



What Is the Internet of Things?

ITIF Technology Explainer Series • www.itif.org

The Internet of Things (IoT) describes the set of physical objects that can automatically collect a wide array of information about people, nature, the built environment, machines, and products and transmit this information over a network. Before the Internet of Things, much of this data either could not be collected, had to be collected manually (such as by inspectors examining faults in bridges), or was collected automatically—but only at great expense via specialized telecommunications links (as in the case of advanced weather stations, for example). Now, with the Internet of Things, it is possible to create intelligent systems that continuously collect vast arrays of data and transmit it over the Internet to be monitored and analyzed.

As the cost of deploying smart devices declines, homes, factories, farms, office buildings, and even entire cities are increasingly generating vast quantities of actionable data this way. The Internet of Things produces myriad economic and social benefits, with applications as diverse as sensor-equipped bridges that can alert authorities when there is a risk of structural failure and devices in waterways that can warn environmental regulators about spikes of fatally toxic algae. Wearable medical devices allow individuals to monitor and address health conditions, and the use of IoT devices in industrial settings is powering smart factories and smart supply chains. These transformations will be significant, but often inconspicuous, because the changes to the physical environment are minimal: a sensor-enabled “smart” building looks much the same as a “dumb” one, but it functions much better.

Why Now?

This revolution has been powered by a combination of technologies that all have been improving rapidly, including low-cost sensors capable of monitoring a wide array of phenomena, low-power processors, scalable cloud computing, and ubiquitous wireless connectivity. In particular, the cost of micro-electromechanical systems (MEMS), which are fundamental to everything from fitness trackers to smartphones, plummeted between 30 and 70 percent from 2010 to 2015. Sensor prices themselves also have fallen significantly, from an average of \$1.30 in 2004 to \$0.70 in 2014.

The Internet of Things has a wide variety of potential applications thanks to better and cheaper sensors that can record everything from temperature and light to sound, humidity, chemical composition, pressure, and other factors. It is now increasingly feasible, both technologically and from a cost-effectiveness standpoint, to embed these sensors in ordinary objects and connect them to the Internet, making them smart devices.

Prospects for Continued Progress

The Internet of Things is still in its early stages of development and deployment, but it is advancing and growing rapidly. Further advancements in the technology will likely continue as sensors keep getting less expensive and more energy efficient. The shift to 5G mobile networks will accelerate IoT progress, particularly for applications where it would be difficult to connect sensors via Wi-Fi networks, such as in transportation, agriculture, and infrastructure. Many of the prospects for advancement relate to the network effects that will arise as more and more individuals and organizations adopt the technologies. For many applications, the benefits expand as the number of connected devices grows, because they generate data that, when aggregated and analyzed, leads to more actionable insights.

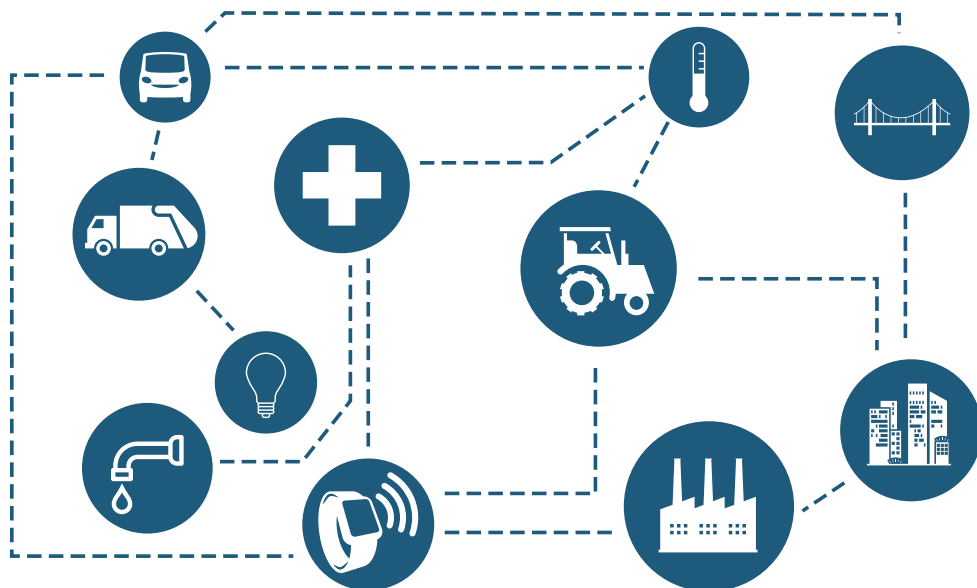
In the past, most Internet users have been people—individuals sending email, reading the news, shopping online, and the like. But by 2020 there will be tens of billions of connected devices in use worldwide, outnumbering human users by an order of magnitude.

