Anticipate, sense, and respond

Connected government and the Internet of Things

A GovLab report in the Deloitte
Future of Government series

Deloitte
University
Press

About the authors

Max Meyers is a GovLab Fellow and senior consultant in Deloitte Consulting LLP's Human Capital practice, where he focuses on workforce strategy—helping clients navigate emerging trends and harness the talent they need to do so. Before joining Deloitte, he taught high school, and his personal experience shapes his interest in bringing creative problem-solving approaches to bear on public sector challenges. You can reach him on Twitter at @TheMaxMeyers and by email at mmeyers@deloitte.com.

Claire Niech is a GovLab Fellow and senior consultant in Deloitte Consulting LLP's Strategy & Operations practice. Her experience at Deloitte includes policy analysis, strategy development, and advanced facilitation design and delivery for federal agencies, primarily in the homeland security space. You can reach her on Twitter at @ClaireNiech and by email at cniech@deloitte.com.

William D. Eggers, Deloitte Services LP, is responsible for research and thought leadership for Deloitte's Public Sector industry practice. He is the author of eight books, including his newest, co-authored with Paul Macmillan, *The Solution Revolution: How Business, Government, and Social Enterprises Are Teaming Up to Solve Society's Biggest Problems* (Harvard Business Press, September 2013). The book, which the Wall Street Journal describes as "pulsating with new ideas about civic and business and philanthropic engagement," was named to 10 "best books of the year" lists. His books have won numerous awards, and his commentary has appeared in dozens of major media outlets, including the *New York Times, Wall Street Journal, Washington Post, Guardian,* and *Chicago Tribune*.

Deloitte's Internet of Things practice enables organizations to identify where the IoT can potentially create value in their industry and develop strategies to capture that value, utilizing the IoT for operational benefit.

To learn more about Deloitte's IoT practice, visit http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/topics/the-internet-of-things.html.

Read more of our research and thought leadership on the IoT at http://dupress.com/collection/internet-of-things.

Contents

Introduction | 2

New tech, new value | 3

IoT applications in government | 7

Privacy and security | 13

Turning vision into reality | 15

Endnotes | 16

Acknowledgements | 19

Introduction

LONG before the advent of today's wrist wearables, Hollywood's James Bond was using his watch to measure radioactivity and receive messages from headquarters.[1] And before any company began prototyping connected cars, he careened through a high-speed chase where he controlled his car from the backseat via mobile phone—augmented by sensors that triggered fixes for safety issues such as flat tires and a video feed that alerted him to obstacles.[2] Previously the domain of fantasy, such devices are becoming reality and even mainstream: Smart watches help verify identity and pay for goods, alarm clocks know the current traffic, and smart glasses provide instant access to expert advice.

> "This wave of technology has more chance of reimagining whole swathes of the world than anything we've seen before."
>
> — Tim O'Reilly, quoted in Chris Witeck, "The Internet of Things (IoT): The best is yet to come," http://bit.ly/1TFHCr1.

What were once imaginative toys for a tech-savvy spy may soon be a new class of tools for public servants more generally. As governments work to deliver quality services in increasingly complex environments, devices that have already begun to make life easier and more efficient for companies and consumers can also help create greater public value.

However, strategic application of the Internet of Things (IoT)—the suite of embedded sensors and wirelessly connected devices—is still nascent in government. In fact, a recent Brookings Institution report found that not a single federal agency mentioned the IoT in its strategic plan.[3] The diverse nature of public sector missions and the citizens they serve frequently complicates attempts to implement new technology. Yet if public sector organizations do not start analyzing the implications of the IoT today, they risk being left behind, making it more difficult to effectively regulate or efficiently deliver services in this shifting reality.

This report aims to help government leaders navigate this emerging reality by providing an overview of how new IoT capabilities can create value, illustrating their impact on three traditional public sector domains (education, public safety, and utilities), and discussing a few considerations as agencies plan for adoption of this technology.

New tech, new value

THE definition of a "computer" is changing again. The continued evolution toward cheaper processors and faster networks has enabled a shift from desktop workstations to mobile phones and, now, to everyday objects, inspiring the term "Internet of Things." Almost any device can be Internet-enabled, linking it to additional computing power and analytic capabilities that make it "smart." The aggregation of outputs from sensors, beacons, machines, and other IoT devices offers far more value than just a better or "smart" product; by connecting these devices and environments, we can understand more about their use, the world, and ourselves—often in real time. As more complex and mature systems take advantage of this connectivity to tap into new capabilities, organizations must think about how these technologies combine to create value in new and different ways.

> Just as the first news shows treated television as "radio with pictures," many early IoT applications have considered only how these devices can improve current performance.

Many current IoT applications, however, simply enhance existing products and processes rather than rethinking them, creating limited value. Just as the first televised news shows featured an anchor reading the events of the day from a typed paper in his hand—treating television as "radio with pictures"—early IoT applications have considered only how these devices can improve current performance. Ultimately, the IoT represents a new way of working, where—as Kevin Ashton, who coined "Internet of Things," describes—machines and other devices supplant humans as the primary means of collecting, processing, and interpreting information.[4] This breaks many of the constraints that have traditionally defined fundamental business processes—from timing to availability of information—and asks organizations to think differently about how they create value.

