Deconstructing the Internet of Things

The system promises substantial benefits, but privacy and security concerns may prompt new rules

BY SANFORD REBACK
Bloomberg Government Senior Technology Analyst

TONY COSTELLO
Director of Government Affairs Research

RELATED ANALYSIS

Big Data, Big Policy Changes?: BGOV Analysis

Cyberattacks Rise; Mandatory Standards Coming?: BGOV Presentation

Cybersecurity Agenda Advances as Congress Stalls: BGOV Analysis

EU Raises Specter of Tough Internet Regs: BGOV Executive Outlook

FINDINGS

The increasingly interconnected world in which objects, buildings and infrastructure communicate with each other and with us freely and frequently — the so-called Internet of Things (IoT) — promises trillions of dollars in economic impact and dramatic improvements in such diverse areas as health care, energy, transportation, logistics and manufacturing. Whether these new technological developments should be accompanied by new regulations is now being examined.

» As the number of "things" connected to the Internet continues to skyrocket, concerns about cybersecurity and privacy will ratchet up.

» IoT development will bring a plethora of cybersecurity issues, many familiar but grander in scale than current ones, and will require a combination of known techniques and new methods in response. In contrast, IoT development may lead to fundamental changes in the principles underlying privacy protection.

» Though new formal government regulations aren't imminent, a process underway at the National Institute of Standards and Technology (NIST) may produce recommendations that become de facto requirements for manufacturers of connected devices.

WHAT'S AHEAD

NIST has formed a cyber-physical systems public working group that is addressing the cybersecurity and privacy implications of the IoT, among other things. The group is expected to produce an initial document in November, and continue its work well into 2015 at least.

Congress also is getting into the act. Four members of the Senate Commerce Committee have asked that the committee hold an oversight hearing on the IoT by the end of the year.

The most immediate risk of IoT regulatory measures may come from overseas. European Union (EU) policymakers historically have taken a more stringent regulatory approach toward privacy issues than their U.S. counterparts.

The Substantial Economic Impact of the Internet of Things

Dollars in trillions

Sources: U.S. Treasury Department, International Data Corporation

WHAT IS THE 'INTERNET OF THINGS?'

There's no agreed definition of the Internet of Things. Indeed, the term is so ill-defined that various names exist for the same phenomenon — in addition to IoT, M2M (for machine-to-machine), cyber-physical systems, intelligent systems, and the Intelligent Internet also are used.

All of these terms generally refer to the same development: the proliferation of very small and low-cost sensors deployed in an increasing number of everyday "things," which are gathering data in unprecedented amounts and communicating with each other and sometimes with us, often by transmitting that data over the Internet.

The scale of sensor deployment is indeed breathtaking and is expected to accelerate rapidly in the next several years. The number of connected "things" deployed is expected to exceed 50 billion by the year 2020, a five-fold increase from the estimated 10 billion connected things in 2013.[1]

Hand-in-hand with sensor deployment is the generation, transmittal and accumulation of tremendous amounts of data. One research organization concluded in 2013 that 90 percent of all data in the world had been generated in the previous two years. [2]

Analysis of this so-called "big data" has the potential to yield substantial economic benefits, such as better insurance fraud prevention systems and earlier detection of disease epidemics. Much of the data that will be generated by connected devices will concern machine-to-machine communications about industrial processes, and won't involve personally identifiable information at all. Even so, the volume and variety of personal information that will be collected has raised concerns that maintaining privacy will become difficult, if not impossible.

The economic impact of the developing IoT could be enormous. One study estimates that IoT technology and services spending will generate global revenues of $8.9 trillion in 2020, while another pegs the economic impact of the IoT at as much as $6.2 trillion annually by 2025.[3, 4]

By way of comparison, U.S. federal government spending totaled about $3.5 trillion in fiscal year 2013. U.S. gross domestic product was $16.8 trillion in 2013.

BENEFITS OF THE IOT

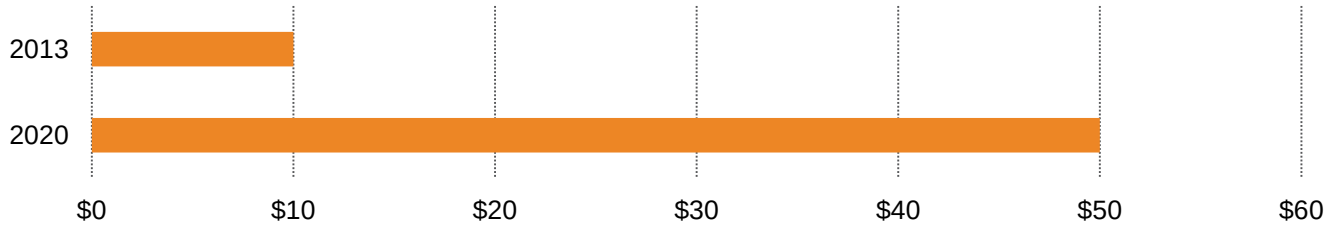
Even those concerned about aspects of IoT deployment generally agree that its continued development will bring significant benefits.

