report R42367, *Medicaid and Federal Grant Conditions After NFIB v. Sebelius: Constitutional Issues and Analysis*, by Kenneth R. Thomas.

[67] Intelligent Transportation Systems Joint Program Office, "About ITS," *Department of Transportation*, 2015, http://www.its.dot.gov/its_program/about_its.htm.

[68] CRS Report R42718, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System*, by Bart Elias.

[69] CRS Report R44192, *Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry*, by Bill Canis.

[70] Denise E Zheng and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military" (Center for Strategic and International Studies, September 2015), http://csis.org/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf.

[71] National Science Foundation, "Cyber-Physical Systems (CPS)," 2015, http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286&org=CISE&sel_org=CISE&from=fund; National Science Foundation, "Partnerships for Innovation: Building Innovation Capacity," 2015, http://nsf.gov/funding/pgm_summ.jsp?pims_id=504708.

[72] Subcommittee on Networking and Information Technology Research and Development, Committee on Technology, "Supplement to the President's Budget for Fiscal Year 2015: The Networking and Information Technology Research

(continued...)

in such R&D include the **Food and Drug Administration** (FDA), the **National Aeronautics and Space Administration** (NASA), the **National Institutes of Health** (NIH), the **Department of Veterans Affairs** (VA), and several DOD agencies.

- The **White House** has also announced a smart-cities initiative focusing on the development of a research infrastructure, demonstration projects, and other R&D activities.[73]

What Issues Might Affect the Development and Implementation of the IoT?

The Internet of Things is often lauded for its potentially revolutionary applications. Indeed, IoT devices are today being implemented in many different sectors for a vast array of purposes. However, it is still unclear how IoT will progress due to challenges associated with both technical and policy issues.

Technical Issues

Prominent technical limitations that may affect the growth and use of the IoT include a lack of new Internet addresses under the most widely used protocol, the availability of high-speed and wireless communications, and lack of consensus on technical standards.

Internet Addresses

A potential barrier to the development of IoT is the technical limitations of the version of the Internet Protocol (IP) that is used most widely. IP is the set of rules that computers use to send and receive information via the Internet, including the unique address that each connected device or object must have to communicate. Version 4 (IPv4) is currently in widest use. It can accommodate about four billion addresses, and it is close to saturation, with few new addresses available in many parts of the world.[74]

Some observers predict that Internet traffic will grow faster for IoT objects than any other kind of device over the next five years,[75] with more than 25 billion IoT objects in use by 2020,[76] and

(...continued)

and Development Program," February 2015, https://www.nitrd.gov/pubs/2016supplement/FY2016NITRDSupplement.pdf.

[73] The White House, "Fact Sheet: Administration Announces New 'Smart Cities' Initiative to Help Communities Tackle Local Challenges and Improve City Services" (Press Release, September 14, 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

[74] Iljitsch van Beijnum, "It's Official: North America Out of New IPv4 Addresses," *Ars Technica*, July 2, 2015, http://arstechnica.com/information-technology/2015/07/us-exhausts-new-ipv4-addresses-waitlist-begins/.

[75] Cisco predicts an annual growth rate of 71% for IoT traffic during that period, with mobile devices at about 63% and desktop computers under 10% (Cisco, "The Zettabyte Era—Trends and Analysis," May 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html).

[76] Lund et al., "Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand"; Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020."

perhaps 50 billion devices altogether.[77] IPv4 appears unlikely to meet that growing demand, even with the use of workarounds such as methods for sharing IP addresses.[78]

Version 6 (IPv6) allows for a huge increase in the number IP addresses. With IPv4, the maximum number of unique addresses, 4.2 billion, is not enough to provide even one address for each of the 7.3 billion people on Earth. IPv6, in contrast, will accommodate over 10^{38} addresses—more than a trillion trillion per person.

It is highly likely that to accommodate the anticipated growth in the numbers of Internet-connected objects, IPv6 will have to be implemented broadly. It has been available since 1999 but was not formally launched until 2012.[79] In most countries, fewer than 10% of IP addresses were in IPv6 as of September 2015. Adoption is highest in some European countries and in the United States,[80] where adoption has doubled in the past year to about 20%.[81] Globally, adoption has doubled annually since 2011, to about 7% of addresses in mid-2015.[82] While growth in adoption is expected to continue, it is not yet clear whether the rate of growth will be sufficient to accommodate the expected growth in the IoT. That will depend on a number of factors, including replacement of some older systems and applications that cannot handle IPv6 addresses,[83] resolution of security issues associated with the transition, and availability of sufficient resources for deployment.[84]

Efforts to transition federal systems to IPv6 began more than a decade ago.[85] According to estimates by NIST, adoption for public-facing services has been much greater within the federal government than within industry or academia.[86] However, adoption varies substantially among

[77] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (Cisco Internet Business Solutions Group (IBSG), April 2011), http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. The latter figure also includes computers and mobile devices such as smartphones.