Doing so may require a fresh approach to information collection and analysis—not simply "Big Data 2.0." Today, only 8 percent of companies are capturing and analyzing IoT data in a timely way, and 86 percent say that faster and more flexible analytics would increase the value of their IoT investments.[5] The current model of mass collection and exploratory analysis is likely unsustainable; instead of collecting all possible information for future analysis, we need to streamline information collection and develop focused rules to make insights actionable now. As Steven Fritzinger, public sector alliance manager for NetApp data management, explains, "Once sensors and networks are cheap, the temptation is going to be to put them everywhere . . . [but] it is going to be much more important to think about the problem."[6]

The CheckLight Sports Impact Indicator developed by hardware start-up MC10 provides an example of how tightly focused data collection can create insights and change behaviors. MC10 worked to develop a better way to test whether an athlete may have taken a dangerous hit to the head—and make it easier for coaches to decide whether to pull athletes off the field to check for concussions. CheckLight uses an accelerometer and gyroscope worn on an athlete's head to collect a few basic data points, and then uses algorithms to detect and determine an impact's severity. The results are shown through a light at the base of the athlete's head. A moderate impact triggers a yellow light; a severe impact triggers a red light. When tested with a football team in which coaches would bench players sustaining a red-light impact, MC10 found that the disincentive of sitting out plays changed athlete behavior: Players improved their tackling form, and head impacts decreased over the course of the season.[7]

A fresh approach to information collection and analysis—not simply "Big Data 2.0."

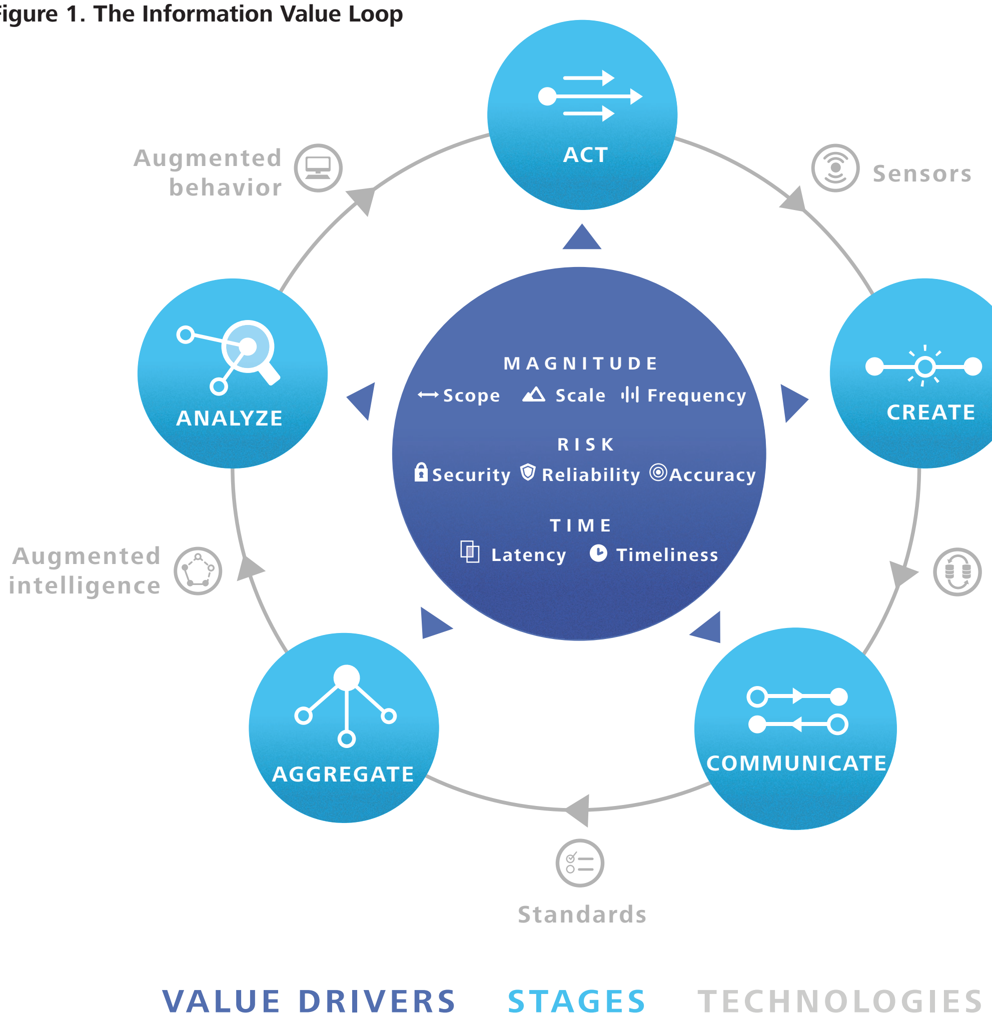
Organizations have the same opportunity to improve outcomes using technologies that provide immediate feedback and drive better decision making—but doing so can require that they orchestrate a complex system of sensors, processors, and actuators. The Information Value Loop (see sidebar, "The Information Value Loop—an overview") offers a blueprint for how the technologies at play in the IoT fit together to generate value. The value loop shifts the focus from what we connect to what we enable, accelerating the relationship between data and action—and enabling governments to more efficiently and effectively drive public value.

THE INFORMATION VALUE LOOP—AN OVERVIEW

Government agencies thinking about how to construct the Information Value Loop should consider five key capabilities: data creation, communication, aggregation, analysis, and action.

