Deloitte.
University Press

Guiding the IoT to safety

The Internet of Things and the role of government as both user and regulator

Deloitte's Center for Integrated Research focuses on critical business issues that cut across industry and function, from the rapid change of emerging technologies to the consistent factor of human behavior. We uncover deep, rigorously justified insights, delivered to a wide audience in a variety of formats, such as research articles, short videos, or in-person workshops.

COVER IMAGE BY: ALEX NABAUM

CONTENTS

Introduction

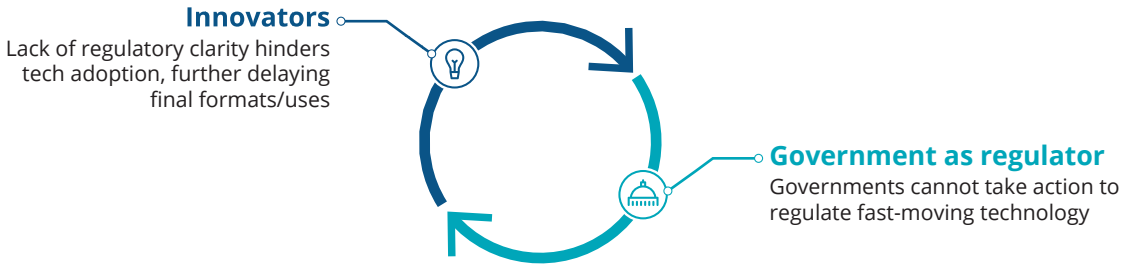
The Internet of Things and the role of government as both user and regulator

IMAGINE Pandora sitting and staring at her box. In a few moments, she will open its bronze lid and release fear, death, and plague into the world. . . but right now she is wracked with uncertainty. What's inside? The box might contain untold riches to help her new kingdom—but Zeus warned her never to open it. Should she open it and risk punishment, or leave it shut and possibly leave valuable resources untapped?[1]

In many ways, the story of technological change and regulation is Pandora's story—technology can be understood only through the lens of risk and uncertainty. Technological change by its very nature causes uncertainty: How could this new technology be used? How might it improve people's lives? How may it harm those same lives? With the Internet of Things (IoT) at the peak of its hype cycle, these questions are swirling more than ever.[2] The challenge is the risk that accompanies all of this uncertainty. Like Pandora, companies looking to implement IoT solutions are facing a box that may contain significant new revenues—and, quite possibly, technical difficulties, future regulatory challenges, or security breaches. Do they risk opening the IoT box and facing these uncertain regulatory issues, or do they leave it closed and risk missing out on the potentially most transformative technology since the Internet?

One key to making an informed decision and ameliorating risk is to reduce uncertainty—in particular, uncertainty about future regulation that may affect IoT practices. For regulators too, pressure is mounting to protect consumers even while IoT technology itself is still developing.[3] But with the often-blunt instrument of regulation, this could become a catch-22 of inaction: Regulators take no action because they are uncertain about the technology, so companies take no action because of uncertainty about regulation, slowing technological adoption. . . and further slowing the action of regulators (see figure 1).

Figure 1. The catch-22 of regulating fast-moving technology



Source: Deloitte analysis.

Figure 2. Using government's other roles to break the catch-22

Source: Deloitte analysis.

But it takes only a shift in perspective to break this catch-22. Consider that government's relationship with IoT technology goes beyond regulation—agencies are also consumers and developers of IoT infrastructure and applications. In these two roles, government can influence the development of IoT technology, guiding it toward safe, secure, and responsible uses—and saving regulation for indisputably necessary areas such as critical infrastructure or health systems (see figure 2).