Applications and Impact

Though use of the Internet of Things is still growing, it is already widely used. For example, cities are increasingly integrating connected sensors into infrastructure to generate data that allows them to tackle key challenges, such as traffic congestion, crime, and pollution. Governments are also using networked sensors to perform large-scale environmental monitoring to improve public health and predict natural disasters.

In the private sector, connected sensors allow manufacturers to monitor factory operations in detail not just to improve efficiency and productivity, but to perform predictive maintenance, increase safety, and improve quality control. Buildings equipped with temperature sensors can dynamically control heating and cooling, lowering costs. Farms with soil moisture sensors can reduce water use while increasing harvests. Supply chains can use sensors in shipping containers to reduce spoilage, better track cargo, and reduce theft. These are just a few ways the Internet of Things is making ordinary objects and routine processes “smart.” Companies are also deploying a wide variety of consumer-facing IoT applications, ranging from smart devices that allow users to improve household energy efficiency to biometric monitoring devices that allow people to better manage chronic diseases and improve their overall health, to connected cars that improve road safety and predict when they are in need of maintenance before they break down. All of this and more is expected to enable the Internet of Things to contribute an additional \$11 trillion in value to the global economy by 2025.

Consumer devices, infrastructure, vehicles, factories, healthcare technology, and even entire cities can collect and transmit data as part of the Internet of Things.



Policy Implications

To support the growth of the Internet of Things, governments should develop national strategies to address a number of market failures, such as chicken-and-egg dynamics that make the success of some IoT applications depend on the success of other technologies. For example, the value proposition for connected vehicles is higher if vehicles can communicate with infrastructure such as parking meters and traffic signals. If left unaddressed, these market failures will slow the technology's progress.

Having government as a lead adopter will help spur IoT innovation and lower costs. There are many opportunities to deploy the Internet of Things that are strongly tied to public sector priorities, such as public health, environmental stewardship, transportation, defense, and city management. For example, accelerating the adoption of smart city technology should be a key priority for governments. It has been slower than it should be in part because individual cities are reluctant to be early adopters of untested IoT technology applications. Moreover, cities could benefit immensely from developing interoperable systems and sharing data with one another, but currently they lack the capacity to coordinate this across jurisdictional boundaries. National governments have important temporary roles to fill in helping overcome these challenges, including allocating a share of infrastructure investments to specifically target smart infrastructure, funding programs to pilot particularly promising applications, and supporting comprehensive smart city applications that deploy sensors and apply analytics to entire verticals of city management, such as water and sewers, rather than just one-off applications.

Congress also can address cybersecurity concerns for consumer-facing IoT applications by requiring device manufacturers to publish security policies just as they publish privacy policies. Currently, it is not easy to differentiate between secure and insecure products, and

as a result there are weak market signals to reward companies for investing in cybersecurity or to help more secure products to gain market share. If companies were all required to publish their security policies, then they would suddenly have a competitive interest in describing the types of security measures they have in place with greater specificity than vaguely claiming "we take security seriously." And the federal government can help spur the deployment of 5G networks, in part by ensuring that local governments do not hold up the deployment process. Overall, developing a national strategy can ensure a country is positioned to take full advantage of the Internet of Things.

Recommended Reading

Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, <http://www2.datainnovation.org/2015-national-iot-strategies.pdf>.

Joshua New, Daniel Castro, and Matt Beckwith, "How National Governments Can Help Smart Cities Succeed," Center for Data Innovation, October 30, 2017, <http://www2.datainnovation.org/2017-national-governments-smart-cities.pdf>.

Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2014, <http://www2.datainnovation.org/2014-iot-policy-principles.pdf>.

Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data Innovation, November 2013, <http://www2.datainnovation.org/2013-internet-of-things.pdf>.

Daniel Castro, "How Congress Can Fix 'Internet of Things' Security," The Hill, October 28, 2016, <http://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security>.