- **Create:** Sensors collect data on the physical environment—for example, measuring things such as air temperature, location, or device status.
- **Communicate:** Networks enable devices to share this information with other devices or a centralized platform.
- **Aggregate:** Aided by common standards, information from multiple sources is combined.
- **Analyze:** Analytical tools help detect patterns that signal a need for action, or anomalies that require further investigation.
- **Act:** Insights derived from analysis either initiate an action or frame a choice for the user.

Figure 1. The Information Value Loop



Graphic: Deloitte University Press | DUPress.com

Figure 2. Traditional versus IoT-enabled approaches to stages in the Information Value Loop

Action	Traditional	IoT-enabled
Create	Data is collected through analog means: surveys, ethnographies, etc.	Sensors passively measure or capture information with no user input
Communicate	Data is manually developed into a report and transmitted	Data is seamlessly transmitted among objects or from objects to a central point
Aggregate	Reports from different sources are brought together; an analyst determines what information is important	Data is aggregated as devices communicate with each other; prescribed rules determine what information is important
Analyze	An analyst frames a question and studies available data to arrive at a conclusion	Amplified intelligence detects patterns and variances across disparate data points and previously unrelated events
Act	Data is presented to an actor or decision maker who then determines how to proceed	Real-time signals make insights actionable, either presenting choices without emotional bias, or directly initiating an action

Organizations can accelerate the value they get from IoT data by extending this loop (adding capabilities they do not yet have) or addressing bottlenecks (improving existing capabilities).

IoT applications in government

"If the Internet of Things has to do with home automation or automation of the car [or] controlling devices like security systems through the Internet . . . what does [it] have to do with any of the service-providing departments of government?"[8]

Just like this respondent in a 2014 GovLoop survey, many people may wonder what the IoT has to do with government.[9] Admittedly, it may be difficult to see the immediate relevance of sport sensors or connected appliances, but deriving value from information collection and analysis is central to many government missions. The IoT can increase value by both collecting better information about how effectively public servants, programs, and policies are addressing mission challenges, as well as helping government deliver services based on real-time and situation-specific conditions.

Early government activity has coalesced around a few main areas, including "smart cities" focused on improving citizen services and federal agencies focused on scaling measurement capabilities. Local experiments include "smart parking" that helps commuters find spots (and streamlines city enforcement), and "smart waste" such as Big Belly Solar—Internet-connected trash bins that communicate their status to help optimize collection routes. New York City is even transforming public pay phones into Internet-connected pylons with the potential to someday broadcast emergency messages or provide places where New Yorkers can provide civic feedback on various topics.[10] At a federal level, agencies are more focused on scaling measurement capabilities: The Department of Defense uses RFID chips to monitor its supply chain more accurately,[11] the US Geological Survey employs sensors to remotely monitor the bacterial levels of rivers and lakes,[12] and the General Services Administration has begun using sensors to measure and verify the energy efficiency of "green" buildings.[13]

As in industry's early IoT-enabled work, many of these government applications focus on optimizing current operations rather than identifying how faster, more precise, and more reliable information might generate new possibilities for service delivery. To fully reap the IoT's potential benefits, public sector organizations will need to rethink how they do business—identifying new models for service and adopting the technology and the corresponding organizational structure(s) to support them. We explore the implications for a few classic public-sector domains and posit three ways in which these new tools might redefine work:

- Eliminate routine tasks: Teachers shift time from classroom procedures to personal instruction
- Enhance capabilities: Public safety officers respond faster and more proactively to emergencies
- Engage partners: Localities build an ecosystem for water conservation and security

Education: Shift time from classroom procedures to personal instruction

Of the 1,025 hours the average American student spends in the classroom each year, more than 300 are likely lost to interruptions. In fact, an estimated one of every five minutes is consumed by "anticipated interruptions": transitions, materials distribution, and starting or ending class.[14] Each minute a teacher spends managing large group procedures takes away from time he or she could spend on student interventions—such as differentiating instruction or developing students' socio-emotional skills—to help close an achievement gap between rich and poor students that has grown more than 50 percent since the late 1980s.[15]

How the IoT can help. Connected devices offer the potential to relieve teachers of some of the administrative burden in taking roll or distributing materials, allowing more time to focus on students' learning needs.

As students take their seats in a connected classroom, attendance could be logged automatically by a wearable "smartband" such as the RFID bands that many theme parks already use to check in to rooms, rides, and even find lost children.[16] A beacon might push a warm-up exercise directly to students' tablets or smart desks. And when it comes to keeping students on task, teachers could send a "haptic" vibration—similar to silent notifications on mobile devices—to a student's wearable or tablet, redirecting her attention or behavior in a way that limits public embarrassment and reduces direct confrontation.

Teachers, freed from managing many classroom procedures, could focus more fully on students—and perhaps focus more incisively too. Pattern-recognition software or data analytics applied to these new inputs might add to a teacher's contextual understanding, mapping the record of behavioral incidents against student stress levels, classroom temperature, or even the teacher's own actions. And IoT technologies could help translate these insights in real time—much like MIT Media Lab's MindRider, a bicycle helmet that picks up on 10 types of brain waves that signal activities like concentration or stress and produces a corresponding light to make drivers more aware of panic-inducing behavior.[17] In the classroom, using similar devices to identify which students are expending higher amounts of cognitive energy on an exercise could help teachers dedicate attention to students who need it the most—not just those who ask for help the loudest. Educators with years of experience often develop an intuitive understanding of such complex behavioral dynamics, but a connected classroom could provide insights even to the teacher just starting out.

