# Smart Cities: Utopian Dream, Security Nightmare, or Political Gimmick?

As smart cities evolve with more and more integrated connected services, cybersecurity concerns will increase dramatically.

By Kevin Townsend

August 23, 2023

How much smart does a smart city need to be called smart? It's not a trivial question. It goes to the heart of understanding the concept of connected cities: what is a smart city, what does it deliver, and is it worth the effort? And is it ultimately a utopian dream or a cybersecurity nightmare?

# What is a smart city?

The term smart city implies that the whole city is smart. Excluding China and a few other rich and authoritarian regimes, this is far from accurate.

The UK's NCSC prefers the term 'connected places'. "The fundamental aim of a connected place," it says, "is to enhance the quality of living for citizens through collaborative, interactive, and connected technology… a connected place can be described as a community that integrates information and communication technologies and IoT devices to collect and analyze data to deliver new services to the built environment, and enhance the quality of living for citizens."

This also falls short. It doesn't differentiate between smart cities and smart villages or even smart streets. It focuses on the term 'community', yet neither defines nor explains who should specify 'the quality of living for citizens'. The result is misleading. A community doesn't suddenly decide it will get smart. Smartness is something imposed upon the members of a community with no element of choice. And within this definition, everyone is likely to be part of several or many connected places, with varying degrees of connectedness between the connected places.

In describing a smart city, it is better to concentrate on 'smart municipal services': traffic control; energy distribution; water services; waste collection; and, of course, elections. Each of these services will be automated and 'intelligent' using sensors, connected devices, artificial intelligence, and communication technologies. They are likely to be overlapping and themselves interconnected, with the citizen as the lowest common denominator across most connected services.

So, returning to our original question, how many of these services must be smart before the municipality itself can be called a smart city? This is unanswerable. Since we cannot define 'smart city', it is best to describe it as currently a journey, because the destination is still unknown.

"Smart city is more of a philosophy, an effort or initiative to use technology and data to become more informed and efficient," comments Michael Sherwood, CISO at the city of Las Vegas. "It's a marathon, not a sprint."

# How do you bake a smart city cake?

The momentum toward smart cities is inevitable and probably unstoppable. We have the technology – in fact, we've had much of the technology for many years. But it is not a natural evolution of community life. The smart city needs to be forced, so it is worth understanding the forces that will shape the future development of smart cities. These are primarily political advantage and big tech lobbying.

The primary purpose of all politicians is to be re-elected. The best way to achieve this is to be seen working for the benefit of the voters (citizens). Smart cities are a highly visible method of working to improve 'the quality of living for citizens'. If smart cities can deliver this, then the introduction of connected services becomes a political advantage.

The result has been instrumental in confusing the concept of smart cities – politicians have promoted the idea that they are creating smart cities even if they have just created a single connected service, or single smart building.

"Political motivation is behind a lot of this movement," suggests Kevin Curran, professor of cybersecurity at Ulster University. "I don't see many valid use cases within smart cities so far." He also questions whether politicians can see the implications of their technological decisions and cites the UK government's war against E2EE as an example. The government is trying to eradicate the citizens' access to E2EE for political reasons. "Apple could pull out of the UK market for messaging and we'll all be weaker as a result. Where smart city implementations are driven by government wishes, you must question whether the government understands what it is requiring and whether it is of any practical value to the citizen."

The second force is lobbying from tech companies. They have the technology, and smart cities are a market opportunity for increasing sales and profits. Fundamentally, it is easy to see smart cities growing from external self-interest rather than internal evolution.

This raises a second observation on smart cities. The most advanced smart cities are in China. China is an authoritarian society where the government has the time, will, and resources to impose its decisions – of whatever magnitude – upon the population. Compare this to most western nations. Here the government is not authoritarian, has checks and balances on its authority, and frequently doesn't own the services it wishes to include within its vision of smartness.

