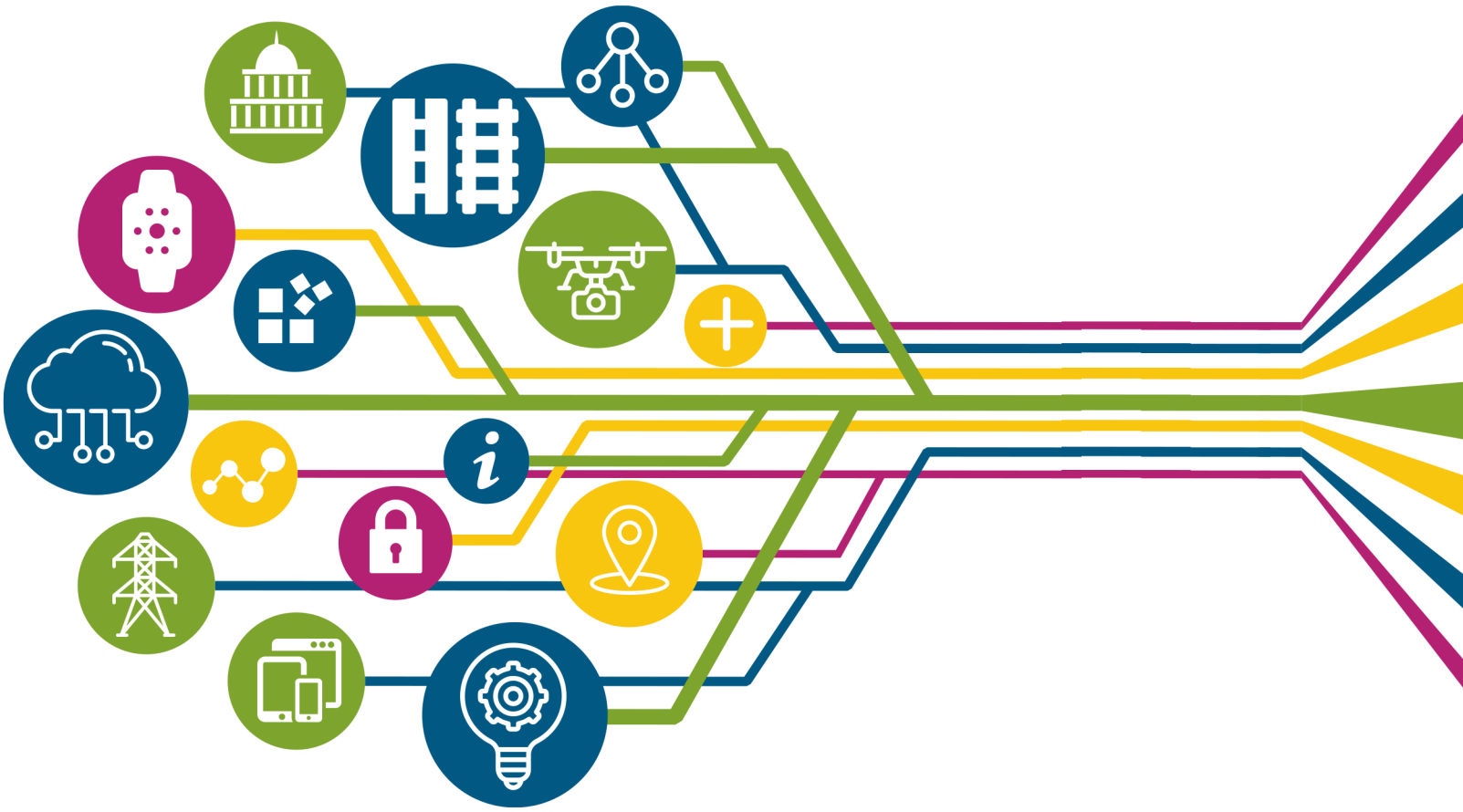
NASCIO

Value And Vulnerability:

The Internet Of Things

In a Connected State Government



When one hears the term “Internet-of-Things” (IoT) the mind immediately goes to refrigerators and coffee pots communicating with our smart phones, or wearables tracking our fitness, or manipulating home security systems or thermostats remotely. Case studies surrounding government use of IoT involve “smart cities” and sensors on parking spots, or the Department of Defense using RFID chips to monitor supply chain. So what does IoT mean to state government?