Implications. Schools and districts looking to take advantage of these capabilities will need more than new technology—they must start by building a culture of digital literacy that can support greater *creation* and *communication* of data, to use the terms from the Information Value Loop. Creating these data requires that teachers use technology as a consistent part of instruction, and schools should empower teachers to decide which devices best fit their specific needs. This approach is a significant change from today's centralized technology budget and procurement process originally designed around computer labs, but districts that embrace opportunities for decentralized technology procurement—such as Idaho's cash-poor but forward-thinking West Ada district—have found that it presents an opportunity to encourage bottom-up experimentation and scale what works.[18] Perhaps counterintuitively, schools and districts should pair this move toward decentralized applications with investments in shared platforms. By providing common information security, data standards, and system monitoring, these platforms enable effective integration into school records and information management systems—and ultimately help communicate and aggregate IoT data.

Public safety: Respond faster and better to emergencies

Emergency response today suffers from information gaps and asymmetries, driven by how quickly and how well those affected are able to alert authorities. As a result, responders are often delayed; for example, in 2011, only 15 percent of Los Angeles 911 dispatchers successfully alerted Los Angeles Fire Department response units within the targeted 60-second timeframe.[19] Waiting for adequate information delays the response, yet responding too early risks endangering underinformed responders or committing unnecessary resources.

How the IoT can help. IoT applications can more quickly *aggregate* and *analyze* information about an event, helping responders better identify incidents, decide how to respond, and communicate decisions (and critical actions) to those involved.

Environmental sensors, for example, can register and report early indicators of an emergency or crime; already, devices such as ShotSpotter can detect the sound of a gunshot and pinpoint its location to within 10 feet. By automatically alerting police dispatch, the device can speed reaction time, as well as reduce reliance on witnesses to report crime, helping to detect crimes that might never have been reported. When police started using ShotSpotter in Camden, NJ, they found that 38 percent of gunshots in one neighborhood were not being reported.[20] Beyond detecting gunshots, data points from other sensors, cameras, and even databases can be aggregated to reveal incident patterns; much as PredPol or Palantir are used today to "hot spot" *where* crimes are most likely to occur, similar algorithms working on data from distributed sensors might be able to report *that* crimes are likely occurring. And these environment-generated alerts can be quickly directed to multiple parties, as PulsePoint, a San Francisco-based nonprofit that uses location-aware apps today to crowdsource CPR skills, does—alerting CPR-trained citizens who are within walking distance of reported incidents and allowing "citizen superheroes" to step in until professional first responders arrive.[21]

Connected devices can also improve officers' performance when responding to an incident. Connected firearms, for example, can track when and where an officer removes a weapon from its holster and discharges it. In the moment, pulling or firing the weapon could dispatch additional support; over time, the record could inform coaching and development discussions. Other wearables might augment these discussions, providing similar insight into officers' behaviors. Sensors that monitor officers' stress levels, heart rate, or voice volume could alert supervisors or fellow responders to elevated tension or other anomalies that might endanger an officer or bystanders, allowing quick intervention and, later, coaching and training on handling future situations. This has particularly powerful implications, as local public safety organizations increasingly play a role in crowd control or longer incident response.

Beyond enhanced alerts and officer performance, IoT applications can aggregate real-time information to provide greater situational awareness. As more cities incorporate smart infrastructure, for example, iPavement—a Wi-Fi- and Bluetooth-enabled paving material that can be embedded in sidewalks—could send out crime alerts or emergency messages to mobile phones located within a certain distance.[22] Or indoor beacons, such as those being deployed in Next Generation 9-1-1 systems,[23] could help direct responders to an exact floor and room. Emergency systems could also integrate this precise location data with local video and social media to give responders context well before they arrive at the scene: Local video from nearby cameras might be streamed directly to the dashboard of the responders' vehicle, and even mapped to streaming social media posts coming from the same area. For example, the police department of one major US city is already experimenting with combining video and social media with facial-recognition or social-network analysis software to help officers better investigate crimes and identify suspects.[24] While today this analysis occurs after the incident, IoT applications can provide real-time insight, moving from a model of prosecution to one of prevention—from *analysis* to *action*, the final stage of the value loop.

Implications. We rely on public safety officers to act as human sensors, naturally aggregating multiple sources of data to assess a situation. Moving forward, machine sensors will enable public-safety organizations to collect a wider array of real-time data, but effectively aggregating and analyzing this data will require new processes. Where many current processes rely on centralized analysis, for example, organizations may glean greater value by empowering offers to make decisions at a local level based on IoT-generated data. And where current systems assume that information moves in one direction, the advent of localized communications via beacons or Bluetooth can allow dispatchers to engage citizens in the area to help—reframing public safety as a shared responsibility.

Moreover, as public safety networks aggregate information from new sources—transit, utilities, or telecommunications—governments should advocate for and implement common data standards to ensure interoperability. Greater volume of and access to information can eliminate distance and accelerate response, but may ultimately require a more elegant understanding of how to properly bridge dissimilar types of data.

