U.S. House Energy and Commerce Sub-committee on Digital Commerce and Consumer Protection

Hearing: “Disrupter Series: Smart Communities”

Statement for the Record:

David J. Bressler, Vice President, API Management Solutions

CA Technologies

March 16, 2017
10:00 a.m.

There's a nuance to the source of the application economy's magic that many overlook. It's not about the app store, not about the ability to easily find and download an app for anything. It's about the creation process.

There are billions of mobile computers in people's pockets. That means there is an army of incredibly talented developers creating experiences. It's into this that smart cities are going to emerge as a platform for creative types to integrate into the mobile economy.

The short-term benefit of automation, or reduced cost of data collection, or more data, is just setting the stage. The real benefit comes when industries are able to do things that are different from the past because of the smartness embedded in the infrastructure. These ideas will not necessarily come from the people who are lighting up the city, but from others who experience the city and want to make it a better place.

In a world of "smart cities" anyone, anywhere in the world, can create an application or "experience" using the world's smart city infrastructure as the starting point.

In New York, some of the subways have sensors and commuters can see how long they have to wait in the station. This kind of information is available elsewhere in the world, like France who are also building a bus tracking system to provide real time information on location and time to arrival of buses in India. What should tracking subways or busses make news? It seems obvious that operators should use GPS to track them, and determine arrival times.

What's interesting isn't just tracking buses. The really exciting angle is the future, when bus data becomes available through secure APIs for people who want to create new commuting experiences.

Individuals who have a multi-hop commute would use schedules, current traffic conditions and expected traffic patterns based on history, and commuters could get an alert of the best bus to catch to minimize the commute across multiple hops and the waits between hops.

The city itself might not create such an app, but the smart-city platform creates the opportunity for the app to be created. Such an app might be best created by the person who experiences the commute (and knows the tricks), rather than someone who sits in an office imagining what such a commute is like.

CA Technologies recommends that communities focus on platforms and security when considering new initiatives to leverage "smart" technologies to unlock innovation.

First, communities should make public information and data accessible through read-write Application Programming Interfaces (APIs).

Healthcare IT provides a useful example. FHIR - Fast Healthcare Interoperability Resources - is an Application Programming Interface (API) standard that uses the JavaScript Object Notation (JSON) standard to represent data. FHIR has captured the imagination of a global pool of developers who see opportunities to innovate in healthcare. This represents a "bottom's up" approach to building a platform for healthcare innovation. A similar approach can be leveraged on behalf of Smart Communities. In

addition, Smart Communities provide an opportunity for overcoming challenges of interoperability, which still face the healthcare IT industry.

Smart-city platforms should follow the model for creating a modern software factory for innovation. This model incorporates security, compliance, and quality and would ensure that the smart-city platform is used "properly." Done well, the people who need to know how it's being used have all the insight they need. They can use what they learn about usage patterns to cultivate it to meaningfully impact people's lives.

Security can't just be a feature, or an afterthought. Rather, security must be a core element on which the Smart City builds trust; without trust, there is no Smart City.

Security of the APIs must be built into the infrastructure when exposing public data for private sector innovation. Many API platforms ignore a platform level of security that would ensure consistent security policy across development teams to protect both data and infrastructure.

When security is part of the platform, security officers own and deploy policies to manage governance, compliance, and security.

Once the infrastructure is secure, we need to ensure three aspects of identity authorization within the smart city framework to ensure accountability and risk management.

Developers must be able to rapidly access security authorization protocols easily, so that security is implemented properly (and not as an afterthought) without presenting a barrier to innovation. Security must ensure that citizens are protected, and also respected. Where possible, the citizen experience should be preserved while providing security; security should not be a barrier to the enjoyment and participation in the smart city experience.

As such, there are three elements to identity and authorization to be considered. At CA we consider these the 'Authentication Triangle™ ' that allows to provide 'Authentication in Depth™ ':

1. **Citizen.** The person. The 'user'. We know how to identify people, even digitally. The technology for mobile identity is catching up, but also fragmenting (between things like mobile phone, smart watches, and various biometrics like voice or facial-recognition that are emerging). Cities need a simple way for developers to leverage the latest user identification technology;
2. **App.** Often activities allowed in one app, are not allowed in another. Learning context of the digital activities being performed from the app, and using that to manage risk and user rights enhances the ability to protect user data and identity;
3. **Device.** The third piece of the Authentication Triangle is the device. Devices must be authenticated so that we can ensure the integrity of data being exchanged between devices, applications, and back-end data systems.

Using these three elements the Smart City can balance security risk centrally, ensure citizen experience when participating in the Smart City offerings, and provide the best possible developer experience for creating secure applications.

Making it real — two broad use cases we are delivering through Latin American cities, where citizen's initial computing experience is often through their mobile device

A mobile, digital ID. Every time the government needs ID multiple identifications are required. The policy is opaque, sometimes hard to follow. It's frustrating for those who trade time for money, because time

taken to prove something as “simple as” identity is time not earning a living. A single digital identity connected to a smart city would streamline every single interaction with the government (and pseudo government organizations like hospitals, utilities, etc.)

Moving paperwork from one department to another is an onerous, time-consuming, and unnecessary process. When citizens need to take paper from one part of the government to another, it’s obvious the government is not connected, not focused on the citizen. One example is the need for parents to physically take a child’s proof of immunization to their school. In an age of mobile devices that are literally with us at all times, why does one need to have a piece of paper printed at the doctor and delivered to a school?

Citizens face the same obstacle when providing proof of residence for payroll taxes or car insurance. Or for sharing health insurance information with healthcare providers.

Smart Communities provide significant opportunities for reducing costs, enhancing citizen services, and improving quality of life. In many ways, they represent low hanging opportunities we can pick easily to start to build both a platform and the trust necessary to get citizen involvement in Smart Communities innovation.