[78] Matt Ford et al., "Address Sharing-Coming to a Network near You," *IETF Journal*, June 2009, http://www.internetsociety.org/articles/address-sharing-coming-network-near-you.

[79] Internet Society, "Ipv6: Making Room for the Next 5 Billion People," March 26, 2014, http://www.internetsociety.org/deploy360/wp-content/uploads/2014/03/gen-ipv6factsheet-201403-en_FA_web.pdf. The launch was essentially an organized attempt to stimulate adoption.

[80] The top five were Belgium (34%), Switzerland (19%), the United States (18%), Germany, and Peru (17% each) (Akamai, "IPv6 Adoption by Country and Network," *State of the Internet*, September 16, 2015, https://www.stateoftheinternet.com/trends-visualizations-ipv6-adoption-ipv4-exhaustion-global-heat-map-network-country-growth-data.html).

[81] Ibid.; Google, "IPv6," September 23, 2015, http://www.google.com/intl/en/ipv6/. Google lists the U.S. adoption rate at 21%.

[82] Google, "IPv6"; Internet Society, "World IPv6 Launch," May 27, 2014, http://www.worldipv6launch.org/infographic/.

[83] IPv6 addresses are four times longer than those in IPv4, and some systems and applications cannot process the longer addresses properly (van Beijnum, "It's Official: North America Out of New IPv4 Addresses").

[84] Sheila Frankel et al., "Guidelines for the Secure Deployment of IPv6," SP 800-119 (National Institute of Standards and Technology, December 2010), http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf; van Beijnum, "It's Official: North America Out of New IPv4 Addresses"; Panayotis A. Yannakogeorgos, "The Rise of IPv6," *Air and Space Power Journal*, April 2015, 103–28, http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2015-Mar-Apr/F-Pano.pdf.

[85] Chief Information Officers Council, "Planning Guide/Roadmap toward IPv6 Adoption Within the U.S. Government," June 2012, https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf; Yannakogeorgos, "The Rise of IPv6."

[86] National Institute of Standards and Technology, "Estimating IPv6 & DNSSEC Deployment Status," September 24, 2015, http://fedv6-deployment.antd.nist.gov/snap-all.html.

agencies, and some data suggest that federal adoption plateaued in 2012.[87] Data were not available for this report on domains that are not public-facing, and it is not clear whether adoption of IPv6 by federal agencies will affect their deployment of IoT applications.

High-Speed Internet

Use and growth of the IoT can also be limited by the availability of access to high-speed Internet and advanced telecommunications services, commonly known as broadband, on which it depends. While many urban and suburban areas have access, that is not the case for many rural areas, for which private-sector providers may not find establishment of the required infrastructure profitable, and government programs may be limited.[88]

Wireless Communications

Many observers believe that issues relating to access to the electromagnetic spectrum[89] will need to be resolved to ensure the functionality and interoperability of IoT devices. Access to spectrum, both licensed and unlicensed, is essential for devices and objects to communicate wirelessly. IoT devices are being developed and deployed for new purposes and industries, and some argue that the current framework for spectrum allocation may not serve these new industries well.[90]

Standards

Currently, there is no single universally recognized set of technical standards for the IoT, especially with respect to communications,[91] or even a commonly accepted definition among the various organizations that have produced IoT standards or related documents.[92] Many observers agree that a common set of standards will be essential for interoperability and scalability of devices and systems.[93] However, others have expressed pessimism that a universal standard is feasible or even desirable, given the diversity of objects that the IoT potentially encompasses.[94] Several different sets of de facto standards have been in development, and some observers do not

[87] Ibid.; Mohana Ravindranath, "Government Outpacing Private Sector in IPv6 Adoption, Official Says," *NextGov: CIO Briefing*, May 18, 2015, http://www.nextgov.com/cio-briefing/2015/05/government-could-be-outpacing-private-sector-ipv6-adoption/113056/.

