As Objects Go Online

The Promise (and Pitfalls) of the Internet of Things

Neil Gershenfeld and JP Vasseur

Since 1969, when the first bit of data was transmitted over what would come to be known as the Internet, that global network has evolved from linking mainframe computers to connecting personal computers and now mobile devices. By 2010, the number of computers on the Internet had surpassed the number of people on earth.

Yet that impressive growth is about to be overshadowed as the things around us start going online as well, part of what is called "the Internet of Things." Thanks to advances in circuits and software, it is now possible to make a Web server that fits on (or in) a fingertip for $1. When embedded in everyday objects, these small computers can send and receive information via the Internet so that a coffeemaker can turn on when a person gets out of bed and turn off when a cup is loaded into a dishwasher, a stoplight can communicate with roads to route cars around traffic, a building can operate more efficiently by knowing where people are and what they're doing, and even the health of the whole planet can be monitored in real time by aggregating the data from all such devices.

Linking the digital and physical worlds in these ways will have profound implications for both. But this future won't be realized unless the Internet of Things learns from the history of the Internet. The open standards and decentralized design of the Internet won out over competing proprietary systems and centralized control by offering fewer obstacles to innovation and growth. This battle has resurfaced with the proliferation of conflicting visions of how devices should communicate. The challenge is primarily organizational, rather then technological, a contest between command-and-control technology

NEIL GERSHENFELD is a Professor at the Massachusetts Institute of Technology and directs MIT's Center for Bits and Atoms.

JP VASSEUR is a Cisco Fellow and Chief Architect of the Internet of Things at Cisco Systems.

and distributed solutions. The Internet of Things demands the latter, and openness will eventually triumph.

THE CONNECTED LIFE

The Internet of Things is not just science fiction; it has already arrived. Some of the things currently networked together send data over the public Internet, and some communicate over secure private networks, but all share common protocols that allow them to interoperate to help solve profound problems.

Take energy inefficiency. Buildings account for three-quarters of all electricity use in the United States, and of that, about one-third is wasted. Lights stay on when there is natural light available, and air is cooled even when the weather outside is more comfortable or a room is unoccupied. Sometimes fans move air in the wrong direction or heating and cooling systems are operated simultaneously. This enormous amount of waste persists because the behavior of thermostats and light bulbs are set when buildings are constructed; the wiring is fixed and the controllers are inaccessible. Only when the infrastructure itself becomes intelligent, with networked sensors and actuators, can the efficiency of a building be improved over the course of its lifetime.

Health care is another area of huge promise. The mismanagement of medication, for example, costs the health-care system billions of dollars per year. Shelves and pill bottles connected to the Internet can alert a forgetful patient when to take a pill, a pharmacist to make a refill, and a doctor when a dose is missed. Floors can call for help if a senior citizen has fallen, helping the elderly live independently. Wearable sensors could monitor one's activity throughout the day and serve as personal coaches, improving health and saving costs.

Countless futuristic "smart houses" have yet to generate much interest in living in them. But the Internet of Things succeeds to the extent that it is invisible. A refrigerator could communicate with a grocery store to reorder food, with a bathroom scale to monitor a diet, with a power utility to lower electricity consumption during peak demand, and with its manufacturer when maintenance is needed. Switches and lights in a house could adapt to how spaces are used and to the time of day. Thermostats with access to calendars, beds, and cars could plan heating and cooling based on the location of the house's occupants. Utilities today provide power and plumbing; these new services would provide safety, comfort, and convenience.

In cities, the Internet of Things will collect a wealth of new data. Understanding the flow of vehicles, utilities, and people is essential to maximizing the productivity of each, but traditionally, this has been measured poorly, if at all. If every street lamp, fire hydrant, bus, and crosswalk were connected to the Internet, then a city could generate real-time readouts of what's working and what's not. Rather than keeping this information internally, city hall could share open-source data sets with developers, as some cities are already doing.

Weather, agricultural inputs, and pollution levels all change with more local variation than can be captured by point measurements and remote sensing. But when the cost of an Internet connection falls far enough, these phenomena can all be measured precisely. Networking nature can help conserve animate, as well as inanimate, resources; an emerging "interspecies Internet" is linking elephants, dolphins, great apes, and other animals for the purposes of enrichment, research, and preservation.

The ultimate realization of the Internet of Things will be to transmit actual things through the Internet. Users can already send descriptions of objects that can be made with personal digital fabrication tools, such as 3-D printers and laser cutters. As data turn into things and things into data, long manufacturing supply chains can be replaced by a process of shipping data over the Internet to local production facilities that would make objects on demand, where and when they were needed.

BACK TO THE FUTURE

To understand how the Internet of Things works, it is helpful to understand how the Internet itself works, and why. The first secret of the Internet's success is its architecture. At the time the Internet was being developed, in the 1960s and 1970s, telephones were wired to central office switchboards. That setup was analogous to a city in which every road goes through one traffic circle; it makes it easy to give directions but causes traffic jams at the central hub. To avoid such problems, the Internet's developers created a distributed network, analogous to the web of streets that vehicles navigate in a real city. This design lets data bypass traffic jams and lets managers add capacity where needed.