Authoritarian societies can build a new connected smart city from the ground up but with top down authority, and little concern for existing rules or regulations. Western cities cannot do this. They are faced with constitutional restrictions, consumer-based legislation, and political change.

The best way to develop a smart city is with a single completely integrated vision and plan. That is almost impossible in western liberal democracies. Most western smart cities develop point solutions for different services, but must then integrate them to maximize the overall benefits. That is why it is a journey.

This journey from point solutions to full integration can help define what is not a smart city. "To be a smart city, you must have the underlying infrastructure in place," explains Martin Zinaich, CISO at the City of Tampa. This involves the city's communications. "You're trying to connect a whole lot of things, so the underlying communications infrastructure must be city-wide, fast, and secure. If that isn't on your radar, you're not a smart city because you're not planning to be a smart city. You're piecemeal at best."

# Advantages

Smart cities have many enthusiasts. "Smart cities use tech and data-driven solutions to bring about positive changes making urban environments more efficient, sustainable, and viable," says Zac Warren, chief security advisor EMEA at Tanium. "These advancements not only address current challenges but also contribute to a better overall urban experience for residents. Ultimately the transformative nature of smart

*Zac Warren, chief security advisor EMEA at Tanium.*

cities has the potential to create a brighter and more resilient future for the people living in these innovative urban areas."

Georgia Weidman, security architect at Zimperium, cites Barcelona as an example. "The traffic management systems, for example, takes into consideration not just traffic, but also energy efficiency, traffic noise, and air quality management," she says. "Most larger cities have moved their mass transit systems online so that you can pay with a mobile device, and see real-time data on when the next bus / train will be arriving – and in some cities you can also tell the current load factors and short-term forecasts (in case you want to avoid being packed cheek-to-jowl on the subway simply by waiting a few minutes)."

Curran – who is certainly not an unmitigated smart city enthusiast – can still see certain advantages to the concept. He likes one example from a US city: "Garbage trucks drive around parks and open spaces to collect rubbish from the bins. But the bins contain sensors that tell the drivers which bins need to be emptied. Empty or quarter-full bins don't need to be visited. It saves time and fuel costs." Noticeably, this application does not involve the collection or use of citizens' personal data.

*Georgia Weidman, security architect at Zimperium*

Sherwood has already embarked on the smart city journey. "For us in Las Vegas, we launched smart city projects to improve the customer experience and interoperability among all public service sectors by leveraging open-source data sharing and real-time data analytics. We knew we'd have to undergo a technology shift and cloud migration from our previously centralized legacy infrastructure before we could truly move the project forward. We started that cloud transformation journey a few years ago."

Weidman notes that even laying the groundwork for a smart city can deliver benefit to the inhabitants. "A fringe benefit of these truly smart cities is that they require ubiquitous networking for the sensor networks and the command-and-control networks (and, alas, the camera networks); however, in many cases these same networks are being used as the root of free public broadband initiatives."

# Security concerns

As smart cities evolve with more and more integrated connected services, cybersecurity concerns will increase dramatically. The risks are not new, but smart cities increase the scale of these risks, and their potential damage. Those threats focus around misuse of personal data by the city, theft of hugely detailed personal information by criminals and nation states, and disruptive cyberattacks that could make the Atlanta ransomware incident seem like a walk in the municipal park.

Personal data will be gathered on a scale not yet seen. CCTV footage will be increased to deliver more efficient law enforcement. Facial recognition will creep into this. Zinaich comments,

“Beijing subways went from scanning your phone to facial recognition. Now, when you get on a subway, you just walk in, and the gate opens because it sees and recognizes your face.”

*Martin Zinaich, CISO at the City of Tampa*

All the different connected services will collect their own user telemetry to improve their service. For efficiency, this telemetry will be shared between multiple services. The greater the sharing, the greater the risk. This introduces a completely new security risk: the possibility of discrimination against a user in one service because of bad behavior in another service. Figuratively speaking, the subway gate might not open because the traffic system caught you jumping a red light – and you are now deemed a bad risk.