[88] For more information, see CRS Report R44080, *Municipal Broadband: Background and Policy Debate*, by Lennard G. Kruger and Angele A. Gilroy, and CRS Report RL30719, *Broadband Internet Access and the Digital Divide: Federal Assistance Programs*, by Lennard G. Kruger and Angele A. Gilroy.

[89] Electromagnetic spectrum, commonly referred to as radio frequency spectrum or wireless spectrum, refers to electromagnetic waves that, with applied technology, can transmit signals to deliver voice, text, and video communications.

[90] For more information, see CRS Report R43256, *Spectrum Policy: Provisions in the 2012 Spectrum Act*, by Linda K. Moore.

[91] Colin Neagle, "A Guide to the Confusing Internet of Things Standards World," *Network World*, July 21, 2014, http://www.networkworld.com/article/2456421/internet-of-things/a-guide-to-the-confusing-internet-of-things-standards-world.html.

[92] Minerva, Biru, and Rotondi, "Towards a Definition of the Internet of Things (IoT)."

[93] See, for example, World Economic Forum, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services."

[94] Christopher Null, "The State of IoT Standards: Stand by for the Big Shakeout," *TechBeacon*, September 2, 2015, http://techbeacon.com/state-iot-standards-stand-big-shakeout.

expect formal standards to appear before 2017. Whether conflicts between standards will affect growth of the sector as it did for some other technologies is not clear.[95]

Other Technical Issues

Several other technical issues might impact the development and adoption of IoT. For example, if an object's software cannot be readily updated in a secure manner, that could affect both function and security. Some observers have therefore recommended that smart objects have remote updating capabilities.[96] However, such capabilities could have undesirable effects such as increasing power requirements of IoT objects or requiring additional security features to counter the risk of exploitation by hackers of the update features.

Energy consumption can also be an issue. IoT objects need energy for sensing, processing, and communicating information. If objects isolated from the electric grid must rely on batteries, replacement can be a problem, even if energy consumption is highly efficient. That is especially the case for applications using large numbers of objects or placements that are difficult to access. Therefore, alternative approaches such as energy harvesting, whether from solar or other sources, are being developed.[97]

Cybersecurity

The security of devices and the data they acquire, process, and transmit is often cited as a top concern in cyberspace.[98] Cyberattacks can result in theft of data and sometimes even physical destruction. Some sources estimate losses from cyberattacks in general to be very large—in the hundreds of billions or even trillions of dollars.[99] As the number of connected objects in the IoT grows, so will the potential risk of successful intrusions and increases in costs from those incidents.

Cybersecurity involves protecting information systems, their components and contents, and the networks that connect them from intrusions or attacks involving theft, disruption, damage, or other unauthorized or wrongful actions.[100] IoT objects are potentially vulnerable targets for hackers.[101] Economic and other factors may reduce the degree to which such objects are designed with adequate cybersecurity capabilities built in. IoT devices are small, are often built to be disposable, and may have limited capacity for software updates to address vulnerabilities that come to light after deployment.

---

[95] Lawson, "Why Internet of Things 'Standards' Got More Confusing in 2014," *PC World*, December 24, 2014, http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html.

[96] See, for example, Roger Ordman, "Efficient Over-the-Air Software and Firmware Updates for the Internet of Things," *Embedded Computing Design*, April 10, 2014, http://embedded-computing.com/articles/efficient-software-firmware-updates-the-internet-things/.

[97] Keita Sekine, "Energy-Harvesting Devices Replace Batteries in IoT Sensors," *Core & Code*, Q3 2014, http://core.spansion.com/article/energy-harvesting-devices-replace-batteries-in-iot-sensors/.

[98] See, for example, National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things."

[99] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime" (McAfee, June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf?cid=BHP028; World Economic Forum, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services."

[100] CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer.

[101] Scott R. Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security & Consent," *Texas Law Review, Forthcoming*, March 1, 2014, http://papers.ssrn.com/abstract=2409074.