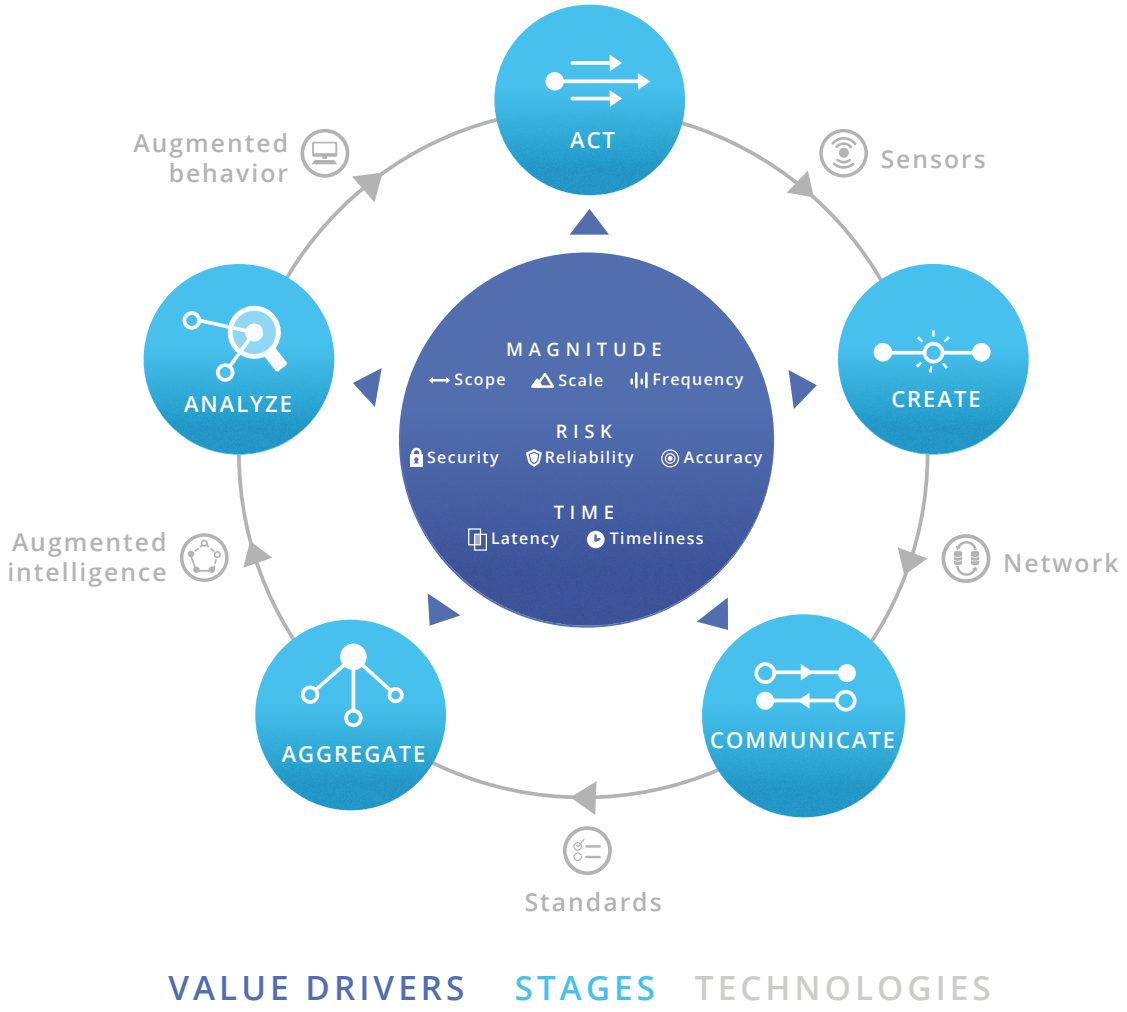
To illustrate exactly how governments at all levels can help to guide the IoT's development—protecting citizens while still encouraging technological growth—this article makes use of a body of industry-specific use cases. The goal: to reduce overall uncertainty, allowing policymakers to understand this complex issue and businesses to see where government action is likely, thereby reducing the risk of their investments in IoT technology.

Governments and the IoT

THE first step to reducing the uncertainty and risk around the IoT is to get a better picture of what it is, and how government agencies may need to interact with it. The IoT is the architecture and suite of technologies needed to create, communicate, aggregate, analyze, and act upon digital information in the physical world (see figure 3).

