The Internet of Things and the explosion of interconnectivity

Stephen Ornes, *Science Writer*

It was 1982, and a group of computer science graduate students at Carnegie Mellon University in Pittsburgh, Pennsylvania, was thirsty for more than knowledge: some wanted a Coca Cola. But the researchers were frustrated. The Coke machine was on the third floor of the university's Wean Hall, and oftentimes they'd venture up to the dispenser only to find it empty, or worse, full of warm soda. So the scientists connected the machine to the university's computer network. By checking online, thirsty researchers could ensure the machine was stocked with cold bottles before visiting. This turned out to be more than an achievement in efficient caffeine delivery; it's thought to be one of the first noncomputer objects to go online (1).

The notion of pervasive computing entails a vision of the world in which computing isn't limited to tablets, smartphones, and laptops. The realization of this vision, called the "Internet of Things" (IoT), is the ever-expanding collection of connected devices that capture and share data. Any object, outfitted with the right sensors, can observe and interact with its environment. A homeowner can adjust the thermostat, close the blinds, or raise a garage door with a voice command to a smartphone app. A connected refrigerator can send a list of its inventory to a shopper. A soccer ball can analyze a kicker's technique and suggest ways to improve her game. Smart tags on a cow alert a farmer when the animal spikes a fever or goes into labor.

Perhaps the greatest potential benefits of the IoT lie in health care. Sensors in a smart floor might detect when an elderly person falls and call an ambulance (2). Mobile devices that continuously monitor a person's vital signs could pick up the first signs of illness or eliminate the need for repeated medical testing. Smart tags on medicine could reduce the problem of counterfeit pharmaceuticals and help patients follow prescribed dosage schedules. [Medical applications will likely be lucrative, as well: in 2015, MindCommerce.com estimated that the IoT healthcare market would reach $117 billion by 2020 (3).]

The potential benefit of the IoT is a smarter, more efficient, and safer world; the potential pitfalls include compromised personal security, a lack of appropriate power sources, and data overload.

Decades in the Making

Like many new ideas in technology, the IoT percolated for decades before becoming a reality. In 1950, British computer scientist Alan Turing proposed building machines that could sense and learn from their surroundings.

Pervasive computing and its realization, known as the "Internet of Things," entails an ever-expanding collection of connected devices that capture and share data. Image courtesy of Shutterstock/a-image.

In 1966, Karl Steinbuch, in Germany, described a future where computers were stitched into just about anything.

In a prescient *Scientific American* article published in 1991, Mark Weiser, a computer scientist with the Xerox PARC information technology company, described the kinds of devices that would enable "ubiquitous" computing in the fabric of everyday life (4). "No revolution in artificial intelligence is needed," Weiser wrote, "just the proper imbedding of computers into the everyday world" (4). Weiser also pioneered smart boards and tablet computers. British technology entrepreneur Kevin Ashton, who helped popularize the use of RFID (radio frequency identification) tags for the wireless tracking of objects, was likely the first person to use the phrase "Internet of Things" in 1999; in 2013, the term appeared in the Oxford English Dictionary (5).

In recent years, smart things have hit the shelves, and there's already ample growth. In a 2011 report, the technology company Cisco estimated that the number of online devices surpassed the world population some time in 2008 (6). Last August, Gartner, an information technology research company, estimated that more than 5 million devices go online every day in 2016 (7). The same company predicted that 20 billion devices—many of them as wired objects—will be online by 2020; Cisco predicts a number closer to 50 billion (6).

www.pnas.org/cgi/doi/10.1073/pnas.1613921113

"The Internet of Things. . . is finally starting to come to fruition in people's homes," a trio of computer scientists wrote in an editorial as part of the May–June 2016 issue of *IEEE Pervasive Computing* (8).

Power Struggle

Connected objects have two components in common: a sensor to collect data and a way to communicate that data. Jason Hong, a computer scientist at Carnegie Mellon University and one of the authors of the *Pervasive Computing* editorial (8), says the IoT has grown quickly, in part because its underlying technologies have matured and become less expensive in recent years.

"The sensing, the computing, the wireless networking, battery life, smartphones—the convergence of all these technologies has enabled the [internet of things] to happen," he says. Hong describes the IoT as a revolution in technology, but notes that it raises multiple difficult, thorny issues.

One challenge is the volume of data generated by the tens of billions of devices that will be online in the next five years or so. Maria Ebling, a computer scientist at IBM's Watson Research Center in New York, says researchers are still figuring out how to manage, store, and use all that data. "To make sense of it, we have to be able to apply analytics and machine learning."