The second key insight in the Internet's development was the importance of breaking data down into individual chunks that could be reassembled after their online journey. "Packet switching," as this process is called, is like a railway system in which each railcar travels independently. Cars with different destinations share the same tracks, instead of having to wait for one long train to pass, and those going to the same place do not all have to take the same route. As long as each car has an address and each junction indicates where the tracks lead, the cars can be combined on arrival. By transmitting data in this way, packet switching has made the Internet more reliable, robust, and efficient.

The third crucial decision was to make it possible for data to flow over different types of networks, so that a message can travel through the wires in a building, into a fiber-optic cable that carries it across a city, and then to a satellite that sends it to another continent. To allow that, computer scientists developed the Internet Protocol, or IP, which standardized the way that packets of data were addressed. The equivalent development in railroads was the introduction of a standard track gauge, which allowed trains to cross international borders. The IP standard allows many different types of data to travel over a common protocol.

The fourth crucial choice was to have the functions of the Internet reside at the ends of the network, rather than at the intermediate nodes, which are reserved for routing traffic. Known as the "end-to-end principle," this design allows new applications to be invented and added without having to upgrade the whole network. The capabilities of a traditional telephone were only as advanced as the central office switch it was connected to, and those changed infrequently. But the layered architecture of the Internet avoids this problem. Online messaging, audio and video streaming, e-commerce, search engines, and social media were all developed on top of a system designed decades earlier, and new applications can be created from these components.

These principles may sound intuitive, but until recently, they were not shared by the systems that linked things other than computers. Instead, each industry, from heating and cooling to consumer electronics, created its own networking standards, which specified not only how their devices communicated with one another but also what they could communicate. This closed model may work within a fixed domain, but unlike the model used for the Internet, it limits future possibilities to what its creators originally anticipated. Moreover, each of these standards has struggled with the same problems the Internet has already solved: how to assign network names to devices, how to route messages between networks, how to manage the flow of traffic, and how to secure communications.

Although it might seem logical now to use the Internet to link things rather than reinvent the networking wheel for each industry, that has not been the norm so far. One reason is that manufacturers have wanted to establish proprietary control. The Internet does not have tollbooths, but if a vendor can control the communications standards used by the devices in a given industry, it can charge companies to use them.

Compounding this problem was the belief that special-purpose solutions would perform better than the general-purpose Internet. In reality, these alternatives were less well developed and lacked the Internet's economies of scale and reliability. Their designers overvalued optimal functionality at the expense of interoperability. For any given purpose, the networking standards of the Internet are not ideal, but for almost anything, they are good enough. Not only do proprietary networks entail the high cost of maintaining multiple, incompatible standards; they have also been less secure. Decades of attacks on the Internet have led a large community of researchers and vendors to continually refine its defenses, which can now be applied to securing communications among things.

Finally, there was the problem of cost. The Internet relied at first on large computers that cost hundreds of thousands of dollars and then on $1,000 personal computers. The economics of the Internet were so far removed from the economics of light bulbs and doorknobs that developers never thought it would be commercially viable to put such objects online; the market for $1,000 light switches is limited. And so, for many decades, objects remained offline.

BIG THINGS IN SMALL PACKAGES

But no longer do economic or technological barriers stand in the way of the Internet of Things. The unsung hero that has made this possible is the microcontroller, which consists of a simple processor packaged with a small amount of memory and peripheral parts. Microcontrollers measure just millimeters across, cost just pennies to manufacture, and use just milliwatts of electricity, so that they can run for years on a battery or a small solar cell. Unlike a personal computer, which now boasts billions of bytes of memory, a microcontroller may contain only thousands of bytes. That's not enough to run today's desktop programs, but it matches the capabilities of the computers used to develop the Internet.

Around 1995, we and our colleagues based at MIT began using these parts to simplify Internet connections. That project grew into a collaboration with a group of the Internet's original architects, starting with the computer scientist Danny Cohen, to extend the Internet into things. Since "Internet2" had already been used to refer to the project for a higher-speed Internet, we chose to call this slower and simpler Internet "Internet 0."

The goal of Internet 0 was to bring IP to the smallest devices. By networking a smart light bulb and a smart light switch directly, we could enable these devices to turn themselves on and off rather than their having to communicate with a controller connected to the Internet. That way, new applications could be developed to communicate with the light and the switch, and without being limited by the capabilities of a controller.

Giving objects access to the Internet simplifies hard problems. Consider the Electronic Product Code (the successor to the familiar bar code), which retailers are starting to use in radio-frequency identification tags on their products. With great effort, the developers of the EPC have attempted to enumerate all possible products and track them centrally. Instead, the information in these tags could be replaced with packets of Internet data, so that objects could contain instructions that varied with the context: at the checkout counter in a store, a tag on a medicine bottle could communicate with a merchandise database; in a hospital, it could link to a patient's records.