States are currently implementing IoT in a variety of ways. Schools and agency buildings are monitored in real-time for energy efficiency. Sensors and smart phone applications are monitoring traffic road conditions to provide updated information for drivers and increase safety. Connected devices in data centers can send information on heat or flooding instantly.

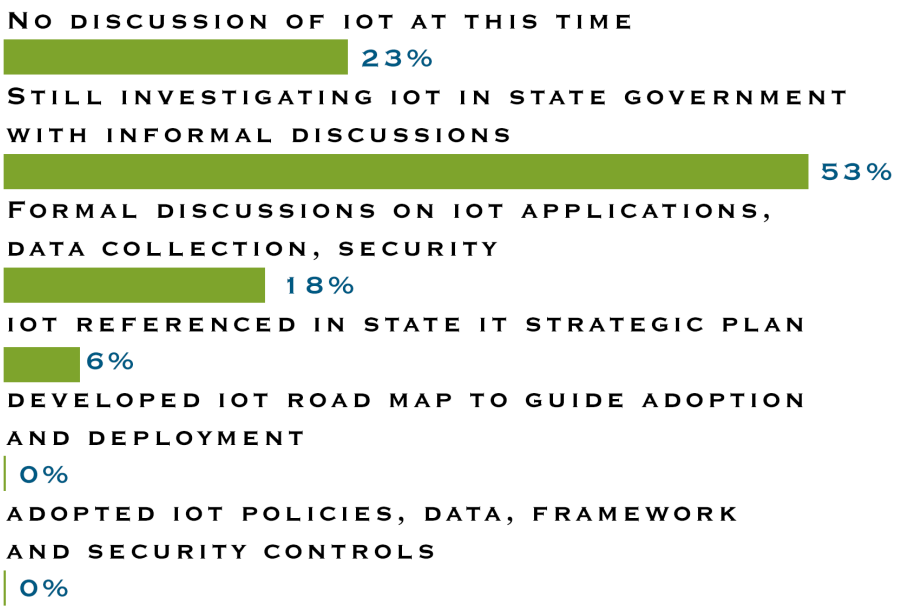
The possibilities are endless. Imagine a state where teachers save time calling roll thanks to wearable devices in the classroom. State police get back up automatically when a weapon is pulled. Car accidents are reduced thanks to smart cars that react faster than humans. Policy decisions are based on real-time information gathered through sensors.

States are implementing new technologies every day. Are they ready?

Considering IoT Policy

In 2015, the National Association of State Chief Information Officers (NASCIO) asked state chief information officers (CIOs) about IoT. While 53% of respondents said they were still investigating IoT with informal discussions, only 1 in 5 had moved to the formal discussion phase and zero states had adopted policies or developed an IoT roadmap.

To what extent is the Internet of Things on your agenda?



States certainly aren't as far along as cities in their development of an IoT roadmap. We hear about "smart cities" but not so much "smart states." A 2013 report from Cisco claims that two-thirds of global civilian benefits from IoT will come from cities in the next decade.[1] In some ways city services lend themselves more easily to connection (parking, waste management, public transportation), and cities can often move policy faster than states, but there are still opportunities for states to adopt IoT, and many are. While a state may not have a bus system to connect to an app, states may use sensor data, mobile platforms, or analytics software for healthcare, transportation or public safety.

Without specific policy on IoT, states will be caught unprepared to deal with the myriad of issues that can arise with increasing connectedness. There are issues of security, privacy, accessibility, data management and standardization, financing, legislation and bandwidth to consider. Before long we won't be talking about IoT, it will just be the way we do business. And states should get ahead of this new way of governing.