The interconnectivity of IoT devices may also provide entry points through which hackers can access other parts of a network. For example, a hacker might gain access first to a building thermostat, and subsequently to security cameras or computers connected to the same network, permitting access to and exfiltration or modification of surveillance footage or other information.[102] Control of a set of smart objects could permit hackers to use their computing power in malicious networks called botnets to perform various kinds of cyberattacks.[103]

Access could also be used for destruction, such as by modifying the operation of industrial control systems, as with the Stuxnet malware that caused centrifuges to self-destruct at Iranian nuclear plants.[104] Among other things, Stuxnet showed that smart objects can be hacked even if they are not connected to the Internet. The growth of smart weapons and other connected objects within DOD has led to growing concerns about their vulnerabilities to cyberattack and increasing attempts to prevent and mitigate such attacks, including improved design of IoT objects.[105] Cybersecurity for the IoT may be complicated by factors such as the complexity of networks and the need to automate many functions that can affect security, such as authentication. Consequently, new approaches to security may be needed for the IoT.[106]

IoT cybersecurity will also likely vary among economic sectors and subsectors, given their different characteristics and requirements. Each sector will have a role in developing cybersecurity best practices, unique to its needs. The federal government has a role in securing federal information systems, as well as assisting with security of nonfederal systems, especially critical infrastructure.[107] Cybersecurity legislation considered in the 114th Congress, while not focusing specifically on the IoT, would address several issues that are potentially relevant to IoT applications, such as information sharing and notification of data breaches.[108]

Safety

Given that smart objects can be used both to monitor conditions and to control machinery, the IoT has broad implications for safety, with respect to both improvements and risks. For example,

[102] Government Accountability Office, "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems," December 12, 2014, http://www.gao.gov/products/GAO-15-6..

[103] See, for example, Eduard Kovacs, "'Spike' DDoS Toolkit Targets PCs, Servers, IoT Devices: Akamai," *Security Week*, September 25, 2014, http://www.securityweek.com/spike-ddos-toolkit-targets-pcs-servers-iot-devices-akamai.

[104] CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[105] Sydney J. Freedberg, Jr., "Cybersecurity Now Key Requirement for All Weapons: DoD Cyber Chief," *Breaking Defense*, January 27, 2015, http://breakingdefense.com/2015/01/cybersecurity-now-key-requirement-for-all-weapons-dod-cio/; Patrick Tucker, "For Years, the Pentagon Hooked Everything to the Internet. Now It's a 'Big, Big Problem,'" *Defense One*, September 29, 2015, http://www.defenseone.com/technology/2015/09/years-pentagon-hooked-everything-internet-now-its-big-big-problem/122402/.

[106] Benjamin Jun, "Make Way for the Internet of Things!" (RSA Conference 2014, San Francisco, CA, February 27, 2014), http://www.rsaconference.com/writable/presentations/file_upload/tech-r02-internet-of-things-v2.pdf; Benjamin Jun, "Endpoints in the New Age: Apps, Mobility, and the Internet of Things" (RSA Conference 2015, San Francisco, CA, April 21, 2015), https://www.rsaconference.com/writable/presentations/file_upload/eco-t07r-endpoints-in-the-new-age-apps-mobility-and-the-internet-of-things.pdf.

[107] Critical infrastructure was defined by the USA PATRIOT Act as "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters" (5 U.S.C. §5195c(e)).

[108] For more discussion of congressional and executive-branch actions in cybersecurity, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer, and related reports.

objects embedded in pipelines can monitor both the condition of the equipment and the flow of contents. Among other benefits, that can help both to expedite shutoffs in the event of leaks and to prevent them through predictive maintenance.[109] Connected vehicles can help reduce vehicle collisions through crash avoidance technologies and other applications.[110] Wireless medical devices can improve patient safety by permitting remote monitoring and facilitating adjustments in care.[111]

However, given the complexities involved in some applications of IoT, malfunctions might in some instances result in catastrophic system failures, creating significant safety risks, such as flooding from dams or levees.[112] In addition, hackers could potentially cause malfunctions of devices such as insulin pumps[113] or automobiles,[114] potentially creating significant safety risks.

Privacy

Cyberattacks may also compromise privacy, resulting in access to and exfiltration of identifying or other sensitive information about an individual. For example, an intrusion into a wearable device might permit exfiltration of information about the location, activities, or even the health of the wearer.

In addition to the question of whether security measures are adequate to prevent such intrusions, privacy concerns also include questions about the ownership, processing, and use of such data. With an increasing number of IoT objects being deployed, large amounts of information about individuals and organizations may be created and stored by both private entities and governments.