With such a broad definition, the applications and impacts of connected technology on the public sector can cover an equally wide spectrum. Utility providers have created mesh networks of smart meters capable of hosting other communications.[4] Automakers and tech companies are investing in autonomous vehicles that may require new public infrastructure.[5] Customer advocacy groups are

Figure 3. The Information Value Loop



Source: Deloitte analysis.

calling on government to create strenuous security and privacy standards for new connected devices.[6] Even with this bewildering mix of uses, roles, and industries, agencies' interactions with IoT technology can be grouped into three categories:[7]

- **Government as IoT end user.** To the extent that reporters and academics have addressed the government's relationship to the IoT, articles (including our *Anticipate, sense, and respond*[8]) have focused on the question of how government can harness connected technology to better provide services. These address how schools, public utilities, law enforcement, and other government functions can take advantage of the new technologies to break traditional trade-offs and find innovative ways to serve the public. In the interest of space, we will address less commonly discussed roles of government.
- **Government as infrastructure provider.** The investigation of what government policies or regulation may be necessary for effective use of IoT technology begins with understanding connected infrastructure. Just as governments are responsible for building and maintaining their countries' highways for vehicles, they may be called upon to provide the infrastructure for the IoT. However, with so many different types of communications mechanisms and protocols within the IoT stack, it is unclear at this point exactly what is required to create foundational infrastructure for IoT.
- **Government as regulator.** New technologies necessarily bring with them new uncertainties about their use. These uncertainties represent a risk to the public, which governments at all levels are responsible for ameliorating. Complicating this issue is that, at the emergence of a new technology, the full array of its eventual possible uses cannot be known. Therefore, it can be quite difficult to forecast the potential dangers that such technologies pose to the public.

The first step in order to strike that balance is to understand what the IoT needs in order to reach its full potential.

Already from these three roles, we can see a tension forming in governments' goals with relation to new technology. As an infrastructure provider, governments seek to support and incentivize further technological development to create new value and new public goods. On the other hand, governments have a duty to protect the public from the risks of both the known and unknown uses of those new technologies. Striking the right balance between these goals, and then crafting appropriate policies to achieve them, is the chief challenge facing officials dealing with emerging technologies.

The first step in order to strike that balance is to understand what the IoT needs in order to reach its full potential. To do so, we'll look at some industry-specific case studies that reveal the key bottlenecks impeding the IoT from creating new value.

Identifying critical needs in industry

THE IoT is fundamentally about bringing the benefits of information to the physical world. Therefore, for the technology to create value for customers, companies, or society at large, the information created by sensors needs to reach those individuals or machines that can take informed action on it. In other words, information must be able to complete the Information Value Loop. In this sense, the race to create IoT solutions is really a race to alleviate a series of bottlenecks that restrict or stop that flow of information. Understanding where and how these bottlenecks are restricting the flow of information, then, can help companies and government alike understand what is holding back the development and implementation of IoT technology as a whole.

Through an extensive IoT research campaign, Deloitte has built up a large collection of use cases, with IoT examples in every industry.[9] In analyzing these use cases, we found that once companies began generating data with IoT technology, the most common bottlenecks arose in the *communication, aggregation*, and *analysis* of that data.[10] By looking at each of these bottlenecks, we can begin to sketch out where government action is needed and where it may be counterproductive. (See figure 4.)

Figure 4. Common bottlenecks that constrain information flow in many different industries

Common bottleneck to information flow	Government action needed to support rapid, responsible development of IoT technology	Ways ahead
Communicate Competition for limited bandwidth can slow development	Government must act as infrastructure provider to ensure effective bandwidth	
Aggregate Lack of common standards can limit aggregation of data	Industry is leading; no government action is needed	
Analyze Analysis of such volumes and new types of data can create privacy issues	Government must act as a regulator to protect customers **But this begs the same catch-22, so agencies need to find novel ways to offer guidance**	Use role of government as user of IoT to **set a good example*** Use role of government as infrastructure provider to **reduce function creep*** Use role of government as both user of IoT and infrastructure provider to **enable transparency***

Source: Deloitte analysis.

Communicate: A role for government as infrastructure provider

At least as far back as the Industrial Revolution, there has been a clear role for governments to coordinate, if not directly provide, the basic infrastructure needed for economic development.[11] When *infrastructure* meant highways, bridges, canals, and airways, the government's role was rather clear: In situations where private industry could not or would not act, the public sector would provide the physical roads, ramps, and rails over which the traffic of commerce could move.[12] Same with power lines and gas connections, and with telephone lines and submarine communications cables: The government has an interest in linking citizens, even in rural areas that companies might find unprofitable to service.

> After all, with IoT technology, it is information that creates value.