Public utility: Building an ecosystem for water security

The United Nations' 2030 Water Resources Group observes that, if current trends continue, the demand for water will exceed supply by 40 percent in 2030.[25] Already, in the United States, California is facing an extended drought and recently implemented water rationing, and the Ogallala aquifer that feeds the Plains States' agricultural communities is at historic lows. However, scaling solutions is difficult in a highly localized and fragmented system of more than 155,000 different US water-supply corporations. Little venture capital or corporate research and development is focused on the water challenge,[26] leaving it to government organizations to close the gap between water supply and demand—a task estimated to require $50 to 60 billion in annual investment over the next 20 years.[27]

How the IoT can help. IoT technology can provide greater comprehension of the complex challenges surrounding water security, enabling governments to better define priorities for water supply, consumer demand, and governance. Like other issues driven by multiple and diverse factors, improving outcomes for water management will require contributions from an ecosystem of partners, many of whom are not even aware of the role they play in water conservation. IoT applications can also help agencies better coordinate response among this set of players by capturing the specific impacts of each policy, not only through predictive models but also through real-time measurement that enables "lean startup"-style A/B testing.

Increasing water supply is often the first option considered as water inventories drop, and traditionally, companies have invested heavily in finding new sources of water—just as Midland, TX, recently spent $197 million to tap into a new source 67 miles away.[28] As new

sources dry up, however, utilities might instead focus on improving the yield for delivery; more than 40 percent of the infrastructure is over four decades old, and water-supply systems lose 16 percent on average during delivery.[29] One of the challenges the IoT could solve is determining exactly *where* to repair to improve yield—and whether the volume saved for that area will offset the capital cost of repair. Sensors can provide a more precise understanding of water flows and help prioritize improvements, even at the level of individual homeowners not typically engaged with the state of water infrastructure. Stopping or slowing in-home leaks, which can waste up to 10,000 gallons a year, can further boost the yield on sanitized water: Products such as LeakSmart, for example, combine a simple sensor and actuator to detect when a pipe has burst and shut off the water.[30]

Conserving water by lowering demand can also be a powerful way to extend limited water supplies. Boston provides an early example: When demand outstripped supply in the early 1980s, the city was able to avoid $500 million in capital infrastructure costs through a conservation campaign that led to a 43 percent reduction in water consumption.[31] IoT applications promise to make conservation campaigns even easier and more effective by tracking progress and offering—or even automating—new ways to conserve. Simply giving consumers more insight into when or where they use water and how they compare to neighbors can encourage conservation, as the Municipal Water Department in East Bay (California) recently demonstrated. Partnering with WaterSmart, the department saved 5 percent in water consumption by giving 10,000 customers access to a Web portal that showed how each stacked up against families of comparable size, as well as by providing ideas for improving water conservation.[32] An IoT system might further support conservation efforts by helping users understand where and how they use water most, and applying rules or reminders to domains such as showers, appliances, or pools. This real-time monitoring might even reinterpret the local "water tower" as a way to create a public display of progress—much like the Southern California Edison energy company distributed "energy joules" that glow different colors to help customers and businesses see the current demand on the grid.[33]

The greatest savings in water consumption can come from automating agricultural and municipal use: More than 70 percent of water consumption today is for agricultural use,[34] and 60 percent of the remainder goes to urban landscape maintenance.[35] In both instances, agribusiness companies often irrigate regardless of current conditions, risking overwatering rather than drought.[36] Sensors with advanced algorithms can help address both problems, aggregating measurements of soil moisture, heat, humidity, and slope to analyze how much water plants need. One startup, Hydropoint, has partnered with several landscape companies to install these systems for urban parks, golf courses, and corporate campuses. Hydropoint's system has cut the Los Angeles suburb Santa Clarita's irrigation costs by more than 25 percent and is projected to save the city approximately 180 million gallons of water annually.[37]

Implications. By creating greater insight into both supply and demand, IoT applications can help government and utilities work together to improve governance of the water ecosystem. However, information alone does not make the water system more efficient: Localities may need to build behavioral and technical foundations to allow people to *act* on information. For example, knowing how customers respond to various scenarios can shape tailored prompts and change behavior around water use. Similarly, servo valves can automatically take action to shut off pipes once a rupture or leak has been detected.

Further, IoT-generated information and action can not only directly save scarce resources but also feed better planning and policy—including enabling decision making based on empirical data as opposed to political pressures. And if government officials and water companies can improve operations, they likely can boost profit margins and free additional capital to invest in additional innovation.

Privacy and security

THE three examples above are predicated on the collection, analysis, and use of large volumes of data, introducing a complex and controversial set of issues: the privacy and security of citizen data.

The proliferation of data created by IoT applications will almost certainly continue to generate concern over how government systems and employees handle that data. Early IoT applications have already sparked national debate and Senate hearings on privacy: One such hearing, a 2015 US Senate Committee on Commerce, Science, and Transportation hearing entitled "The connected world: Examining the Internet of Things," addressed "how to strike the appropriate balance between encouraging IoT innovation and protecting privacy and data security."[38] Driving public acceptance of government application of IoT technology will likely mean proactively framing the discussion of "privacy" around concepts of "value, security, and trust."

Deliver value to citizens. Our society is accustomed to exchanging data for valuable services. From Facebook to fitness trackers, users continue to grant companies access to their data if they feel they are realizing value in return.[39] This seems to hold true for government applications as well: US Customs and Border Protection's optional Global Entry program, which provides participants an expedited customs experience, has 1.8 million members and receives 50,000 new applications every month, despite requiring sensitive personal information—beyond that required for a passport—to enroll, including fingerprints.[40]