With respect to government data collection, the U.S. Supreme Court has been reticent about making broad pronouncements concerning society's expectations of privacy under the Fourth Amendment of the Constitution while new technologies are in flux, as reflected in opinions over the last five years.[115] Congress may also update certain laws, such as the Electronic Communications Privacy Act of 1986, given the ways that privacy expectations of the public are evolving in response to IoT and other new technologies.[116] IoT applications may also create

[109] Adam Lesser, "Internet of Things: The Influence of M2M Data on the Energy Industry" (GigaOm Research, March 4, 2014), http://research.gigaom.com/report/internet-of-things-the-influence-of-m2m-data-on-the-energy-industry/.

[110] Cronin and Dopart, "Connected Vehicles—Improving Safety, Mobility, and the Environment."

[111] Couturier et al., "How Can the Internet of Things Help to Overcome Current Healthcare Challenges."

[112] AIG, "The Internet of Things: Evolution or Revolution?," June 10, 2015, https://www.aig.com/Chartis/internet/US/en/AIG%20White%20Paper%20-%20IoT%20English%20DIGITAL_tcm3171-677828.pdf.

[113] FTC Staff, "Internet of Things: Privacy and Security in a Connected World."

[114] Ian Foster et al., "Fast and Vulnerable: A Story of Telematic Failures," in *Proceedings of the 9th USENIX Conference on Offensive Technologies* (USENIX Association, 2015), 15–15, https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf; Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," accessed October 6, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[115] In the 2010 case *City of Ontario v. Quon*, the Court sidestepped the question whether individuals have a reasonable expectation of privacy in their electronic communications by resolving the case on other grounds (City of Ontario v. Quon, 560 U.S. 746 (2010) ["The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."]). Similarly, in the 2012 GPS tracking case *United States v. Jones*, the majority avoided the question of whether people should expect privacy in their public movements over a long period of time by instead relying on a hundreds-year-old trespass theory of the Fourth Amendment (United States v. Jones, 132 S. Ct. 945, 954 [2012]). More recently, in the 2015 case *California v.Riley*, the Court held that the government must obtain a warrant before accessing the data on a cellphone confiscated upon an arrest; however, the ruling did not separately opine on the level of protections for data stored in the cloud, on which IoT applications will undoubtedly rely (California v. Riley, 134 S. Ct. 2473, 2495 [2015]).

[116] See, CRS Report R44036, *Stored Communications Act: Reform of the Electronic Communications Privacy Act* (continued...)

challenges for interpretation of other laws relating to privacy, such as the Health Insurance Portability and Accountability Act and various state laws, as well as established practices such as those arising from norms such as the Fair Information Practice Principles.[117]

Other Policy Issues

Federal Role

As described in the section, "What Is the Current Federal Role?" many federal agencies are involved in different aspects of the IoT. Some business representatives and others have stressed the role of effective public/private partnerships in the development of this technology space.[118] However, observers have also expressed concerns about the role of government regulations and policy, as discussed further in sections below, and about the degree and effectiveness of coordination among the involved federal agencies.[119] Concerns of some extend beyond the federal role to that of state, local, and foreign governments.[120]

Given the eclectic nature of the IoT, overall coordination of federal efforts may be challenging with respect to identification of both the goals of coordination and the methods for achieving them. Nevertheless, several observers have argued in favor of a national strategy for the IoT,[121] including in resolutions considered in the 114th Congress (see "What Actions Has Congress Taken?").

Some interagency initiatives have been established with respect to specific aspects of the IoT. For example, in addition to the R&D coordination activities for cyber-physical systems under the NITRD program,[122] a specific framework has been developed for smart cities[123] as part of the overall White House initiative involving several federal agencies, local governments, and the private sector.[124]

(...continued)

(ECPA), by Richard M. Thompson II and Jared P. Cole.

[117] FTC Staff, "Internet of Things: Privacy and Security in a Connected World"; Thierer, "The Internet of Things and Wearable Technology."

[118] See, for example, Brookings Institution, "Getting Smarter About Smart Cities"; House Committee on Energy and Commerce, *The Internet of Things: Exploring the Next Technology Frontier*, 2015, http://energycommerce.house.gov/hearing/internet-things-exploring-next-technology-frontier; House Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet, *Internet of Things*.