IoT in the States

Though the majority of states are only informally discussing IoT, or not discussing it at all, there are still some who are already implementing some innovative technological projects. The following are examples of ways that states can improve services in a connected world and how some are already doing that.

Transportation

IoT use for departments of transportation can result in better real-time driving information for citizens and government, safer roads, more efficient citizen services and innovative ways of paying for infrastructure. Most states now have a system to monitor speeds and road conditions and a corresponding website to share the information with citizens. States can also use IoT for more efficient fleet management.

- Oregon developed a pilot project using installed ports in cars or GPS to charge citizens for miles driven instead of charging a gas tax.[2]
- The Utah Department of Transportation is using Intelligent Transportation Systems to save lives, time and dollars. This includes closed-circuit television, variable message signs, traffic signal coordination, traffic monitoring systems, pavement sensors and weather sensors to provide real-time information to citizens through mobile apps.[3]

Health Care

There is vast potential for IoT in the healthcare realm from data analytics to home health monitoring to fitness trackers. States will want to consider how technology can improve both the health of their citizens and give the government a better understanding of habits or health issues of the populace while saving taxpayer dollars and protecting privacy.

- Texas and Illinois mandate (and many other states use) electronic visit verification for home health services—GPS systems are used along with smart phones and tablets to ensure health care providers are actually making required home visits, reducing fraudulently documented visits and ensuring better care for patients.[4]

Public Safety

Public safety officials are at the front-line of citizen safety and face danger on a daily basis. Not only can IoT enhance response times and safety, it can improve the safety of first-responders. The Center for Data Innovation recently submitted comments to the he U.S. National Institute for Occupational Safety and Health on the potential of sensors in emergency response activity.[5] The comments point out that not only can sensors reduce response times and locate victims, but they can prevent disasters from happening by alerting engineers that a structure needs repair.

- Ohio is working on Next Generation 911, allowing emergency service requests from a variety of communication methods and devices including text, VoIP and video.[6]
- The Florida Department of Highway Safety and Motor Vehicles uses dashboard cameras to collect footage for evidence in trials. Wi-Fi antennas have been installed around the state to reduce upload times to 20 minutes, saving the department $1.1 million a year in overtime.[7]

Tourism

States can get in on high tech tourism much like cities or private organizations. From apps to find state parks, to allowing citizens to get information about sites using a smart phone, there are a lot of fun possibilities.

- North Carolina is testing Bluetooth low energy wireless beacons at the state's museums, aquariums, historic sites and zoos. The beacons transmit contextual information to Bluetooth enabled smart phones and tablets.[8]

The uses for sensors and connected devices are limitless in state government. In addition to applications in transportation, healthcare, public safety and tourism, states can and are using IoT for a variety of other activities. States use sensors and mobile devices in facilities management to monitor and integrate heating, cooling, ventilation, security, refrigeration and lighting. Sensors can monitor water and air quality and track movement of wildlife to aid in environmental protection. Soil quality and droughts can be monitored and assessed using sensors for agricultural applications. Sensors can detect the start of a wildfire before it gets out of hand. Continuous monitoring of rivers, faults, mountains, bridges, oceans, buildings, and gas and water pipelines makes for more effective emergency management and better outcomes for citizens impacted in emergency situations. Beacons and sensors can be used to analyze the flow of foot traffic through a museum or event and help to usher people through in more efficient ways.

The Policy Framework

Obviously there is a wealth of opportunity for states to improve services and budgets using IoT. But along with the benefits come the concerns. This is where creating a roadmap or designing policy around the use of IoT will be useful before issues arise. If a state invests in sensors in all areas of government without a policy framework for how to use the sensors and collect the data, then at best they are a waste of resources and, at worst, a portal for disaster.