But when it comes to the Internet of Things, government's role is less clear—as are its possible actions as an infrastructure provider. After all, with IoT technology, it is information—not trucks, planes, or rail cars—that creates value.

No question, though, that government does play a key role. While you may not be able to see it, information still travels via public-sector infrastructure much as cars traverse highways. For example, every smartphone is able to deliver driving directions only because of the multibillion-dollar government investment in GPS satellites[13]—not to mention the electromagnetic spectrum, a finite resource that government regulates to carefully share among competing public, private, and even military uses. With the number of IoT-connected devices expected to increase by 3 to 30 times over the next 15 years, the strain on existing spectrum allocations is enormous.[14] So it is perhaps unsurprising that governments around the world are taking steps to open up more spectrum to wireless uses. Whether allocating previously unused spectrum to IoT applications or repurposing spectrum from older uses, governments are working to provide the raw materials that connected technology needs to grow.[15]

Perhaps most interestingly, where paving highways and laying track cost taxpayers millions, allocation of spectrum is technically free—save for the time it takes to do the work. In fact, the potential IoT-based advances mean that governments can in some cases actually generate significant revenue from reallocating portions of spectrum. Recently, both US and Canadian telecom regulators were able to raise billions of dollars from spectrum auctions, with the 2015 Canadian sale raising more than $2 billion and the US auction a year earlier generating a record $44.9 billion.[116] In exercising its role as IoT infrastructure provider, a government may be able to efficiently allocate scarce wireless resources and, in the process, create benefits for both companies and taxpayers.

Aggregate: Where regulation may not be necessary

For connected technology to create real value, it should be able to sense not just one particular piece of data but data from multiple sensors and sources. In reality, this means that different devices from different manufacturers often must be able to seamlessly communicate and share data. To do so requires common standards for data format and communications protocols. At first glance, this represents a great opportunity for government to intervene in its role as regulator to create one common standard and accelerate the IoT's growth.

However, government action on standards may be superfluous or even counterproductive. Industry is not insensitive to the need for standards and has formed a number of competing groups aimed at designing the standards of the future.[17] While none of these standards has yet won out, that is more a function of the continuing development of the technology and market, rather than intransigence of the groups.

In fact, with many of the underlying standards in place for communication protocols, such as 4G and Wi-Fi, and device addressing, such as IPv6, the situation resembles the early days of mobile operating-system competition.[18] In that arena, it was not government regulation but, rather, a dominant player creating a superior platform that created the de facto standard. Industry leaders produced winning mobile OS platforms that unified many elements of a fragmented technology landscape to produce industry standards.[19]

A similar process may be under way with IoT technology, leading both government and industry leaders to conclude that government regulation of IoT standards would be a mistake.[20] While there may be a role for agencies to play in setting out IoT guidelines for specific critical industries—such as ensuring interoperability of electronic health data—full regulation of IoT standards may actually slow innovation rather than accelerating it.[21]

Analyze: A role for government as regulator

This is not to say that there is no role for government in its capacity as a regulator. The IoT's expanding implementation means more and more data being generated about things and people. Companies aim to combine and analyze all of this data to create new insights and provide services to consumers. The catch: In the process, IoT technology may expose individuals' privacy in new ways. Research shows that it can take as few as four data points from mobile communications to individually identify an individual.[22] In analyzing data such as purchasing history or speed patterns of your connected car, an IoT system can unintentionally reveal sensitive private information such as attendance at a particular church or movements of a competitor's sales force. Apart from obvious security concerns from such data attracting criminals and identity thieves, breaches may leave users justifiably uneasy.[23]

In the interest of building confidence in connected technology, there is an undeniable need for government to regulate the IoT from the perspective of consumer protection, especially as it relates to security and privacy. The difficulties will sound familiar to anyone involved in government regulation of technology: IoT applications are fast proliferating—with new technologies, processes, and uses emerging almost daily—while traditional regulatory processes are often measured and slow, with publishing a new rule in under three months usually possible only in an "emergency."[24] This is to say nothing of the legislative gridlock that can stall for years the authority to even make those new rules in the first place.[25]

As digital information moves rapidly around the globe, it can encounter many different regulatory regimes.