Technically, a smart city would be able to penalize people for bad behavior. Since one of the primary functions of the smart city is “to enhance the quality of living for citizens”, the reduction of bad behavior could be viewed as a valid, if dystopian, function.

In traditional cybersecurity terms, the smart city will become a massive target. ‘Smart’ will become functional on two primary technologies: IoT sensors and communications. Both technologies are currently abused by attackers. “In essence,” said Zinaich, “the smart city expands the attack surface and increases the opportunity for threat actors to exploit a vulnerability. The worst case scenario is that when attackers exploit one of those systems, they can start moving laterally across networks and create an event that is cross-sector and can take out full infrastructure operations.”

This possibility will be hugely attractive for criminal hackers with ransomware, and for adversarial nations wishing to cause disruption (perhaps with a wiper disguised as ransomware and difficult to define as an act of cyberwar). This introduces a further complication. Attackers of all denominations seek to compromise supply chains to gain multiple opportunities. The components of the smart city will be provided by third parties and used by multiple smart cities.

Curran gives an extreme example. Certain technologies are reliant on foreign devices. Huawei could be used as a hypothetical example (with the fear that the Chinese government ultimately has access to Huawei equipment). “Some of the contracts to fulfill the smart city are going to be huge. Which countries will be able to bid for them? What if the country concerned can include a hidden switch?” The result, both literally and metaphorically, would allow a foreign state to turn off the lights – perhaps in multiple smart cities simultaneously.

This problem is real at many levels. Cities do not own all the services they deliver. The devices that provide the smart element will come from the service owner and/or other third parties. “Now you’ve got this third party risk, and integration,” says Zinaich. “In essence, you’re going to lose visibility into the collective system itself.”

One area we haven’t considered is personal privacy. The city will collect and use huge volumes of personal information. This will be a target for criminals and a tool for bureaucrats and law

enforcement. Zinaich points out that his iPhone and CarPlay already predicts where he is likely to go on Thursday based on where he has been on other Thursdays.

“I don’t know if I want that overview of my life,” he said. “But that’s the privacy concern — it’s all there and now is going to be hackable and available to government overreach. You tie AI on top of that. Add a central bank digital currency (CDBC) and now everything you spend — and whether you can spend it — will be riding on somebody else’s rules. I find that very scary.”

He points to several questions that haven’t yet been asked or discussed. “Is every citizen or company obliged to be part of the smart city? Or is it voluntary? What kind of information will go public? And how do you keep stuff confidential if you want it confidential? None of these questions have been properly addressed.”

The more integrated a smart city becomes, the greater becomes the cybersecurity challenge. Many of the challenges are well understood by security defenders. But complexity is an enemy of security, and smart cities will be the epitome of technological complexity. The security and privacy risks we have outlined are not inevitable – but they could happen, so they should be considered.

# Are smart cities worth the effort?

To have or have not smart cities is not a binary decision – they are going to happen, driven by politics and economy. We should not simply reject them because of the ‘cybersecurity nightmare’ side of the equation – “Don’t throw the baby out with the bathwater,” says Curran. He believes that aspects of the smart city can benefit citizens if they are chosen and implemented with care. He cites two examples: the guided waste bin emptying service, and sensors switching lights in municipal buildings on or off dependent on the detection of motion.

Both can save money; both are driven by sensors reacting to physical conditions; and neither involve the collection and use of personal data. This approach is ultimately a series of separate point solutions that may never be interconnected with other services. The danger, however, is that once technology is used for individual smart services, smart city feature creep will lead to its expansion.

“Technology is never, never the solution to all of society’s ills,” added Curran. He accepts that technology can provide efficiencies and improve the quality of life, but only if it is chosen with care and implemented safely. “We need to make sure it is safe, and that we don’t add to the problem with more sensors that are insecure and only have a shelf life of a few years – just because some politician wants a press release to get more votes.”

In short, we need to be smart about smart cities. Are smart cities a utopian dream or cybersecurity nightmare? They are both.