Along with simplifying Internet connections, the Internet 0 project also simplified the networks that things link to. The quest for ever-faster networks has led to very different standards for each medium used to transmit data, with each requiring its own special precautions. But Morse code looks the same whether it is transmitted using flags or flashing lights, and in the same way, Internet 0 packages data in a way that is independent of the medium. Like IP, that's not optimal, but it trades speed for cheapness and simplicity. That makes sense, because high speed is not essential: light bulbs, after all, don't watch broadband movies.

Another innovation allowing the Internet to reach things is the ongoing transition from the previous version of IP to a new one. When the designers of the original standard, called IPv4, launched it in 1981, they used 32 bits (each either a zero or a one) to store each IP address, the unique identifiers assigned to every device connected to the Internet—allowing for over four billion IP addresses in total. That seemed like an enormous number at the time, but it is less than one address for every person on the planet. IPv4 has run out of addresses, and it is now being replaced with a new version, IPv6. The new standard uses 128-bit IP addresses, creating more possible identifiers than there are stars in the universe. With IPv6, everything can now get its own unique address.

But IPv6 still needs to cope with the unique requirements of the Internet of Things. Along with having limitations involving memory, speed, and power, devices can appear and disappear on the network intermittently, either to save energy or because they are on the move. And in big enough numbers, even simple sensors can quickly overwhelm existing network infrastructure; a city might contain millions of power meters and billions of electrical outlets. So in collaboration with our colleagues, we are developing extensions of the Internet protocols to handle these demands.

THE INEVITABLE INTERNET

Although the Internet of Things is now technologically possible, its adoption is limited by a new version of an old conflict. During the 1980s, the Internet competed with a network called BITNET, a centralized system that linked mainframe computers. Buying a mainframe was expensive, and so BITNET's growth was limited; connecting personal computers to the Internet made more sense. The Internet won out, and by the early 1990s, BITNET had fallen out of use. Today, a similar battle is emerging between the Internet of Things and what could be called the Bitnet of Things. The key distinction is where information resides: in a smart device with its own IP address or in a dumb device wired to a proprietary controller with an Internet connection. Confusingly, the latter setup is itself frequently characterized as part of the Internet of Things. As with the Internet and BITNET, the difference between the two models is far from semantic. Extending IP to the ends of a network enables innovation at its edges; linking devices to the Internet indirectly erects barriers to their use.

The same conflicting meanings appear in use of the term "smart grid," which refers to networking everything that generates, controls, and consumes electricity. Smart grids promise to reduce the need for power plants by intelligently managing loads during peak demand, varying pricing dynamically to provide incentives for energy efficiency, and feeding power back into the grid from many small renewable sources. In the not-so-smart, utility-centric approach, these functions would all be centrally controlled. In the competing, Internet-centric approach, they would not, and its dispersed character would allow for a marketplace for developers to design power-saving applications.

Putting the power grid online raises obvious cybersecurity concerns, but centralized control would only magnify these problems. The history of the Internet has shown that security through obscurity doesn't work. Systems that have kept their inner workings a secret in the name of security have consistently proved more vulnerable than those that have allowed themselves to be examined—and challenged—by outsiders.

The open protocols and programs used to protect Internet communications are the result of ongoing development and testing by a large expert community.

Another historical lesson is that people, not technology, are the most common weakness when it comes to security. No matter how secure a system is, someone who has access to it can always be corrupted, wittingly or otherwise. Centralized control introduces a point of vulnerability that is not present in a distributed system.

The flip side of security is privacy; eavesdropping takes on an entirely new meaning when actual eaves can do it. But privacy can be protected on the Internet of Things. Today, privacy on the rest of the Internet is safeguarded through cryptography, and it works: recent mass thefts of personal information have happened because firms failed to encrypt their customers' data, not because the hackers broke through strong protections. By extending cryptography down to the level of individual devices, the owners of those devices would gain a new kind of control over their personal information. Rather than maintaining secrecy as an absolute good, it could be priced based on the value of sharing. Users could set up a firewall to keep private the Internet traffic coming from the things in their homes—or they could share that data with, for example, a utility that gave a discount for their operating their dishwasher only during off-peak hours or a health insurance provider that offered lower rates in return for their making healthier lifestyle choices.

The size and speed of the Internet have grown by nine orders of magnitude since the time it was invented. This expansion vastly exceeds what its developers anticipated, but that the Internet could get so far is a testament to their insight and vision. The uses the Internet has been put to that have driven this growth are even more surprising; they were not part of any original plan. But they are the result of an open architecture that left room for the unexpected. Likewise, today's vision for the Internet of Things is sure to be eclipsed by the reality of how it is actually used. But the history of the Internet provides principles to guide this development in ways that are scalable, robust, secure, and encouraging of innovation.

The Internet's defining attribute is its interoperability; information can cross geographic and technological boundaries. With the Internet of Things, it can now leap out of the desktop and data center and merge with the rest of the world. As the technology becomes more finely integrated into daily life, it will become, paradoxically, less visible. The future of the Internet is to literally disappear into the woodwork.