Even beyond the general difficulties in regulating fast-moving technologies, privacy presents special challenges. As digital information moves rapidly around the globe, it can encounter many different regulatory regimes. Sure, companies can aim to comply with each nation's privacy rules, but these different rule sets are often built upon entirely different legal conceptions of privacy, resulting in at times contradictory rules, making compliance with all rules impossible.[26] If the IoT is to reach its potential, it will almost certainly involve collecting and transmitting data across national borders. Decades and centuries of transnational trade have firmly established regulation across borders, but data is both different and intangible, and nations' underlying differences on the core concepts of privacy make such regulation highly unlikely for IoT technology. Issues with transnational fragmentation await resolution in a way that both protects consumers globally yet allows connected technology to thrive.[27]

In this way, we have returned to Pandora's box—the fundamental issue of regulating new technology. Governments should step in to protect consumers in some way, despite uncertainty about rapidly

changing technology. Similarly, companies working to develop IoT applications face uncertainty around potentially impactful regulations. That said, however new and expansive IoT technology might be, these uncertainties shouldn't dramatically hold up development of either applications or regulations. For one thing, as we have seen, only a few areas actually demand regulatory intervention. Second, the consumer privacy and security issues raised by connected technology are not new. While the mobile nature of IoT technology may cause these issues to pop up in new and unexpected places, governments and companies are well equipped to deal with security and privacy issues once identified. In the United States, agencies such as the Consumer Protection Bureau and legislation like the Fair Credit Reporting Act are empowered to act to protect consumers from IoT-based security and privacy challenges, even if the pace of new IoT developments may require these familiar actors to pick up some new tools.

Finding new tools

Concrete steps for government to guide the IoT

If regulation's ultimate purpose is to encourage companies and others to take into account externalities such as security and privacy, there can be a number of effective tools that can accomplish this.[28] Two untapped tools for governments at every level are their actions in other roles relating to IoT technology—namely, user and infrastructure provider—which, again, offer more certain and stable starting points than trying to hit the moving target of regulating a rapidly changing new technology. Agencies can use their activities as IoT users and infrastructure providers to help guide and shape the development of connected technology.

Set a good example: government as an IoT user. First and foremost, governments exist to provide services to citizens. Given the IoT's tremendous power to increase efficiency and provide new services, it is no surprise that much of the discussion centers on how agencies can use connected technology to better serve citizens. Hardik Bhatt, CIO of the state of Illinois, summarizes: "The first and very active role of government is government as a customer."[29] It is exactly by being large-scale consumers of connected services and technology that agencies can influence IoT development through buying power, not regulations. By setting responsible requirements and buying secure, privacy-respecting solutions, government can, as Bhatt describes, "start being the role model of how the Internet of Things technology can be used."[30]

First and foremost, governments exist to provide services to citizens.

The impact of a public-sector role can go beyond the economic impact of the dollars that agencies spend to set up IoT solutions. It can extend to the heart of the technology itself. Humans can be both incredibly creative and also incredibly lazy, and programmers are no exception. As a result, once a programmer finds a successful solution to a certain problem, others tend to copy that code and paste it into new applications, skipping the usual rounds of testing. The jumbled result, dubbed "spaghetti code," can introduce unintended bugs and flaws, and with fast-moving technologies, this problem has the potential to quickly spread security holes. While spaghetti code is a problem in every industry, government's open, public-service nature may put it in a unique position to help the situation: By creating good, solid code and making it publicly available, an agency can be the source or seed for other organizations using connected technology more responsibly.

Reduce function creep: government as infrastructure provider. There's no question that function creep—a product being used in unanticipated ways—can be an incredibly powerful tool for innovation, such as when a teacher noticed that a wallpaper cleaning putty made a good toy, giving birth to Play-Doh. But function creep can introduce critical security and privacy flaws into new technologies,[32] exacerbated by a lack of purpose-built tools, forcing developers to plug in close-enough hardware and software. Government can play a strong role in limiting function creep—and thereby reducing the likelihood of security and privacy vulnerabilities—by making available stable infrastructure for connected technology.

Enable transparency: government as both user and infrastructure provider. The IoT-based distributed denial-of-service attack that shut down Internet access to millions of people

on October 21, 2016, highlights a key vulnerability of connected technology. Many people whose devices were compromised by the Mirai malware that launched the attack were unaware that their devices' security might be substandard; in fact, many did not even know their devices had been compromised.[33]

Whether dealing with security or privacy, transparency is a critical virtue.