[119] See, for example, Gary Arlen, "Internet of Things Caucus Readies House Hearings," *Multichannel News*, July 8, 2015, http://www.multichannel.com/blog/i-was-saying/internet-things-caucus-readies-house-hearings/392024; Darren Samuelson, "The Agenda—Internet of Things," July 2015, http://www.politico.com/agenda/issue/internet-of-things-july-2015.

[120] See, for example, Helen Rebecca Schindler et al., "Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things" (RAND Europe, July 26, 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf; Thierer, "The Internet of Things and Wearable Technology."

[121] See, for example, Samuelson, "The Agenda—Internet of Things."

[122] See "What Is the Current Federal Role?" above.

[123] Subcommittee on Networking and Information Technology Research and Development, Committee on Technology, "Smart Cities and Connected Communities Framework," September 11, 2015, https://www.nitrd.gov/sccc/.

[124] The White House, "Fact Sheet: Administration Announces New 'Smart Cities' Initiative."

Spectrum Access

Radio frequency (electromagnetic) spectrum is widely regarded as a critical link in IoT communications, with reliable and affordable access to it required to accommodate the billions of new IoT devices projected to go online over the next decade.[125] New technology for mobile communications is predicted to allow devices to operate on any available radio frequency and potentially permit communications technologies and cyber-physical systems to converge further.[126] Concerns have been raised that current spectrum policy may favor consumer-oriented mobile services and the wireless industry, rather than emerging markets for IoT devices, such as transportation and manufacturing.[127] Congress may therefore be faced with decisions about whether the current policy needs to be revised.

Net Neutrality

The concept of "net neutrality" includes the two general principles that owners of the networks that comprise and provide access to the Internet should not control how end users lawfully use that network, and that they should not be able to discriminate against content provider access to that network.[128] The FCC adopted an order in February 2015 that established regulatory guidelines to protect the marketplace from potential abuses that could threaten the net neutrality concept.[129] The order bans broadband Internet access providers (both fixed and wireless) from blocking and throttling lawful content, and it prohibits paid prioritization of affiliated or proprietary content.[130] The order also creates a general conduct standard that Internet service providers cannot harm consumers or providers of applications, content, and services. These rules went into effect, with limited exceptions, on June 12, 2015, but have been challenged in the U.S. Court of Appeals for the D.C. Circuit.[131]

It remains unclear how the FCC order will affect IoT devices and services. Some observers view the implementation of FCC regulations as a positive development. They believe that it will ensure openness and nondiscrimination for service providers, leading to the growth of new services and consumer demand. Others have expressed concerns that the regulations will stifle investment and innovation to the detriment of the expansion and growth of Internet deployment and services. Furthermore, the rules are subject to "reasonable network management," as defined by the FCC, and a category of "specialized services" defined as those that "do not provide access to the Internet generally" are exempt from the rules established by the order.[132] Depending on how individual IoT services and devices are categorized and the degree of network management such

[125] CRS Report R43256, *Spectrum Policy: Provisions in the 2012 Spectrum Act*, by Linda K. Moore.

[126] CRS Insight IN10191, *What Is 5G? Implications for Spectrum and Technology Policy*, by Linda K. Moore.

[127] CRS Insight IN10221, *The Robot Did It: Spectrum Policy and the Internet of Things*, by Linda K. Moore.

[128] For additional information on the net neutrality issue see CRS Report R40616, *Access to Broadband Networks: The Net Neutrality Debate*, by Angele A. Gilroy, and CRS Report R43971, *Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order*, by Kathleen Ann Ruane.

[129] Federal Communications Commission, "Protecting and Promoting the Open Internet; Final Rule," *Federal Register* 80, no. 70 (April 13, 2015): 19738–850, http://www.gpo.gov/fdsys/pkg/FR-2015-04-13/pdf/2015-07841.pdf.

[130] Paid prioritization occurs when a broadband Internet access provider accepts payment (monetary or otherwise) to manage its network in a way that benefits particular content, applications, devices, or services.

[131] The challenges were consolidated under U.S. Telecom Association v. FCC, D.C. Cir. No. 15-1063, April 14, 2015.

[132] The FCC order cited heart monitors and energy consumption sensors as examples of "specialized services." See Federal Communications Commission, "Protecting and Promoting the Open Internet; Final Rule" para. 35.

specialized services may need, the order could also affect IoT applications on a case-by-case basis.

What Actions Has Congress Taken?