Some IoT applications already are commonplace. An increasing number of consumers program their DVRs remotely by using their smartphones, and television advertisements abound touting programs that allow customers to control their home electrical and alarm systems remotely. A variety of cars on the market feature automatic parallel parking systems. Google Inc.'s self-driving cars, still in the testing phase, have reportedly traveled more than 700,000 miles, with the few reported incidents due to human error.[5]

As deployed sensors become ubiquitous and connected devices proliferate, the advances promised by the IoT become much more significant. Rather than just individual self-driving cars, for example, increased sensor deployment may bring smart citywide transportation systems that route as well as drive cars, alleviating congestion, conserving energy and reducing accidents. Bridges and tunnels may constantly self-monitor themselves, detecting conditions that require correction and alerting engineers so that repairs can be carried out before catastrophic failures occur. Increasingly automated

Billions and Billions of Connected 'Things'

The number of "things" connected to the Internet is expected to increase fivefold between 2013 and 2020.
Dollars in billions



Source: Cisco Systems Inc.

supply chains in many industries will allow the monitoring of inventory, the ordering of supplies and the delivery of goods with limited human involvement.

POLICY CONCERNS

The continuing development of the IoT is not without controversy. Policy concerns generally center around two related but distinct areas: cybersecurity and privacy.

Cybersecurity

Cybersecurity has been at the forefront of policymakers' concerns in Washington for several years. As IoT development proceeds, concerns about the security of data and the systems using it almost certainly will increase, though government action to mandate specific product and process standards isn't likely in the near term.

IoT development could increase security vulnerabilities at both the individual and systemic levels. Part of the problem is that while a variety of new "things" are being connected to the Internet, the manufacturers of these objects may not have either the experience or expertise to implement appropriate security safeguards.

For individuals, the concerns range from the unsettling to the truly terrifying. On the bizarre side, hackers have already demonstrated an ability to break into web-enabled baby monitors and yell obscenities at young children.[6] The doctor for then-Vice President Dick Cheney insisted that the wireless feature of Cheney's implanted defibrillator be disconnected, for fear that terrorists would try to make it malfunction, a life-imitates-art example of a capability demonstrated on the television series *Homeland*.[7] More ominously, researchers have shown that they can remotely hack into an automobile and take over the car's basic functions. [8]

The consequences of successful attacks on larger connected systems could be catastrophic. If researchers can make a single self-driving car malfunction, imagine the havoc that could ensue from a successful breach of the smart transportation system of a major metropolitan area. Or the chaos that could result from a successful hack of an automated system through which drug manufacturers provide hospitals with critical supplies.

In short, IoT development seems likely to exacerbate already well-known concerns about data and system security. However, that doesn't mean that new government requirements will soon follow.

With a few exceptions, the U.S. government approach to improving cybersecurity currently is predicated on a hortatory rather than a regulatory approach. Companies are encouraged to participate in public-private partnerships and adopt voluntary documents best exemplified by the NIST cybersecurity framework published in February. They are exhorted, but not yet required, to "bake" cybersecurity into their products and services. It's not yet clear whether this approach will be sufficient to keep pace with technological changes or whether it will yield the desired improvements in cybersecurity.

Privacy

The IoT promises the same kinds of data security concerns we're currently familiar with, only more so, and a mixture of familiar cybersecurity practices and new techniques will be necessary as the number of deployed connected systems skyrockets. The implications for privacy policy could be even more fundamental.

There's no overarching privacy law in the U.S. Laws and regulations that exist generally cover only selected areas of consumer information, such as financial transactions and health-care data, a design often referred to as a "patchwork quilt" of protection. The Federal Trade Commission (FTC) serves as a kind of backstop, working to ensure that companies that promulgate privacy policies don't engage in deceptive or misleading practices.

By and large, privacy protection currently is based on the concept of "notice and consent." Before signing up for a new product or service, consumers are given the opportunity to review what kind of personal information the company will collect and how it will use the information collected.

It's far from clear that the system in place is working well today. Most consumers give a cursory glance, if that, to privacy policies displayed online on sign-up pages before clicking to accept.

