CALYTERA

Building a Truly Smart Community

Principle Four: Provide Security and Transparency

GOVTECH SOLUTIONS SERIES

As communities continue their quest to become “smart,” government professionals need to carefully think through a number of technological, budgetary, and policy-related decisions to ensure that the smart communities they create benefit their citizens.

One of the most important considerations is how data collected by smart community systems and solutions will be protected. In this Solutions Series paper, we focus on the fourth principle of creating a truly smart community – providing robust data security and transparency about data management and usage.

Smart communities build systems with robust security to prevent access by bad actors and are open and transparent about the rules for using the data.

In an era when there is more data than ever, governments must address concerns and gain citizen trust in how data will be used and managed, especially as smart communities are being developed. Consumer awareness of and concerns about data privacy and security are higher than ever, particularly as high-profile data breaches continue.

Much of this consumer awareness tends to focus on how businesses are using consumer data. Consumer relationships with businesses around this issue are complicated, but trust has eroded over time. The 2017 PwC U.S. Protect.me Survey showed that nearly 7 in 10 consumers (69 percent) believe companies are vulnerable to hacks and cyberattacks. And, only 25 percent of consumers believed that most companies handle their personal data properly. Significantly, 85 percent of respondents reported that cybersecurity and privacy risks are among the biggest risks facing society today.

Consumers’ relationships with governments around the issue of data privacy and security are also complex. While consumers want governments to digitize services, their trust in governments’ management of data security is low.

One key reason is the number of data breaches that governments have experienced. According to a research conducted by cybersecurity firm Comparitech, U.S. governments have experienced 443 data breaches since 2014, with 2018 being the worst year on record. These

breaches are especially concerning for citizens given the personal data that governments need and have about them such as drivers' license numbers, personal contact information, financial records, and more.. According to a 2017 survey by Pew Research Center, about half of consumers (49 percent) feel that their data is less secure than it was five years ago. Tellingly, 28 percent of Americans are not confident at all that the federal government can keep their personal information safe and secure from unauthorized users.

The advent of Internet of Things (IoT) devices and sensors – especially those used by governments in infrastructure – vastly increases the data about our everyday actions and movements to which governments have access. Combining individual data about movements and actions with the huge amount of available data about online habits, consumer preferences, personally identifiable details, and more opens a Pandora's box of potential issues about the continuing erosion of personal privacy. If not carefully managed and planned for, government access to this data will likely erode citizen trust in governments' use and management of data even further.

Previous papers have discussed how many state and local governments' smart community efforts and use of IoT are focused on three key areas. The first is infrastructure, which includes projects like better aligning traffic signals to improve traffic flow and cut commute times and making street lights "smarter" to conserve energy. Second is projects that enhance public safety. Examples include using sensors to monitor air and water quality to protect citizens and make real-time changes (such as removing extra cars from the road on a low air-quality day) when needed and preparing for the potential dangers of natural events like storms and earthquakes to protect citizens. The third is actioning the data of smart city operations to inform decisions about where best to invest money in future infrastructure so that communities attract growth and provide a good quality of life to citizens.

The installation of IoT sensors in public infrastructure is the area that will both generate much more data about citizen movements and is most vulnerable to data security breaches and violations of privacy if proper precautions are not taken.

There are several things that government CIOs and technology professionals can do to meet the fourth principle while building smart communities.

First, systems designed to capture and collect data must have the highest level of end-to-end security possible. Encrypting data once it reaches a master dataset inside a government's operations is important. But that alone won't ultimately secure information from IoT devices in infrastructure if that data is broadcast on an open network – in fact, that's an open invitation for hackers. Keep in mind that networks of the future, especially ones with

artificial intelligence (AI), will perform many operations with edge computing. All parts of any system must be protected with industry-leading encryption and security practices.

Second, government professionals managing these systems should receive robust data security training. The Comparitech survey about government data breaches showed the majority of those resulted from human error rather than cyber-attack – mostly due to phishing scams. The most robust security on an IoT network won't be effective if an untrained government employee unintentionally gives a bad actor access to data about citizen movements. Government CIO partnership with their HR colleagues is key to the success of this effort.

Third, it is essential to plan for systems that ultimately rely on metadata and patterns to make decisions and changes. Systems should be designed so that in the data generated by one citizen's movements tracked by IoT sensors is not of direct value to a government. Rather, when strategic decisions are made based on patterns and data from the movements of many individuals, governments can help secure the privacy of each individual. Important decisions, such as how long data should be retained, how to ensure individual data is not tracked, and more must be made when smart community projects are being designed.

Fourth, complete transparency with the citizens is paramount. Once the hard decisions about planning the system are made, it is easier to clearly inform citizens exactly how data will be used and protected, and what "rules of the road" will be followed. Equally important is informing citizens that government professionals with access to data have received sufficient training on how to protect it. Clear communications can help head off any objections that citizens may have when smart community efforts are planned and funded which can help lead to success. Additionally, the metadata collected and created may have monetary value in the future – which can help pay for smart community initiatives. That makes it even more critical that there are clear rules for how individual data is protected and that governments are completely transparent with citizens about how this data will be managed once it is passed to a third party.

A close partnership between the IT and Communication departments in a government is critical for the creation of robust and transparent communications with citizens. It's equally important that leaders in that government, including elected officials, are well informed about and can clearly describe how citizens and their data are being protected.

Citizens increasingly expect their community to be "smart." Achieving that goal can be a challenging one for government professionals. Careful planning, following the four principles,

and clearly communicating goals, processes, and plans to citizens can all help guarantee success for any smart community initiative.

If there are topics you would like to hear about in future GovTech Solutions Series papers, let us know!

If your government is ready to build a smart community, we would love to help. Contact us today to set up a demo of our Amanda Platform, or to take a preview before we talk, visit our short Amanda product overview video.