Whether dealing with security or privacy, transparency is a critical virtue. In the United States, for example, privacy is governed largely by contracts and user agreements, an arrangement that is untenable if companies conceal their usage of consumer data. Similarly, both governments and companies are powerless to begin to plug IoT cyber vulnerabilities unless they are aware of the basic state of their hardware and software. And when that hardware and software is compromised, each party needs to be able to share information about the attacks and signatures with each other.

In its dual role as IoT user and infrastructure provider, government can help to lay the foundation for this needed transparency.[34] Transparency is a critical unsolved challenge in IoT technology, since there's no practical way to adequately inform consumers about all the uses of their data stemming from potentially hundreds of small devices. Agencies can serve as a model of transparency by finding new ways to solve this challenge, clearly and concisely communicating to users what data is collected and how it will be used.

Similarly, as infrastructure providers, governments can begin to create stakeholder groups and information-sharing venues that can allow for the transparency necessary to combat cyber threats. Here companies can share information on attacks and threats, preemptively benefiting from shared information and concerns—better for everyone than regulators requiring them to reveal data losses. Finally, given the continued threat posed by botnets such as Mirai, governments should consider establishing a security rating system or evaluation organization for new hardware and software products. A public-private working relationship on the model of Underwriters Laboratory may be an effective model for quickly and efficiently establishing the baseline of transparency required for IoT security.[35]

These same principles can have a double impact at reducing uncertainty: Not only do they help governments act amid uncertainty around connected technology—they can help companies understand how regulators are likely to respond to IoT-related issues. These seemingly small actions can give companies the confidence to innovate and drive the technology further, while protecting citizens' rights and personal information.

In this way, the IoT resembles Pandora's box less than it does Schrödinger's box:[36] You can never know ahead of time whether the cat is alive or dead—if the technology will be a boon or a hazard—so you need to plan for both eventualities and try to build in as much certainty as possible. Of course, unknowns are inevitable and not necessarily fatal—after all, uncertainty around the state of the electron did not stop Erwin Schrödinger and others from building modern electronics; in fact, chances are that the touchscreen of the laptop or phone on which you are reading this article harnesses exactly those quantum effects.[37] And for government, the key to ameliorating uncertainty, encouraging corporate innovation, and protecting citizens is to consider IoT technology as both user *and* regulator.

ENDNOTES

1. According to Greek mythology, Pandora was the first woman the gods created to live on Earth. She was married to Perseus, who had angered Zeus by stealing fire and giving it to man. In retribution, Zeus fashioned a bronze box full of all evils and miseries and gave it to Pandora as a wedding present, warning her to never open it. Overcome by curiosity, Pandora opened the box, releasing death, sickness, and all other miseries into the world. However, Pandora also later discovered and released *hope*—perhaps another fitting analogy to the story of technology.

2. Gartner, *2016 Hype Cycle for Emerging Technologies*, August 16, 2016, www.gartner.com/newsroom/id/3412017.

3. From new privacy regulation in Brussels to congressional hearings in Washington, governments are struggling to come to grips with how to approach the IoT. In 2015, *Politico* devoted an entire issue to the topic; see www.politico.com/agenda/issue/internet-of-things-july-2015. However, as a recent *Fortune* article points out, as a result of the uncertainty around connected technology, most of these efforts focus on what could go wrong with the IoT, not how to effectively manage it; see http://for.tn/1GVbNVB.

4. Rob Young, John McCue, and Christian Grant, *The power is on: How IoT technology is driving energy innovation*, Deloitte University Press, January 21, 2016, http://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-electric-power-industry.html.

5. Scott Corwin, Joe Vitale, Eamonn Kelly, and Elizabeth Cathles, *The future of mobility: How transportation technology and social trends are creating a new business ecosystem*, Deloitte University Press, September 24, 2015, http://dupress.deloitte.com/dup-us-en/focus/future-of-mobility/transportation-technology.html.

6. Loek Essers, "Internet of Things companies need to ensure consumer privacy, warns US regulator," *PC World*, January 7, 2015, www.pcworld.com/article/2866372/iot-companies-should-ensure-consumer-privacy-warns-us-regulator.html.