Make security a priority. Given their intrinsic responsibility to protect the public interest, public sector organizations are uniquely positioned to help develop a secure IoT; where private companies must balance profit incentives, government's core mission is naturally aligned with safety and security. Gilad Meiri of Neura, a platform designed to integrate the management of IoT devices, agrees: "The market is not asking for security and privacy. Start-ups are focused on acquiring customers over designing for security."[41] To fill this gap, governments should lead, incentivize, and often own the development of airtight solutions that can advance security in both public and private sector applications. As Kerry O'Connor, chief innovation officer for the city of Austin, notes, "This is not a commodity we're acquiring. This is something we need to design and work iteratively."[42] One potential approach to security that has gained recent popularity—championed by thinkers such as Marc Goodman, author of Future Crimes—is the idea of addressing security in the same way as public health, focusing on educating the public, tracking symptoms, and isolating outbreaks quickly.[43] This model looks to improve resiliency by shifting focus from "who's getting in to what's getting out."[44]

Build trust through transparency. Government organizations, perhaps even more so than industry, have a responsibility to their users, and should offer transparency—for example, being clear on what data are requested, how the data are being used, and who will see the data. A director of policy for one mobile cybersecurity company frames this in terms of "surprise minimization": the idea that "a user should never be surprised by what an organization is doing with his or her data."[45] Transparency helps users feel they have control over their inputs, and it should also give them a choice over their outputs, which generally makes people more likely to use a service. In fact, in a 2014 study, 80 percent of users said they would be willing to provide personal information to a "trusted brand."[46]

Government organizations can look to a few current initiatives for practical ways to build in these concepts while implementing new IoT applications (figure 3).

Figure 3. Approaches to managing security and privacy in government IoT applications

	1 Deliver value in exchange for information	2 Make safety a priority	3 Keep citizens informed
How can government act?	Give citizens tangible benefits in exchange for using their data.	Lead on developing a secure IoT—through direct development and acquisition, and by acting as a convener.	Build trust by being clear when constituent data is collected and explaining how it will be used. Public sector organizations can also ensure that citizens understand laws and regulations around device security and data privacy.
Where do we see this today?	**TSA Pre✓**: Administered by the Transportation Security Administration, the Pre✓ program allows registered travelers to go through expedited screening lanes at the airport, allowing them to move through the airport more quickly. To enroll in the program, travelers submit biographic and biometric data and pay a fee.	**Hague Security Delta (HSD):** Headed by the Dutch government, the HSD is the largest security cluster in the world, bringing together governments, businesses, and industry experts to develop innovations in technology security. The HSD focuses on cyber security, forensics, national and urban security, and critical infrastructure.	**Consumer Finance Protection Bureau (CFPB):** CFPB regulates private financial institutions while also educating consumers about financial products. CFPB works to reduce complexity in the financial products market, so consumers clearly understand the ramifications of their financial choices.

Turning vision into reality

ONE thing is certain: Government agencies that adopt a wait-and-see attitude toward the IoT are unlikely to develop the expertise or engender the trust needed to effectively and efficiently deliver services in this new reality and to reassure citizens concerned about how this new technology will affect them.

On an organizational level, public sector leaders ready to start tapping into the potential of IoT technology can begin by identifying specific, pressing mission challenges, and then analyze how more or better information, real-time analysis, or automated actions might help address them. By solving for concrete problems, governments can more effectively identify the technical, organizational, and talent changes necessary to realize new benefits—and scale what works.

At the US federal level, additional changes may include organizations such as the Office of Management and Budget or the General Services Administration working across agencies to avoid creating the siloed or incompatible systems endemic to previous technology transformations. And organizations such as the National Institute of Standards and Technology and the National Information Exchange Model may work with industry to create standards and ensure interoperability, particularly important given that data integration is foundational to the IoT's value proposition.

Beyond the tactical changes for organizations and broader government policy, governments can be particularly sensitive to the potential social implications of IoT applications. As the data from IoT devices offer new insights, they may also usher in new social complexities. For example, the ubiquity of these data can lead to the potential to discriminate by using algorithms to automatically categorize, make decisions, or treat people differently—without an appreciation for the social, economic, or racial factors at play.[47] Understanding such social risks up front is key to the design of effective public IoT applications.

Ultimately, the IoT is not simply a cool new technology but an inflection point in how we do work, structure businesses, and govern the resulting economy and society. David Bray, 2015 Eisenhower Fellow and CIO of the Federal Communications Commission, recognizes the public sector's crucial role in this transition: "empowering consumers to make choices, encouraging new [IoT] partnerships across private sector and public sector organizations, and exploring new ways to increase [IoT] privacy and resiliency by design [that] will encourage a future with more beneficial opportunities for us all."[48] Government agencies need to be active players to understand and shape this future—and should start today.