Power is another issue. Connected devices require constant current. "If you want all these sensors in a smart building that can open and close windows and doors, they require a lot of sensors and actuators, and those require power," says Ebling. At the same time, recharging wireless devices and replacing batteries are human-intensive activities, which means the time people save with the devices may be lost in maintaining the power source. "Battery technology is not improving at the rate at which computer technology is improving."

The increased demand for power is pushing engineers to develop new ways of harvesting energy from the sun or other sources. In a recent issue of *Science*, colleagues of Ebling's from the Watson Research Center report on a simple study, suggesting that current lithium-ion batteries, although providing a steady current, will be insufficient to power small, smart, connected devices for more than a few days at a time (9). The authors suggest a solution: merging thin-film photovoltaic devices with batteries that can store power for future use.

Too Many Windows?

Security is another key concern in a world with an extensive IoT. If a person's personal data are represented as a house, then each connected device acts like a window, offering hackers a way inside. That threat will increase as more devices come online. Individuals and companies that build smart, connected things don't prioritize security, says Jonathan Margulies, a security consultant who heads up a company called Evil Associates in New Jersey. "They're rushing to get something to market," he says. In addition, "there are no good internet of things security standards right now."

Consider the case of Samsung's SmartThing system, which offers consumers a large array of connected smart devices—from self-dimming light bulbs to security motion detectors—that can be controlled from a phone. Software developers can build custom apps for the system, which offer customers more ways to control aspects of their home and devices.

But that control comes with a cost. Researchers from the University of Michigan recently analyzed security flaws in the Smart Things system and carried out a number of mock attacks, including eavesdropping on a user as they set the PIN for their front door lock. The researchers reported their findings in May 2016 at the IEEE Symposium on Security and Privacy in San Jose, California (10).

Michigan graduate student Earlence Fernandes, who led the study, says the way apps are written makes it easy for hackers to obtain sensitive data. When people download and use these apps, they expose themselves to unknown third-party developers.

"Widespread security is a barrier to the adoption of the internet of things," says Fernandes, whose research focuses on both finding attacks and solutions. Since his report on Smart Things, Fernandes says he's met with Samsung to discuss the technology's vulnerabilities.

Hong says trade groups are working on guidelines to make connected devices safer for consumers, but security still varies from object to object in the IoT. "There's a double-edged sword in all this data and sensing," says Hong. "There are a lot of benefits for education, society, and other kinds of things, but they can also be used in ways you may not like."

1 https://www.cs.cmu.edu/~coke/history_long.txt.
2 Feng G, et al. (2016) Floor pressure imaging for fall detection with fiber-optic sensors. *IEEE Pervasive Comput* 15(2):40–47.
3 MarketResearch.com (2015) Big Data in Internet of Things (IoT): Key Trends, Opportunities and Market Forecasts 2015 – 2020. SKU: CCJQ5530605, Mind Commerce, Portland, OR. Press release available at http://www.prnewswire.com/news-releases/marketresearchcom-iot-deployments-in-healthcare-to-reach-117-billion-by-2020-says-new-mind-commerce-report-300070129.html and report available at http://www.bigmarketresearch.com/big-data-in-internet-of-things-iot-key-trends-opportunities-and-forecasts-2015-2020-market. Accessed September 19, 2016.
4 Weiser M (1991) The computer for the 21st century. *Sci Am* 265(3):94–104.
5 Chen J (2013) 'Internet of things' added to hall of fame for words, i.e., the Oxford English Dictionary. Available at https://blogs.microsoft.com/firehose/2013/09/09/internet-of-things-added-to-hall-of-fame-for-words-i-e-the-oxford-english-dictionary/. Accessed September 16, 2016.
6 Evans D (2011) The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco White Paper. Available at www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed September 16, 2016.
7 (2015) Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. Available at www.gartner.com/newsroom/id/3165317. Accessed September 16, 2016.
8 Brush AJ, et al. (2016) Pervasive computing moves in. *IEEE Pervasive Comput* 15(2):14–15.
9 Haight R, Haensch W, Friedman D (2016) ENGINEERING. Solar-powering the Internet of Things. *Science* 353(6295):124–125.
10 Fernandes E, Jung J, Prakash A (2016) Security Analysis of Emerging Smart Home Applications. *IEEE Symposium on Security and Privacy*, 10.1109/SP.2016.44.