Security

One of the main concerns for states in an ever more connected world is security and data breaches. While private companies have the burden of balancing profit incentives with security, governments can really be the leaders of developing a secure IoT. Because sensors and the ability to connect objects is relatively inexpensive, states and consumers need to be aware of the security risks of purchasing such items outside of procurement guidelines as mentioned above. While IoT can create convenience, efficiency and savings, it can also create targets and vulnerabilities. Governments need to ensure that the data being collected doesn't provide information on government operations (which would be appealing to a malicious outsider). States must have a security policy for IoT specifically when developing an IoT roadmap.

Privacy

While privacy is a concern at every level of government, states are particularly concerned given the vast amount of information citizens are required to share with the state. One of the most important things a state can do is to be transparent. Citizens should know what they are sharing and why and should never be surprised that the state has certain information about them. People tend to be more willing to share information when they feel they are receiving a service or something useful in return (i.e. Facebook, TSA pre-check). On the flip side, states need to be mindful of the way they are collecting data from citizens when it is being collected by sensors or mobile devices. States should be aware of the vulnerability of this information and proactive about protecting it.

Data Management and Standardization

When a state department of transportation is gathering, saving and processing data one way and that state's department of health and human services is doing it differently, you end up with silos of data and no consistency. In September 2015, the National Institute of Standards and Technology (NIST) released a draft Framework for Cyber-Physical Systems.[9] The Framework, if enacted, may serve as a blueprint for secure, safe and compatible systems across the spectrum of IoT. In the meantime, states should consider interoperable systems of data collection and storage at the enterprise level. States will also need to think about storage. In an October 2015 paper, Cisco predicted that data generated by IoT would quadruple over the next five years resulting in over 500 zettabytes of traffic per year by 2019 and consuming 8.6 zettabytes of cloud storage.[10]

Funding and Investments

While some upfront costs are to be expected when implementing new IoT technology, in many cases states are seeking these solutions because they are cost-saving in the long run. For example, in Utah, each time a new road is built or repaired, the state includes fiber in the project to enable high speed connections. This kind of forward thinking increases the long term value of the project. Costs savings also come from more efficient practices or less waste or fraud. As the 2013 Cisco study predicts, IoT will create $4.6 trillion in value for the public sector globally in the next decade.[1] Cisco also points out that this value will come from benefits for agencies, employees and citizens; quantified citizen outcomes such as reduced crime; cost savings, increased revenues and productivity gains; and allowances for implementation and operational costs. CIOs should be ready to support this point when making the case for investments in technology.

The low cost of connecting "things" via sensors could raise some issues with procurement rules as well. State employees can buy sensors cheaply, avoiding procurement laws and therefore oversight. New guidelines surrounding procurement of sensors or beacons may need to be put in place.

Legislation

While legislatures may be tempted to enact legislation on IoT surrounding security, privacy and standardization, states should proceed with caution given how quickly technology is changing. It would be unfortunate to have legislation enacted only to become outdated in a few years, causing new problems. The FTC stated in a January 2015 report on IoT that legislation at this point would be premature for those reasons.[11] That said, many states have laws surrounding Internet security and privacy. The National Conference of State Legislatures tracks state legislation on issues such as constitutional privacy protections, automated license plate readers, event data recorders, and security breaches. [12]

Broadband

If, as some experts are claiming, tens of billions of devices will be connected to the Internet in the next few years, states may need to consider how that affects broadband and spectrum capacity. Some high-traffic areas are already reaching capacity for wireless signals—a problem that is sure to get worse. State's may want to consider improving broadband capacity state-wide ahead of the surge.

Emerging Trends in IoT

The market for IoT is on the verge of exploding in the next several years. One area that will emerge is a greater sophistication in securing the IoT. These immature technologies pose a greater risk than more "seasoned" technologies such as your work laptop. According to Gartner, as hackers find ways to attack devices the "things" will need updateable hardware and software to remain secure.