Endnotes

1. One of the original James Bond gadgets, a Geiger counter in a watch, is a holdover from the books and appears in several movies. Continuing the theme, watches with teletypes, tracking beacons, and televisions appear in at least three separate films.
2. In *Tomorrow Never Dies*, Bond uses a smartphone to drive his custom BMW from the back seat and to control weapons and tire inflation. He is even able use this system to improve his customer experience and "returns" the car by using the phone remotely to drive it off a roof and onto the rental-car lot below.
3. Kena Fedorschak, Kevin C. Desouza, and Gregory Dawson, "Federal agencies behind the curve: IoT and BYOD," *Brookings TechTank*, March 16, 2015, www.brookings.edu/blogs/techtank/posts/2015/03/16-iot-byod-government-computers, accessed April 10, 2015.
4. Kevin Ashton, "That 'Internet of Things' thing," *RFID Journal*, June 22, 2009, www.rfidjournal.com/articles/view?4986, accessed November 12, 2014.
5. ParStream, "Internet of Things meets big data and analytics: A survey of IoT stakeholders," March 3, 2015, http://sites.parstream.com/parstream-iot-survey-whitepaper, accessed June 14, 2015.
6. Catherine Andrews, *The Internet of Things: Preparing yourself for a connected government*, GovLoop, 2014, www.govloop.com/wp-content/uploads/2014/07/GL-Internet-of-Things-Guide-.pdf, accessed October 11, 2014.
7. Rav Sheth, "Designing for 24/7 wearability," presented at Designers of Things Conference, San Francisco, September 24, 2014.
8. Catherine Andrews, *The Internet of Things: Preparing Yourself for a Connected Government*.
9. Govloop is an online social network for people who work in, study, or are involved with government.
10. Kyle Vanhemert, "NYC's new pay phones will provide super-fast wifi—and super-smart ads," November 19, 2014, www.wired.com/2014/11/new-york-linknyc-free-internet, accessed July 20, 2015.
11. *Defense Industry Daily*, "RFID daily: Keeping track of DoD's stuff," July 13, 2010, www.defenseindustrydaily.com/RFID-Technology-Keeping-Track-of-DoDs-Stuff-05816/, accessed November 12, 2014.
12. Ohio Nowcast: A daily nowcast of recreational water conditions, "The Ohio Nowcast for the Cuyahoga River," www.ohionowcast.info/nowcast_cuyahoga.asp, accessed May 12, 2015.
13. GSA Public Buildings Service, *Green building performance: A post occupancy evaluation of 22 GSA buildings*, www.gsa.gov/graphics/pbs/Green_Building_Performance.pdf, accessed July 20, 2015.
14. Donald C. Orlich et al., *Teaching Strategies: A Guide to Effective Instruction* (Belmont, MA: Wadsworth Cengage Learning, 2014, 10th ed.) p. 336.
15. Sabrina Tavernise, "Education gap grows between rich and poor, studies say," *New York Times*, February 9, 2012, www.nytimes.com/2012/02/10/education/education-gap-grows-between-rich-and-poor-studies-show.html?_r=2, accessed May 12, 2015.
16. Cliff Kuang, "Disney's $1 billion bet on a magical wristband," *Wired*, March 10, 2015. www.wired.com/2015/03/disney-magicband, accessed July 17, 2015; Ann Bednarz, "RFID everywhere: from amusement parks to blood supplies," *Network World*, May 3, 2004, www.networkworld.com/article/2333045/access-control/rfid-everywhere--from-amusement-parks-to-blood-supplies.html, accessed July 20, 2015.
17. Madhumita Venkataramanan, "Brain-reading bike helmet shows how stressed you are," *Wired*, November 8, 2012, www.wired.com/2012/11/mit-media-lab-bike-helmet, accessed July 17, 2015.

18. Reed Stevens, "Innovation starts in the classroom," *Digital Promise*, www.digitalpromise.org/blog/entry/a-teacher-driven-approach-to-21st-century-learning-in-meridian, accessed July 20, 2015.
19. Robert J. Lopez and Ben Walsh, "LAFD looks at ways to speed up emergency response times," *Los Angeles Times,* November 20, 2012, http://articles.latimes.com/2012/nov/20/local/la-me-1121-lafd-response-20121121, accessed March 12, 2015.
20. Crime-sensing microphones hear, locate gunshots," *CBS News*, January 12, 2015, www.cbsnews.com/news/crime-sensing-microphones-hear-locate-gunshots/, accessed May 19, 2015.
21. PulsePoint, "Overview," www.pulsepoint.org/pulsepoint-respond/, accessed May 19, 2015.
22. Eric Mack, "iPavement adds apps to the ground beneath your feet," *CNET*, April 25, 2012, www.cnet.com/news/ipavement-adds-apps-to-the-ground-beneath-your-feet/, accessed March 9, 2015.
23. National Emergency Number Association, "NG9-1-1 Project," www.nena.org/?NG911_Project, accessed June 11, 2015.
24. Zachary Tumin, "Digital law enforcement," presented at Suits & Spooks Conference, Washington, DC, February 5, 2015.
25. *Charting our water future: Economic frameworks to inform decision-making*, 2030 Water Resource Group, 2009, p. 5, www.2030waterresourcesgroup.com/water_full/Charting_Our_Water_Future_Final.pdf, accessed February 26, 2015.
26. Newsha K. Ajami, Barton H. Thompson Jr., and David G. Victor, *The path to water innovation*, The Hamilton Project, October 2014, p. 14, figure 4, www.hamiltonproject.org/files/downloads_and_links/path_to_water_innovation_thompson_paper_final.pdf, accessed March 19, 2015.
27. *Charting our water future*, p. 18
28. Tom Arrandale, "Drought plagued regions struggle to conserve water and make money," *Governing*, July 2014, www.governing.com/topics/transportation-infrastructure/gov-drought-water-revenue.html, accessed April 12, 2015.
29. US Environmental Protection Administration 2013; Maxwell 2013.
30. Eamon Kunze, "LeakSmart can automatically shut off your water if a pipe burst in your house," *WT VOX*, November 27, 2014, https://wtvox.com/2014/11/leaksmart-can-automatically-shut-off-your-water-if-a-pipe-burst-in-your-house/, accessed February 28, 2015.
31. Sandra Postel, "Lessons from the field—Boston conservation," *National Geographic*, http://environment.nationalgeographic.com/environment/freshwater/lessons-boston-conservation, accessed March 21, 2015.
32. Steve Towns, "A little neighborly competition can help reduce water usage," *Governing*, March 2014, www.governing.com/columns/tech-talk/gov-keeping-wown-with-the-joneses.html, accessed March 8, 2015.
33. David Rose, *Enchanted Objects: Design, Human Desire, and the Internet of Things* (New York: Scribner, 2014), p. 81.
34. Igor Shiklomanov, *World water resources and their use*, State Hydrological Institute and United Nations Educational Scientific and Cultural Organization, 1999, table 18, http://webworld.unesco.org/water/ihp/db/shiklomanov, accessed April 28, 2015.
35. The Corporate Social Responsibility Newswire, "HydroPoint subscribers reduce water use and energy demand," August 11, 2009, www.csrwire.com/press_releases/27456-HydroPoint-Subscribers-Reduce-Water-Use-and-Energy-Demand, accessed February 24, 2015.
36. Initial research suggests that increased data about plant and soil conditions can reduce the risk of both over- and under-watering, enabling more efficient use of water resources. For example, see R. J. Bailey and E. Spackman, "A model for estimating soil moisture changes as an aid to irrigation scheduling and crop water-use studies," *Soil Use and Management* 12, No. 3 (September 1996), pp. 122–28.
37. HydroPoint, "Santa Clarita gets smart to cut costs in irrigation," www.hydropoint.com/santa-clarita-gets-smart-to-cut-costs-in-irrigation/, accessed July 20, 2015.
38. *Inside Privacy*, "Senate holds Internet of Things hearing," February 12, 2015, www.insideprivacy.com/about, accessed April 16, 2015.
39. Ibid.