7. These three categories draw on similar research done relating to government's possible roles in data exchange. For more, see William D. Eggers, Rob Hamill, and Abed Ali, *Data as the new currency: Government's role in facilitating the exchange*, Deloitte University Press, July 24, 2013, http://dupress.deloitte.com/dup-us-en/deloitte-review/issue-13/data-as-the-new-currency.html.

8. Max Meyers, Claire Niech, and William D. Eggers, *Anticipate, sense, and respond: Connected government and the Internet of Things*, Deloitte University Press, August 28, 2015, http://dupress.com/articles/internet-of-things-iot-in-government/.

9. See Deloitte University Press's series of articles on the Internet of Things, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things.html.

10. In fitting with both anecdotal and other survey data, the most common bottleneck has been at the beginning: using IoT technology to generate data in the first place. However, as the cost of sensor and computing power continue to decline and familiarity with connected technology grows, we expect the rate of IoT adoption to grow. Therefore, the challenge facing government is what will happen once IoT use becomes more widespread.

11. Björn Hasselgren, *Government's role for transport infrastructure: Theoretical approaches and historical development*, doctoral thesis, KTH Royal Institute of Technology, Stockholm, August 26, 2013, www.diva-portal.org/smash/get/diva2:628222/FULLTEXT01.pdf.

12. Michael Raynor and Mark Cotteleer, "The more things change: Value creation, value capture, and the Internet of Things," *Deloitte Review* 17, July 27, 2015, http://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/value-creation-value-capture-internet-of-things.html.

13. The cost of the most recent upgrade to the GPS constellation alone cost more than $5.8 billion, not including the costs of previous satellites or R&D. See Mark Sullivan, "A brief history of GPS," *PC World*, August 9, 2012, www.pcworld.com/article/2000276/a-brief-history-of-gps.html.

14. Range of estimates taken from Amy Collins et al., "United States: The Internet of Things part 2: The old problem squared," Socially Aware, April 3, 2014, www.sociallyawareblog.com/2014/04/03/the-internet-of-things-part-2-the-old-problem-squared/; Gartner, *Forecast: The Internet of Things, Worldwide, 2013*, November 18, 2013.

15. UK telecommunications regulator OFCOM has repurposed 10 MHz of existing spectrum for IoT uses, while in the United States the FCC has both repurposed existing spectrum and taken advantage of new technology to open up previously unused buffer spectrum. For more information, see OFCOM, *VHF radio spectrum for the Internet of Things*, March 23, 2016, http://stakeholders.ofcom.org.uk/binaries/consultations/radio-spectrum-internet-of-things/statement/vhf-iot-statement.pdf; and Association of Professional Wireless Production Technology, "Using mobile duplex gaps and guard bands for PMSE," 2014, www.apwpt.org/downloads/using-mobile-duplex-gaps-and-guard-bands-for-a.pdf.

16. For the results of the Canadian auction, see Innovation, Science, and Economic Development Canada, "AWS-3—final results," April 30, 2015, www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10954.html; for the US auction, see Alina Selyukh and Malathi Nayak, "US wireless spectrum auction raises record $44.9 billion," Reuters, January 29, 2015, www.reuters.com/article/us-usa-spectrum-auction-idUSKBN0L227B20150129.

17. Adam Justice, "A quick guide to Internet of Things standards groups," Embedded Computing Design, July 31, 2014, http://embedded-computing.com/guest-blogs/a-quick-guide-to-internet-of-things-standards-groups/.

18. For information on existing standards, see Ian Brown, "Regulation and the Internet of Things," presentation to the 15th Global Symposium for Regulators, 2015, www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf.

19. Terry Hughes, "Will industry muscle win the IoT standards war?," IoT Agenda, April 24, 2016, http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Will-industry-muscle-win-in-the-IoT-standards-war.

20. Samantha Ehlinger, "Experts: Government should use IoT and enable its development, not over-regulate it," *FedScoop*, September 1, 2016, http://fedscoop.com/experts-government-should-enable-and-use-iot-not-over-regulate-it.