The market will also need to develop new ways of analyzing the vast amounts of data generated from connected devices. As Gartner points out, new tools and algorithms will be needed as the volume of data increases and the needs of IoT split from traditional analytics.

Other emerging trends on Gartner's list will include device management; low-power, short-range IoT networks; low-power, wide-area networks; IoT processors; IoT operating systems; event stream processing; IoT platforms and IoT standards and ecosystems.[13]

Advanced machine learning will also emerge as an important feature of connected devices. As computers and machines and connected devices become more intelligent they will be better able to predict and adapt.[14]

CIO Role

So, where to start? First of all, don't be a "wait-and-see" state. As a GovLab report[15] lays out:

> *"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…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."*

CIOs can also work at the enterprise level with agency heads or CIOs to develop standardization, avoiding silos and individual systems. Incompatible systems for IoT and data management will slow down the effectiveness and benefits of IoT for state government. CIOs should not understate the dollar value of IoT on the state budget. They can help legislators understand the cost-saving potential of IoT while cautioning against pre-mature legislation.

Recommendations

One thing is certain—the Internet of Things is here to stay. IoT applications will be both a boon and a burden for states. While creating immense value, there will be bumps along the way. Security, privacy, accessibility, standardization and citizen expectations must be managed carefully. NASCIO recommends that CIOs integrate IoT into their formal enterprise architecture discussions on asset management and risk assessment. Additionally, CIOs should craft an IoT roadmap to smooth the way for early adoption. CIOs should also take the time to learn from city, county and federal counterparts who may be further along in their usage of IoT. The time for formal discussion and planning for a connected state, citizenry and world is now.

Staff Contact:
Amy Hille Glasscock
aglasscock@NASCIO.org, 859-514-9148

Contributors
Doug Robinson, Executive Director, NASCIO
Meredith Ward, Senior Policy Analyst, NASCIO
Eric Ellis, Chief Technology and Innovation Officer, State of North Carolina
Dave Fletcher, Chief Technology Officer, State of Utah
Dan Lohrmann, Chief Strategist and Chief Security Officer, Security Mentor

(Endnotes)
1. Internet of Everything. A $4.6 Trillion Public-Sector Opportunity. http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf
2. Oregon Road Usage Charge. http://www.oregon.gov/ODOT/HWY/RUFPP/pages/index.aspx
3. Utah Traffic Management Division. https://www.udot.utah.gov/main/f?p=100:pg:0:::1:T,V:191,
4. GPS Cuts Fraud, Costs for Home Healthcare. http://www.informationweek.com/healthcare/gps-cuts-fraud-costs-for-home-healthcare/d/d-id/1317202
5. Center for Data Innovation Comments to the National Institute for Occupational Safety and Health. http://www2.datainnovation.org/2016-sensors-emergency-response.pdf
6. Next Generation 911 State of Ohio and Morgan County. http://www.nascio.org/portals/0/awards/nominations2015/2015/2015OH5-NASCIO%20OH%20NG%209-1-1%20Nomination%20FINAL.pdf
7. Public Safety, Justice and the Internet of Everything. http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-ioe-safety-justice.pdf
8. iCenter Beacon Technology. https://icenter.nc.gov/project/beacon-technology
9. NIST Draft Framework for Cyber-Physical Systems. http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm
10. Cisco Global Cloud Index. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html
11. Internet of Things. Privacy and Security in a Connected World. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
12. NCSL Digital Privacy and Security. Overview of Resources. http://www.ncsl.org/research/telecommunications-and-information-technology/telecom-it-privacy-security.aspx
13. Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018. http://www.gartner.com/newsroom/id/3221818
14. Check Out 10 Technologies that Could Change Your Life in 2016. http://www.techradar.com/us/news/world-of-tech/future-tech/10-hugely-important-it-trends-for-2016-1308808
15. Anticipate, Sense and Respond. Connected Government and the Internet of Things. http://dupress.com/articles/internet-of-things-iot-in-government/