40. "CBP announces reciprocal arrangement with Germany for trusted traveler programs," CBP Press Release, December 29, 2014, www.cbp.gov/newsroom/national-media-release/2014-12-29-000000/cbp-announces-reciprocal-arrangement-germany, accessed Feb. 17, 2015.
41. Gilad Meiri (founder and CEO, Neura), interview at Neura offices, September 25, 2014.
42. Dr. Reginald Brothers, Dr. Robert Griffin, and Kerry O'Connor, "Reinventing government R&D to save lives," presented at South by Southwest Interactive Festival 2015, Austin, TX, March 13, 2015.
43. Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It* (New York: Doubleday, 2015).
44. Jeffrey Carr, Max Meyers, and Claire Niech, "What the IoT means for public safety," presented at South by Southwest Interactive Festival 2015, March 17, 2015.
45. Deepti Rohatgi, Gautam Hans, and Jon Callas, "Privacy matters: Baking privacy into your apps," presented at South by Southwest Interactive Festival, March 15, 2015.
46. "Study: 80 percent of U.S. consumers willing to give personal info to 'trusted brands,'" March 4, 2014, http://washington.cbslocal.com/2014/03/04/study-80-percent-of-us-consumers-willing-to-give-personal-info-to-trusted-brands/ , accessed March 18, 2015.
47. Seeta Peña Gangadharan, *Data and discrimination*, Open Technology Institute, October 27, 2014, www.newamerica.org/oti/data-and-discrimination/, accessed May 3, 2015.
48. David Bray, "Democracies and the Internet of Everything," *FedScoop*, February 25, 2015, http://fedscoop.com/democracies-and-the-internet-of-everything, accessed March 7, 2015.

Acknowledgements

We are grateful to our colleagues who generously contributed their time and insights to this report. **Carmen Medina** of Deloitte Consulting LLP advised us through all phases of our research, always willing to engage with each barrage of new ideas and intuitively pick out the most promising pieces. Our thinking and writing benefited from her mentorship, and this paper would not have been the same without her critical and much-appreciated guidance.

Several Deloitte colleagues also provided invaluable feedback on our research. Thanks to GovLab leadership, including **Mark White**, global CTO for Deloitte Consulting LLP, and **Shrupti Shah**, Deloitte Consulting LLP director, as well as the Deloitte Services LP IoT Eminence Campaign team, particularly **Michael Raynor**, US Eminence director, and **Joe Mariani**, lead market insights analyst, for their insights and input.

We would also like to thank those outside Deloitte whose thoughts and expertise shaped our research: those at numerous start-ups and others working to bring the IoT to market who agreed to be interviewed, the researchers at the **MIT Media Lab,** and the excellent speakers at the 2015 South by Southwest Interactive Conference.

Lastly, we would like to thank our GovLab colleagues for the countless conversations and for creating a culture of innovation. We benefited greatly from your companionship and insights. GovLab was a place that never failed to support us and push us to refine our thinking, and for that we are grateful.

About GovLab

GovLab is a think tank in the Federal practice of Deloitte Consulting LLP that focuses on innovation in the public sector. It works closely with senior government executives and thought leaders from across the globe. GovLab Fellows conduct research into key issues and emerging ideas shaping the public, private, and nonprofit sectors. Through exploration and analysis of government's most pressing challenges, GovLab seeks to develop innovative yet practical ways that governments can transform the way they deliver their services and prepare for the challenges ahead.

Contacts

William D. Eggers
Director
Deloitte Services LLP
+1 571 882 6585
weggers@deloitte.com

Max Meyers
Senior consultant
Deloitte Consulting LLP
+1 703 395 9640
mmeyers@deloitte.com

Claire Niech
Senior consultant
Deloitte Consulting LLP
+1 571 970 7333
cniech@deloitte.com

Deloitte University Press

Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.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 Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 200,000 professionals are committed to becoming the standard of excellence.