But even that level of protection won't exist in the fully developed IoT world. Some deployed sensors don't have human interfaces at all, so consumers won't have an opportunity to weigh the benefits of a service or adjust its parameters before purchasing it. Others, such as deployed sensors in a home television, will be able to collect and

transmit information unrelated to viewing habits, such as other activities going on in the home.

Some critics have said that people may one day be deprived of free choice.[9] They fear that, because companies will have compiled such detailed profiles of consumers based on the vast amounts of personal information collected, they will offer consumers only the products or services they seem most likely to purchase.

The solution to this issue — one that even vigorous proponents of IoT development acknowledge is a potential problem — isn't clear. Among other things, business groups and even some academics argue that the potential benefits of the IoT should be weighed against the costs of lost personal privacy protection before restrictions on IoT deployment are imposed.

The FTC says that, while privacy principles may need to be adjusted in the IoT era, protection should rest on three core principles: privacy by design, simplified consumer choice, and transparency. The agency released a report containing these recommendations in 2012, but they have yet to gain legislative traction.

A more fundamental change, endorsed by business groups and embraced in a recent White House report on big data, would be to transition the basis of privacy protection from a concept of "notice and consent" to one of "responsible use." Rather than trying to restrict the kinds and amount of data companies collect at the front end, regulators instead would focus on ensuring that companies didn't misuse whatever data they had collected.

It's not clear exactly how a responsible-use system would work or whether privacy advocates would find it palatable. That being said, such a system could shift more of the responsibility for ensuring privacy protection to companies from individuals, which many would find a welcome development.

WHAT TO WATCH

While new regulations governing the Internet of Things aren't imminent, several regulatory bodies have begun examining its policy implications. In some cases, these processes may establish de facto standards for various aspects of IoT development. Interested parties should monitor and participate in these processes.

The most important of these, with the most significant potential impact on IoT standards and requirements, may turn out to be the process underway at NIST. The agency established a cyber-physical systems public working group in June. The working group is composed of four subgroups: cybersecurity and privacy; definitions, taxonomy, and reference architecture; use cases; and timing and synchronization. Members of the public may participate in the working group.

Each subgroup is expected to produce a summary report by early November, but the working group's tasks are expected to continue well into 2015 at least.

Some of the group's work will focus on the development of IoT infrastructure — for example, how to ensure interoperability among the various IoT systems being deployed in specific industries. But the cybersecurity and privacy subgroup in particular may edge into broader policy areas. The group may end up recommending, for example, requirements that deployed systems should satisfy to ensure data security.

Federal Trade Commission Policy Recommendations

The agency's proposals were designed to articulate best practices by companies and serve as the basis for possible legislation.

Recommendation	Suggested Company Actions
Privacy by design	Companies should incorporate substantive privacy protection throughout the life cycle of their products/services, including data security, reasonable collection limits, sound retention and disposal practices, and data accuracy
Simplified consumer choice	Companies should offer choice to a consumer when that customer is making a decision about a company's use of personal data. No choice is required for data collection consistent with the context of the transaction or the existing relationship with the consumer.
Transparency	Companies should increase the transparency of their data practices by providing shorter and more standardized privacy notices, reasonable access to the consumer data they maintain, and better education about commercial data privacy practices.

Source: Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission, March 2012

Whether the working group produces a framework of recommended practices for cyber-physical systems, or instead simply details how the existing NIST voluntary cybersecurity framework should be adapted for the Internet of Things, isn't yet clear. In either case, the influence of the group's work could prove to be far greater than simply a suggestion of recommended practices.

The NIST cybersecurity framework, though presumptively voluntary, has already achieved a more elevated status. Attorneys have begun advising their clients to implement the framework or face additional legal exposure in the event of a cyberbreach, and companies have begun requiring their suppliers to adhere to the framework's standards and processes. A cybersecurity framework for cyber-physical systems, even though not officially mandatory, could achieve a similar status.

Other agencies that have been examining the privacy and security implications of IoT development probably won't push for new regulations in the near term. The FTC is the federal government agency most active in protecting consumer privacy, but the agency seems unlikely to soon urge new regulatory measures with respect to the IoT. The agency's workshop on the privacy and security implications of the IoT held last November suggests that the FTC is currently in a "listen and learn" mode.[10]

Even so, companies would be well-advised to remain abreast of the agency's thinking on these issues. As it demonstrated in an action against a maker of hacked Web-enabled home surveillance cameras last year, the FTC isn't afraid to use its enforcement powers in appropriate cases.[11]

Congress also is getting into the act. Four members of the Senate Commerce Committee, two Democrats and two Republicans, on Oct. 20 wrote to committee leaders asking them to hold an oversight hearing on the IoT by the end of the year.[12]

The senators said that the developing Internet of Things "presents a wide range of cutting-edge policy issues impacting a broad set of businesses and industrial sectors." They said that the relevant policy questions included those related to consumer protection, security, privacy and manufacturing, among other things.

