CENTER FOR TECHNOLOGY IN GOVERNMENT
UNIVERSITY AT ALBANY State University of New York

The IoT Challenge for Local Governments as Data Stewards

By: Derek Werthmuller, Director of Technology Innovation & Web Services
A version of this issue brief was published on GovTech.com

Introduction

The 'Internet of Things,' (IoT) is all around us, every day and everywhere. The boardroom, courtroom, classroom, and coffee shop; wherever you go, people are sporting a smart watch they use as a phone, tracking their activity level with a bracelet, or even using a prescription bottle cap that reminds them when it's time to their medication. The uses across industries and sectors are seemingly endless and increasingly, local governments are taking notice and beginning to explore how they too might benefit.

Sensing, communicating, computing, controlling and informing are essentially what makes an IoT an IoT; the ability to have devices that connect to networks and generate data is the difference between an ordinary, run-of-the-mill device and something with the potential to be truly transformative. IoT networks

are made up of multiple complex systems working together, and in these networks, different system components are often designed and managed by different entities. The data generated from these 21st century devices travels from the device itself over networks, to be processed and used for a variety of purposes, sometimes even for critical decision making. IoT devices are part of a "Cyber-Physical System," defined by the National Institute of Standards and Technology (NIST) as "'smart' systems that are co-engineered interacting networks of physical and computational

components." And, as with any new technology, the IoT network and any cyber-physical system brings a new set of challenges that government leaders must be aware of as they consider how best to deploy such systems. They must consider that what is technically possible, may not be organizationally feasible or socially or politically desirable. The potential benefits of IoTs need to be matched by equally persuasive cautions about citizen privacy and greater vulnerability to malicious cyber-attacks, among others. Government's efforts to innovate with technology to provide public value should be balanced with the commitment to be good stewards of the public's data.

The big question local governments need to be asking themselves, is "are we prepared to steward the public's data in the context of IoT?" While there are some exceptions, we suspect that in many cases, the answer to that question is "no." Technology has evolved faster than the organizations trying to use them,

and public policies lag farther still behind organizational change. IoTs represent a new type of technology that, except in a few cases such as in New York City, is quickly outpacing the range of government structures and policies being used to manage IT investments as well as data collected. All governments considering the IoT, in particular local governments who are already struggling with data stewardship responsibilities, should carefully consider the following three issues.

IoT Technologies Blur Data Ownership

IoT data ownership is conflated by the mix of vendors needed to deploy and support an IoT network. Several models exist to finance, maintain and support an IoT network, and IoT devices can be purchased or paid for as a service. It's in this type of "IoT as a service model," that data ownership can become less clear, similar to how data in cloud computing services raises concern of data ownership and appropriate access. Different components or sections of the IoT network may be operated by different partners, each with their own interests. When IoT devices, communication networks, analytical tools, and storage systems are run as a service, the 'Terms of Service' agreements with the IoT system vendors may claim that they have both data ownership and use . And, when data from multiple sources and devices are combined and aggregated, it results in *new* types of data being created, making it difficult to identify the original source of specific data sets. Therefore, effective data stewardship by local governments relies on the government's ability to address data ownership from the perspectives of all the stakeholders involved. Once ownership is established and agreements struck about how to manage changes to the existing stakeholder mix, then effective stewardship practices can be put in place.

IoT Data is Vulnerable

An IoT device has three major components: hardware, operating system software, and the data it creates or senses. All three of these components are vulnerable to attack, perhaps even more so than other IT innovations due to the fact that IoT devices typically live outside of an organization's normal IT boundaries (both in a network firewall and physical location sense). This limits IT mangers' ability to use existing security infrastructure to provide security and management for IoT devices.

And, the security of the data is dependent on the security of the hardware and software generating it; hardware and software vulnerabilities contribute to data vulnerability. Furthermore, some IoT products are simply not equipped with high level computing capability, restricting the ability to encrypt and secure the devices and the data they generate. An additional challenge lies in the fact that the low powered, remotely connected devices that make up the IoT, including the software updates and configuration changes that manage the devices security, are generally harder to maintain.

Once data created from an IoT is transferred to central storage locations (usually either the cloud, city data center or office systems), it can become an additional hacking target that needs to be maintained and secured. For example, in 2015 several cities discovered that quite literally anyone could access the license

plate recognition cameras and therefore could also access the data; data that was already in use by the police departments in those cities.

IoT Challenges Current Assumptions about Privacy and Access

Sensors have the ability to collect many different types of data from a wide range of sources including people, environment, buildings, and machines. With this ability comes questions: What information are they collecting? How is the data being used? Who has access? With the large range of capabilities of sensors, and the networking capabilities to combine the data, sensors used in public spaces need a new set of rules to meet citizen and government expectations of privacy. Things such as who governs how the information can be shared and with whom and whether or not all public IoT sensor data or just the processed data should be made public on open data portals, are all factors that must be considered. For example, traffic light cameras use several video cameras pointing into an intersection in order to capture images of cars running red lights. These videos are quickly processed by computers that are trained to track changes in the street light and placement of cars. This process generates several different types of data including pictures of people in their cars, license plate information, and if a car ran a red light. Questions that should be considered here include what portion of this data should be kept by the local traffic authority and for how long, what is the data classifications for each of the different types of data, and can some (or all) of the data be sold or published on Open Data Portals?

Some Getting Started Advice for Local Governments Exploring IoT-Based Applications

As local governments begin to consider deploying cyber-physical systems whether in the form of new sensor networks on light poles and cameras on parking spaces or others, they must invest in new understanding of the accompanying policy and management infrastructure required to ensure that they continue to meet their obligations as stewards of the public's data. Put simply, local governments need to think holistically and in terms of capability when considering the IoT. To do so, local government officials should ask themselves the following five questions:

1. Do I, as a local government official, understand my responsibilities as a steward of the public's data?
2. Do I, as a local government official know the capabilities of my team with respect to data stewardship?
3. Am I, as a local government official, fully aware of the implications of the purchase and use of IoT-based applications in terms of my role as a public data steward?
4. Is the policy, management and technology infrastructure in my local government robust enough to be responsive to the changing conditions under which data is collected, effectively manage that data, secure access to it and permit appropriate access and use?
5. Does my local government have an action plan for ensuring that data is secure and where appropriate, privacy protected, while also ensuring the level of access and use that policy allows?
6. Does my local government have the resources to fill any related capability gaps?