Legislation

Bills

No bills have been introduced in the last two Congresses relating specifically to the IoT. However, many bills have been introduced with provisions related to aspects of the IoT such as connected vehicles, cyber-physical systems, smart cities, and the smart grid. None of those bills were enacted as of September 2015, although some bills with provisions on applications and appropriations relating to telehealth and telemedicine were enacted in both the 113th and 114th Congresses. Several bills in the 114th Congress would address issues that are potentially relevant to IoT applications, such as information sharing in cybersecurity, privacy, and notification of data breaches.[133]

Resolutions

Two similar resolutions on the IoT have been submitted in the 114th Congress, one in the House (H.Res. 195/Lance, introduced April 13, 2015) and one in the Senate (S.Res. 110/Fischer, introduced and passed March 24). Both call for

- a U.S. strategy for development of the IoT to improve social well-being while allowing for innovation and protecting against misuse,
- recognition of the importance of a consensus-based approach and the role of businesses in that development,
- federal government commitment to use the IoT, and
- a U.S. commitment to use the IoT for developing new technologies to address challenging societal issues.

The House version also calls for the use of cost-benefit analysis to determine when federal action is needed to address "discrete harms" in the marketplace. It also refers explicitly to energy optimization and the need for cybersecurity.

Hearings

Both the House and the Senate have held hearings on the IoT in 2015. In the Senate, the Committee on Commerce, Science, and Transportation held a hearing on February 11.[134] In the House, one was held by the Energy and Commerce Committee on March 24,[135] and another by the Subcommittee on Courts, Intellectual Property, and the Internet of the Committee on the

[133] For more information, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer, and related reports.

[134] Senate Committee on Commerce, Science, and Transportation, *The Connected World: Examining the Internet of Things*, 2015, http://www.commerce.senate.gov/public/index.cfm/hearings?ID=d3e33bde-30fd-4899-b30d-906b47e117ca.

[135] House Committee on Energy and Commerce, *The Internet of Things: Exploring the Next Technology Frontier*.

Judiciary on July 29.[136] The hearings featured witnesses from businesses and associations who discussed the growth, uses, and economic potential of the IoT, as well as some of the issues described in this report, such as privacy, regulation, security, spectrum management, and standards.

Caucuses

There are several congressional caucuses that may consider issues associated with the IoT. Among them are caucuses on cloud computing,[137] cybersecurity,[138] the Internet,[139] and high-performance buildings. In addition, new caucuses announced in this session included one expressly on the Internet of Things,[140] and one on smart transportation.[141]

Where Can I Find Additional Resources on This Topic?

For additional assistance on the IoT and related topics, see CRS Report R44225, The Internet of Things: CRS Experts, by Eric A. Fischer and Glenn J. McLoughlin. Congressional offices may also contact CRS by placing a request via telephone or online through the CRS website (see http://www.crs.gov/AboutCRS/Contact-Us).

Author Contact Information

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071

Acknowledgments

This report was originally coauthored by Stephanie M. Logan while she was a CRS research assistant. Stephanie performed most of the research and provided much of the organizational structure and text for the report. Her insights and other contributions were invaluable.

[136] House Committee on the Judiciary, Subcommittee on Courts, *Intellectual Property, and the Internet, Internet of Things*.

[137] Cloud Computing Caucus Advisory Group, "Home," 2015, https://www.cloudcomputingcaucus.org/.

[138] Congressional Cybersecurity Caucus, "Welcome," 2015, http://cybercaucus.langevin.house.gov/.

[139] Congressional Internet Caucus Advisory Committee, "NetCaucus," 2015, http://www.netcaucus.org/.

[140] The Honorable Suzan DelBene, "U.S. Reps. DelBene and Issa Announce Creation of the Congressional Internet of Things Caucus" (Press Release, January 13, 2015), https://delbene.house.gov/media-center/press-releases/us-reps-delbene-and-issa-announce-creation-of-the-congressional-internet.

[141] Senator Gary Peters, "Peters, Gardner Announce New Bipartisan Smart Transportation Caucus" (press release, June 10, 2015), http://www.peters.senate.gov/newsroom/press-releases/peters-gardner-announce-new-bipartisan-smart-transportation-caucus.

The following CRS staff contributed to sections of this report: Angele A. Gilroy to "Net Neutrality," Linda K. Moore to "Spectrum Access," Megan Stubbs to "Agriculture," and Richard M. Thompson II and Jared P. Cole to "Privacy."