The more immediate risk of IoT regulatory measures may come from overseas. EU regulators historically have taken a more stringent approach to privacy issues than their U.S. counterparts. At a recent conference of data protection commissioners, several officials from EU countries voiced concern about the potential impact of IoT development on personal privacy.

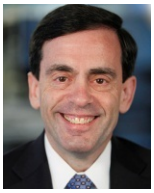
ABOUT BLOOMBERG GOVERNMENT

Bloomberg Government is the only comprehensive web-based information service for professionals who are affected by and interact with the federal government. Bloomberg Government provides rich data, analytical tools, timely news and in-depth analysis from policy experts — all from the leader in business information services.

ANALYST CONTACT INFORMATION

Sanford Reback, Senior Technology Analyst sreback1@bloomberg.net +1 202 416 3421

ABOUT THE ANALYST



Sanford Reback is a Senior Technology Analyst with Bloomberg Government. He previously served as an executive at MCI, then a Fortune 100 company; UUNET, then the world's largest Internet services provider; and two venture-backed technology companies. At the Office of the U.S. Trade Representative, he helped negotiate NAFTA and the World Trade Organization agreements and technology sector agreements. Reback holds a B.A. in political science from Stanford University, a J.D. from Harvard Law School, and a master's degree from Harvard's Kennedy School. He was a Fulbright Fellow in London. Follow Sandy on Twitter: @SandyReback

ENDNOTES

[1] Cisco Systems Inc., Connections Counter: The Internet of Everything in Motion, July 29, 2013, http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342 (retrieved Oct. 20, 2014).

[2] SINTEF, "Big Data — for better or worse," http://www.sintef.no/home/Press-Room/Research-News/Big-Data--for-better-or-worse/ (retrieved Oct. 27, 2014).

[3] International Data Corporation, "The Internet of Things is Poised to Change Everything, Says IDC," press release, Oct. 3, 2013, http://www.idc.com/getdoc.jsp?containerId=prUS24366813, (retrieved Oct. 27, 2014).

[4] McKinsey Global Institute, "Disruptive technologies: Advances that will transform life, business, and the global economy, May 2013, http://www.mckinsey.com/insights/business_technology/disruptive_technologies (retrieved Oct. 27, 2014).

[5] Sebastian Anthony, "Google's self-driving car passes 700,000 accident-free miles, can now avoid cyclists, stop at railroad crossings," Extremetech, April 29, 2014, http://www.extremetech.com/extreme/181508-googles-self-driving-car-passes-700000-accident-free-miles-can-now-avoid-cyclists-stop-for-trains (retrieved Oct. 28, 2014).

[6] Kashmir Hill, "The Half-Baked Security of Our 'Internet of Things,'" Forbes, May 27, 2014, http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/ (retrieved Oct. 27, 2014).

[7] Sanjay Gupta, Dick Cheney's Heart, 60 Minutes, Oct. 20, 2013, http://www.cbsnews.com/news/dick-cheneys-heart/ (retrieved Oct. 27, 2014).

[8] John Markoff, "Researchers Show How a Car's Electronics Can Be Taken Over Remotely," The New York Times, March 9, 2011,http://www.nytimes.com/2011/03/10/business/10hack.html?_r=2& (retrieved Oct. 27, 2014).

[9] Stephen Gardner, "World's Data Protection Leaders Highlight Internet of Things, Big Data Privacy Risks," Bloomberg BNA, Oct. 15, 2014, http://www.bna.com/worlds-data-protection-n17179897174/ (retrieved Oct. 21, 2014).

[10] Federal Trade Commission, "Internet of Things - Privacy and Security in a Connected World," workshop, Nov. 19, 2013, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (retrieved Oct. 27, 2014).

[11] Federal Trade Commission, FTC Approves Final Order Settling Charges Against TRENDnet, Inc., Press Release, Feb. 7, http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc (retrieved Oct. 27, 2014).

[12] Senator Deb Fischer et. al., letter to Senate Commerce Committee leaders requesting an Internet of Things oversight hearing. Oct. 20, 2014, http://www.fischer.senate.gov/public/_cache/files/e0a5801e-e239-4db8-812f-b9843f111b7d/internet-of-things-commerce-hearing-letter-1-.pdf (retrieved Oct. 22, 2014).