21. Under the 2009 Health Information Technology for Economic and Clinical Health Act, the US Office of the National Coordinator for Health Information Technology works to ensure interoperability of electronic health records, messaging formats, e-prescriptions, and other information.

22. Yves-Alexandre de Montjoye et al., "Unique in the crowd: The privacy bounds of human mobility," *Scientific Reports 3*, article number 1376, March 25, 2013, www.nature.com/articles/srep01376.

23. Michael E. Raynor and Brenna Sniderman, "Power struggle: Customers, companies, and the Internet of Things," *Deloitte Review* 17, July 27, 2015, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-customers-companies.html.

24. For more information, see the "Regulatory timeline" on regulations.gov, which discusses the process for creating a new rule by a federal agency and its inclusion in the *Federal Register*.

25. Gary E. Marchant, Douglas J. Sylvester, and Kenneth W. Abbott, "What does the history of technology regulation teach us about nano oversight?", *Journal of Law, Medicine, and Ethics* 37(4), Winter 2009.

26. European legal conceptions of privacy are built upon a fundamental right to privacy by which individuals "retain effective control over their information." (Věra Jourová, "How does the data protection reform strengthen citizens' rights?", European Commission Directorate-General for Justice and Consumers, January 2016, http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf.) On the other hand, the United States has no explicit right to privacy outside of certain protected cases such as

health records, and in fact, holds that any information publicly transmitted to a third party has "no reasonable expectation of privacy." (*Katz vs. United States*; see https://casetext.com/case/katz-v-united-states.) As a result, the United States tends to regulate privacy not as a fundamental right but as a contractual agreement between company and consumer.

27. Rolf H. Weber, "Governance of the Internet of Things—from infancy to first attempts of implementation?," *Laws* 5(28), June 24, 2016, www.mdpi.com/2075-471X/5/3/28.

28. Jonathan Weiner, "The regulation of technology, and the technology of regulation," *Technology in Society* 26, 2004, pp. 483–500.

29. Ehlinger, "Experts: Government should use IoT and enable its development, not over-regulate it."

30. Ibid.

31. James Donelan, "Stop making spaghetti: Removing custom code will ease heartburn," *Tech Beacon*, March 2, 2016, https://techbeacon.com/stop-making-spaghetti-removing-custom-code-will-ease-heartburn.

32. Bruce Schneier, "Security and function creep," Schneier on Security, January/February 2010, www.schneier.com/essays/archives/2010/01/security_and_functio.html.

33. Steven Krebs, "Hacked cameras, DVRs powered today's massive Internet outage," KrebsOnSecurity Blog, October 21,2016,https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

34. Angela Simpson, "Increasing the potential of IoT through security and transparency," National Telecommunications and Information Administration, August 2, 2016, www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.

35. Now known simply as UL, Underwriters Laboratory is a private safety consulting and certification company approved by the US Occupational Safety and Health Administration to perform safety testing.

36. In attempting to describe the mind-stretching aspects of quantum mechanics, physicist Erwin Schrödinger used the analogy of a cat trapped in a box with a radiation source and vial of poison. If a detector senses any radiation from the source, it smashed the vial of poison killing the cat. Schrödinger reasoned that after a certain period of time, the cat is both alive and dead, illustrating the concept of quantum superposition. When the box is opened, the superposition collapses, and only one state—alive or dead—is observed.

37. For more information on how touchscreen devices harness quantum mechanics, see this short lecture from Philip Moriarty of the University of Nottingham: www.sixtysymbols.com/videos/touchscreens.htm

ABOUT THE AUTHORS

JOE MARIANI

Joe Mariani is a manager in Deloitte Services LP's Center for Integrated Research, where he is series editor for Deloitte's research campaign on the Internet of Things (IoT). Mariani is responsible for examining the IoT's impact on a diverse set of issues from business strategy to technical trends. His broader research focuses on how new technologies are put to use by society and the organizations within it.

ACKNOWLEDGEMENTS

The author would like to thank **Bill Eggers**, **Jonathan Holdowsky**, **Brenna Sniderman**, and **Natasha Buckley** for their patience, help, and advice. A special thanks as well to **Matthew Budman** for his tireless efforts to improve the article.

CONTACTS

Bill Eggers
Executive director
Center for Government Insights
Managing director
Deloitte Services LP
+1 571 882 6585
weggers@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte