

# Smart Cities and Privacy

By Paige M. Boshell



**This article offers a high-level overview of smart city use cases, technologies, and data analytics and discusses how privacy management and citizen engagement is critical to the successful deployment of smart city efforts—privacy is critical to citizen buy-in.**

## Smart cities generally

The goal of the smart city is to use technology and data to better the lives of its citizens.

The deployment of connected information and communication technologies and widespread collection and analysis of data is intended to improve the quality of life for the city's residents through decreased costs (such as via the elimination of waste and/or allocation of resources where most needed and/or beneficial), identification of potential needs or problems as they develop, and recognition of opportunities. Specific benefits include increases in efficiencies and improvements in public safety and health; transportation; access to digital technologies; resident and workforce engagement; municipal government services, policy-making, and budgeting; utilities and infrastructure; economic development; environmental impact; and land use and development.

The term is used to apply to cities that have fully-integrated these technologies and data strategies, as well as to those that are working towards implementation or using isolated technologies for specific purposes.

A basic overview of “technology enablers” for smart cities includes connectivity, the Internet of things (IoT), mobile

devices, and crowdsourcing.<sup>1</sup> Urban sectors served by such technology include transportation, utilities, telecommunications, government services, and environmental.<sup>2</sup> Stakeholders using the technologies include individuals, businesses, government, and private-public sector arrangements.<sup>3</sup> The Future of Privacy Forum offers an informative and accessible interactive graphic showing how these technologies, sectors, and stakeholders interact and the specific technologies implemented to serve them.<sup>4</sup>

## Use cases for smart cities

In order to consider the privacy concerns implicated by smart cities, it is important to understand the many benefits that smart city technologies can confer on citizens and government. Smart city paradigms use technology and data analytics to solve city problems, whether they are problems that are common to a majority of cities or unique to specific types of or individual cities.

1 “Shedding Light on Smart Cities,” *Future of Privacy Forum* (2017) - <https://fpf.org/2017/03/30/smart-cities/>.

2 Ibid.

3 Ibid.

4 Ibid.

## Public safety

Smart cities can improve their efforts to prevent and solve crime (including cybercrime and terrorism) or detect and respond to natural disasters or epidemics by enhancing and increasing efficiencies in existing traditional (more cumbersome) methods or introducing new methods:

- Predicting where crime or disaster (like a fire) is likely to occur so that prevention and detection efforts can be enhanced like airports, sports stadiums, highways, or utilities—for example, by more efficiently deploying patrol officers or increasing surveillance.
- Detecting when a crime is in progress and accessing the situation for first responders—for example, through the use of video or other surveillance to detect crime and the use of drones to measure the threat to firefighters.
- Enhancing communications among city agencies and first responders—for example, to coordinate efforts between firefighters, police, and emergency rooms in the event of a fire.
- Coordinating with other local and federal government agencies in the event of widespread criminal events, attacks, natural disasters, or other weather emergencies—for example, through enhanced communications or faster sharing of data and assessment and allocation of resources to effectively evacuate communities and deploy first responders and to increase readiness of potentially-affected citizens and communities.
- Detecting disease and coordinating information and response within the city across departments and with other federal and local agencies to ensure efficient allocation of detection and response resources and enable citizens to protect themselves.

## Decreasing pollution and climate change impacts

Smart cities more effectively detect sources of pollution and address them through more efficient deployment of existing resources and new approaches to easing impacts:

- Altering geolocation and timing patterns for traffic congestion by changing traffic flows and laws; encouraging carpooling and use of existing public transportation; facilitating the ease of using bicycles, scooters, and shared self-driving vehicles; and empowering citizens to use less gas and drive less by optimizing parking availability and access (and driver knowledge of which parking is available).
- Detecting patterns in pollutants (including spikes in contaminants) in order to deploy remediation and prevention measures.
- Optimizing energy consumption by increasing efficiencies in municipal government facilities and coordination with consumers to reduce their energy footprints.

- Deciding which prevention and remediation measures are more effective and cost-efficient in order to prioritize response and remediation.
- Informing city planning like expansion or placement of parks and trees, deployment of bike lanes, coordination of lights to contemplate alternate modes of transportation, and encouragement of pedestrian traffic.

## Other use cases

Smart cities can address a variety of other resident problems by increasing expedited access to city services, increasing revenue via smart tourism, improving access to and efficiencies in utilities, and directing existing resources and determination of the most efficient new, tailored approaches to improve education and health care. Smart cities in process can prioritize problems, more efficiently access existing resources, and precisely determine less painful and more productive cost-cutting efforts.

Think of a smart city as a platform or grid on which a variety of technologies may be deployed and reallocated depending on the changing needs of the individual city. There will be certain commonalities in deployment of technology and data strategy across cities, but personalization to individual city needs is easily achievable over time so that municipal governments can respond more quickly and efficiently to the evolving needs of its residents. The goal of any effective smart city is to improve the quality of life for its citizens.

## Smart city technologies

A wide variety of technologies are used to implement the smart city model. Key features include connectivity and precision and accuracy in data collection. Some of these technologies rely heavily on the IoT. For example:

- A sensor placed on a patrol car gun rack can alert police headquarters when a gun has been removed from the rack and trigger camera surveillance of the car, which is immediately viewable by headquarters to facilitate emergency response.<sup>5</sup>
- Sensors placed on light poles or under pavement can monitor traffic in real time, including vehicle and pedestrian counts and vehicle speeds to be used to immediately impact traffic and street lights and facilitate traffic planning.<sup>6</sup>
- Sensors placed in garbage bins can photograph and analyze bin contents and, in connection with other bin sensors, optimize trash collection routes.<sup>7</sup>
- Sensors in parking lots can alert drivers to available spots.<sup>8</sup>

5 Phil Goldstein, "5 Smart City IoT Use Cases to Keep in Mind," StateTech (August 24, 2018) – <https://statetechmagazine.com/article/2018/08/5-smart-city-iot-use-cases-keep-mind>.

6 Ibid.

7 Ibid.

8 Pushp Kumar Dutt, "IoT and Smart Cities—Use Cases and Implementation Strategies—Part I," NetObjex Blog (January 2019) – <https://www.netobjex.com/iot-and-smart-cities-use-cases-and-implementation-strategies-part-i/>.

- Sensors on electrical transformers or wastewater/sewage systems can facilitate responsiveness and efficiencies in utility maintenance.<sup>9</sup>

The connectedness among systems and across agencies facilitates automation of data collection.

Other smart city technologies enhance the precision of data inputs. For example, facial recognition technology allows faster processing of airport ticketing, security, and onboarding<sup>10</sup> and detection of suspected terrorists or individuals with outstanding criminal warrants at nation entry points<sup>11</sup> and in areas or events carrying greater risks of terrorism or crime.<sup>12</sup>

Artificial intelligence (AI) facilitates automated responsiveness based on these data inputs. AI can process data accumulated via sensors or other technologies to detect patterns and report data outputs. The value of facial recognition technology may be based on the immediate processing of the individual's face into data points, but the immediate analysis of those inputs and comparison to data points (faces) of known individuals is critical. Other AI examples include:

- Using live video feeds or sensor inputs to count vehicles and pedestrians, track vehicle speeds and traffic flow, and detect patterns in large volumes of raw data.
- Adaptive traffic systems and intelligent traffic light systems to respond to traffic in real time to change the timing and flow to minimize congestion, travel times, and energy usage and to redirect traffic to enable first responders to move more quickly.
- Input from gunshot sensors in light poles to determine the location of gunfire and alert police.
- Rainfall gauge inputs combined with radar data to transmit hyper-localized weather warnings.<sup>13</sup>

Augmented reality helps to provide useful outputs to government officials and employees and residents:

- Motorcycle helmets can assist with driver navigation, visualize roadways, and warn the driver of imminent construction, accidents, or other obstacles or risks.<sup>14</sup>
- Digital models for urban planning can help the government visualize construction impacts.<sup>15</sup>

9 White paper, "IoT Innovation: How Government Is Uncovering New Opportunities," Center for Digital Government (2018) - [https://media.erepublic.com/document/CDG18\\_WHITE\\_PAPER\\_Cisco-IoT-NewOps\\_V.pdf](https://media.erepublic.com/document/CDG18_WHITE_PAPER_Cisco-IoT-NewOps_V.pdf).

10 Melissa Locker, "Report: 20 Major Airports May Get Face Recognition for International Travelers by 2021," Fast Company (March 2019) - <https://www.fastcompany.com/90318183/20-major-airports-may-mandate-face-recognition-for-international-travelers-by-2021>.

11 Jenni Fink, "Airport Facial Recognition Is Here and Expanding: What Are Your Rights and Can You Opt Out?," Newsweek (March 2019) - <https://www.newsweek.com/facial-recognition-technology-what-are-your-rights-can-you-opt-out-1360477>.

12 Melissa Locker, "Brazil Is Using a Facial Recognition System During Rio's Carnival," Fast Company (January 2019) - <https://www.fastcompany.com/90299268/brazil-is-using-facial-recognition-tech-during-rios-carnival>.

13 Jon Walker, "Smart City Artificial Intelligence Applications and Trends," EMERJ (January 2019) - <https://emerj.com/ai-sector-overviews/smart-city-artificial-intelligence-applications-trends/>.

14 Stephen Goldsmith and Chris Bousquet, "AR Is Transforming Tech. What Can It Do for Smart Cities?" Harvard Ash Center (August 2018) - <https://datasmart.ash.harvard.edu/news/article/ar-transforming-tech-what-can-it-do-cities>.

15 Ibid.

- City forms can be easily accessed by residents using a variety of devices, increasing citizen engagement and reducing costs.<sup>16</sup>

- Firefighter helmets can facilitate vision in the presence of smoke, rubble, and other impediments.<sup>17</sup>

All of today's emerging technologies have potential smart city uses. These technologies act as the interface between the user (government, business, or individual) and the smart city platform. Some may appear seamless (such as the use of traffic sensors), and others may require direct engagement (such as police interactions with gunfire detection systems and citizen use of utility waste management applications).

## Data analytics

Smart cities rely on vast amounts of data from a variety of internal and external sources. Technology is used to collect, process, and provide outputs of this data in ways that humans cannot. All smart city use cases depend upon data analytics.

Consider Amsterdam, which has for years engaged in public-private partnerships to deploy technologies throughout the city. In addition, the city has worked to integrate its inventory of 12,000 different data sets. Here are the following innovations that Amsterdam has implemented:

- Finding a correlation between the number of secondhand cars in an area and an increase in the incidence of crime.
- Pinpointing the households of most active criminals in order to provide intervention to younger siblings.
- Identifying populations less likely to use bikes in order to offer education and incentives for bike riding.
- Measuring grocery store vegetable sales to determine if education to improve children's diets is working in certain neighborhoods.
- Comparing depression rates to availability of care and treatment costs.<sup>18</sup>

A Harvard University project offers specific guidance for smart city development of data analytics programs: (1) identify the problem, (2) assess data readiness, (3) project scoping, (4) pilot launch, and (5) implementing and scaling the model. The report analyzed successful use cases like:

- New Orleans' combination of US census data regarding households with smoke alarms with other related data to identify neighborhoods by block to determine outreach and distribution of smoke alarms in order to combat fire fatalities.
- A partnership with Chicago to determine predictors of adverse incidents by patrol officers to implement early intervention.

16 Gregory Curtin, "Six Ways Augmented Reality Can Help You See More Clearly," Smart Cities Council (March 2017) - <https://smartcitiescouncil.com/article/six-ways-augmented-reality-can-help-you-see-more-clearly>.

17 Ibid.

18 Frank Harmsen, "Smart Cities: A world of Opportunity in Data," INFORM Analytics Magazine (2016) - <http://analytics-magazine.org/smart-cities-a-world-of-opportunity-in-data/>.



Other cases involved predicting urban blight, forecasting outbreaks of the West Nile and Zika viruses, optimization of restaurant inspections, development of baiting programs to combat rodent infestations, and decreasing traffic fatalities.<sup>19</sup> Several cities use algorithms to rank residences according to house fire risk.<sup>20</sup>

Data analytics facilitate “data storytelling,” which is critical to citizen and government employee buy-in. St. Petersburg, Florida, has implemented dashboards for 12 city agencies that enable real-time visual displays of problems that the agency is charged with addressing and possible causes and solutions. These dashboards translate vast amounts of raw data into stories for the agencies to solve. For example, the city agency enforcing code compliance was able to determine areas where the most code violations occurred in order to reallocate underutilized investigators to assist those who were overworked. New York City has deployed 1700 kiosks to allow public access to city data and tell stories about how residents have used this data. In this way, these cities have translated the raw data into stories that enable users to solve specific problems.<sup>21</sup>

### Citizen buy-in

A recent McKinsey and Company publication, “Smart Cities: Digital Solutions for a More Livable Future,” reports on the potential of smart cities to improve residents’ lives and the 50 cities worldwide that have been most successful to date.<sup>22</sup> The report identifies three layers of “smartness”:

1. The technology base, including sensors and IoT networks
2. The data analytics capabilities and applications
3. Adoption and usage “often leading to better decisions and behavior change”

The third level, user buy-in, is critical. Although the report does not delve into the third layer, it is fairly intuitive. Certain technologies, like traffic sensors or video cameras, may be deployed without resident knowledge or consent; others, like biometrics or facial recognition, may involve consumer opt-in or opt-out. Much of the technology is expensive and all aspects of smart city implementation involve widespread allocation of city resources, both public and private. Many use cases require active citizen participation, such as efforts to reduce individual carbon footprints or install smoke alarms. Certain data collection systems require affirmative input or

consent, use cases involve actual use, and residents vote on leadership and allocation of resources.

### Privacy is a key driver for citizen buy-in

Privacy is a hot topic worldwide. Scandals involving Big Data and Big Tech are ubiquitous and have alarmed consumers about how their data is being collected, used, and shared. Some of the technologies, like facial recognition, can seem invasive and susceptible to misuse, whether by government or others who have authorized access or third parties that wrongfully obtain access to the data. Others are not easily understood. The sheer volume of data collected and shared can be overwhelming. Further, several significant private-sector partners, like Google, have had their own privacy scandals and may be untrusted by residents.

Data storytelling is important for city residents so that they can understand the beneficial impacts that smart cities can have on their lives. Transparency about data collection and use and security and privacy of individual resident data is key to acceptance. Cybersecurity is a significant concern and is currently addressed—or addressable—by cities at each stage of data collection, usage and analytics, and sharing. Privacy-by-design (PbD) is not widespread and not usually squarely addressed in the literature regarding development of smart city programs.

Smart cities won’t work without privacy. Citizen education and transparency is critical:

Will we, as smart city residents, know what data is being collected, how it’s being monitored, how it’s being used, to whom it’s being sold, and what will be done with it in the future? Will we have the option to “opt-out” of some elements of data collection if they aren’t being de-identified? All of these questions will need to be answered clearly to assuage privacy concerns for smart cities.<sup>23</sup>

Consider RAVEN911. The Regional Asset Verification Emergency Network allows city, county, and state governments to collaborate in real-time response to “emergency situations like extreme weather events, bomb threats, crowd control, and more.”<sup>24</sup> The technology combines the use of fixed maps (like residential, geographic, or infrastructure) with immediate data feeds (like weather radar or social media scans) and live data inputs (for example, from first responders) to allow coordinated response among various governments. Privacy was critical to government and citizen trust and buy-in:

Any time governments are asked to share data across traditional silos, privacy concerns inevitably arise. To assure agencies that their data was safe with RAVEN911, [the founding] team met with target departments across the region to go over their privacy policies and security measures. The team assured them that the system only grants

19 Jessica Gover, “Analytics in City Government,” Harvard Ash Center (July 2018) – <https://datasmart.ash.harvard.edu/news/article/analytics-city-government>.

20 Jonathan Jay, “Can Algorithms Predict House Fires,” Harvard Ash Center (March 2017) – <https://datasmart.ash.harvard.edu/news/article/can-algorithms-predict-house-fires-990>.

21 Zack Quaintance, “New York City, St. Petersburg, Fla., Ramp Up Data Storytelling,” GOVTECH (January 2019) – [https://www.govtech.com/analytics/New-York-City-St-Petersburg-Fla-Ramp-Up-Data-Storytelling.html?utm\\_term=READ%20MORE&utm\\_campaign=New%20York%20City%2C%20St.%20Petersburg%2C%20Fla.%2C%20Ramp%20Up%20Data%20Storytelling&utm\\_content=email&utm\\_source=Act-On+S](https://www.govtech.com/analytics/New-York-City-St-Petersburg-Fla-Ramp-Up-Data-Storytelling.html?utm_term=READ%20MORE&utm_campaign=New%20York%20City%2C%20St.%20Petersburg%2C%20Fla.%2C%20Ramp%20Up%20Data%20Storytelling&utm_content=email&utm_source=Act-On+S).

22 Jonathan Woetzel, Jaana Remes, Brodie Boland, Katrina Lv, Suveer Sinha, Gernot Strube, John Means, Jonathan Law, Andreas Cadena, and Valerie von der Tann, “Smart Cities: Digital Solutions for a More Livable Future,” McKinsey Global Institute (June 2018) – <https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-cities-digital-solutions-for-a-more-livable-future>.

23 Daniel Newman, “Are Privacy Concerns Halting Smart Cities Indefinitely,” Forbes (January 2019) – <https://www.forbes.com/sites/danielnewman/2019/01/08/are-privacy-concerns-halting-smart-cities-indefinitely/#131ead1369ba>.

24 Daniel Curtis, “RAVEN911 Gives Emergency Responders a Bird’s Eye View,” Harvard Ash Center (October 2015) – <https://datasmart.ash.harvard.edu/news/article/raven911-gives-emergency-responders-a-birds-eye-view-758>.

access to emergency responders that have been vetted by the Cincinnati Police Department. What's more, the login credentials required by [the RAVEN911 software] are encrypted and expire periodically, making it extremely difficult for undesired users to get into the system and impossible for them to stay there. These measures proved enough to allay the fears of data providers and have kept their information secure ever since.<sup>25</sup>

Privacy concerns may vary by community. Early involvement by citizens and advocacy groups can help frame the conversation, identify specific concerns, and address them as part of smart city development.<sup>26</sup>

Privacy concerns also vary by the type of technology involved. For example, San Francisco has become the first city in the US to ban city government use of facial recognition technology outright and require stricter processes for the implementation of other types of surveillance technologies.<sup>27</sup> The "Stop Secret Surveillance" ordinance was motivated by the "propensity" of facial recognition and other surveillance technologies to "endanger civil rights and civil liberties."<sup>28</sup>

Indeed, privacy concerns can delay or derail smart city initiatives. Google's parent company Alphabet recently announced a new app, CommonSpace, which is intended to "make it easier for people—namely those interested in the subject matter, like city and county officials, to collect, analyze, and use data about people in public spaces."<sup>29</sup> The app relies on "the personal observations" of app users regarding "[w]ho does what, where, and when" in public spaces so that cities can determine how to efficiently invest in and use those spaces in ways that are responsive to the community of users.<sup>30</sup>

The tech start-up that created the app, Sidewalk Labs, offers a platform of technologies including the app and IoT sensors to offer customizable smart city solutions. Toronto's proposed new waterfront development, Quayside, is a pilot project for Sidewalk Labs:

**Driverless cars will have a big role.** Sidewalk Labs assumes they will navigate more precisely and obey traffic laws more consistently than human drivers, so it wants to put narrower lanes in Quayside and carve out more room for

sidewalks and parks. In theory, using shared self-driving vehicles will mean that fewer people need to own cars, saving families a projected \$6,000 a year.

**Sensing and monitoring public activity accurately and frequently will be key.** Running autonomous buses on city streets requires knowing when to change lights and other signals to give cyclists and pedestrians priority.

**Sidewalk Labs says the sensor information would also support long-term planning.** The data would fuel a virtual model of Quayside that urban planners could use to test infrastructure changes quickly, at low cost, and without bothering residents. It could also be stored in a shared repository that entrepreneurs and companies could draw on to make their own products and services for Quayside.<sup>31</sup>

The near-constant surveillance required for the platform to work has threatened resident support:

Most of the scrutiny relates to the company's plan to install sensors across Quayside to measure everything from building occupancy to sewage flow rates to how often a public waste bin is used. The company is also devising a system that would give Quayside residents and workers a quick way to pay for things and gain access to services, similar to the way people can buy products off Amazon with a single click or get billed for Uber rides through an app.

Though Sidewalk Labs says the data would be used for a community purpose, such as giving transit discounts to low-income residents, regulating building temperatures, and keeping trash cans from overflowing, not everyone is convinced. "There are definitely questions about whether Sidewalk Labs will try to make money by tracking people's daily interactions," says David Roberts, who studies cities at the University of Toronto. "What data will be collected, how personal will it be, how will it be used, and who will have access to it?"<sup>32</sup>

Privacy pushback on Quayside has been pervasive and high profile:

But what has caused most alarm is that, in this quayside city of the future, residents' every move would be recorded. Inevitably, anxieties about privacy and covert surveillance have followed. Small hidden cameras would snap low-resolution images of people and cars as they move through the streets. Sidewalk says its systems would blur identifiable information, label pictures either "pedestrian" or "vehicle," then enter it into a "public data trust." The data would be used to plan services in real time in what it calls a "feedback of residents". . . Critics include local technologists, property developers, politicians from both the left-leaning NDP and Conservative parties, urbanists, academics, privacy experts, business leaders, and the Ca-

25 Ibid.

26 Skip Descant, "Smart City Data Projects Need Transparency and Oversight," GOVTECH (October 2018) – [https://www.govtech.com/fs/data/Smart-City-Data-Projects-Need-Transparency-and-Oversight.html?utm\\_term=READ%20MORE&utm\\_campaign=Smart%20City%20Data%20Projects%20Need%20Transparency%20and%20Oversight%2C%20Cook%20County%20Bets%20Big%20on%20New%20ERP&utm\\_con](https://www.govtech.com/fs/data/Smart-City-Data-Projects-Need-Transparency-and-Oversight.html?utm_term=READ%20MORE&utm_campaign=Smart%20City%20Data%20Projects%20Need%20Transparency%20and%20Oversight%2C%20Cook%20County%20Bets%20Big%20on%20New%20ERP&utm_con).

27 April Glaser, "San Francisco Is About to Be the First U.S. City to Ban Police from Using Facial Recognition Tech," Slate (May 2019) – <https://slate.com/technology/2019/05/san-francisco-first-city-ban-facial-recognition.html>.

28 Lucas Ropek, "Will San Francisco Ban Facial Recognition Technology?" GOVTECH (April 2019) – [https://www.govtech.com/policy/Will-San-Francisco-Ban-Facial-Recognition-Technology.html?utm\\_term=READ%20MORE&utm\\_campaign=Will%20San%20Francisco%20Ban%20Facial%20Recognition%20Technology&utm\\_content=email&utm\\_source=Act-On+Software&utm\\_medium=email](https://www.govtech.com/policy/Will-San-Francisco-Ban-Facial-Recognition-Technology.html?utm_term=READ%20MORE&utm_campaign=Will%20San%20Francisco%20Ban%20Facial%20Recognition%20Technology&utm_content=email&utm_source=Act-On+Software&utm_medium=email).

29 News staff, "Sidewalk Labs Wants People, Not Tech, to Study Public Spaces," GOVTECH (April 2019) – [https://www.govtech.com/biz/Sidewalk-Labs-Wants-People-Not-Tech-to-Study-Public-Spaces.html?utm\\_term=READ%20MORE&utm\\_campaign=Sidewalk%20Labs%20Wants%20People%2C%20Not%20Tech%2C%20to%20Study%20Public%20Spaces&utm\\_content=email&utm\\_source=Act-On+Software&u](https://www.govtech.com/biz/Sidewalk-Labs-Wants-People-Not-Tech-to-Study-Public-Spaces.html?utm_term=READ%20MORE&utm_campaign=Sidewalk%20Labs%20Wants%20People%2C%20Not%20Tech%2C%20to%20Study%20Public%20Spaces&utm_content=email&utm_source=Act-On+Software&u).

30 Ibid.

31 Martina Paukova, "A Smarter Smart City," MIT Technology Review – <https://www.technologyreview.com/s/610249/a-smarter-smart-city/>.

32 Ibid.

nadian Civil Liberties Union.<sup>33</sup>

The motives of the Google affiliate have been widely questioned: “critics say the environmental features are a smoke-screen for the real goal: extracting as much private data as possible from residents of the Canadian city to boost Sidewalk Labs’ profits.”<sup>34</sup>

The Quayside controversy highlights the tensions of technology as a great equalizer versus the diminishment of humanity, convenience of automated services versus the loss of the value of interpersonal exchanges, greater knowledge through data analytics versus the loss of privacy, and technology in the service of people versus people as data capital:

In a government-funded survey published earlier this year by McMaster University in Ontario, 88 percent of Canadians said they are concerned about their privacy in smart cities, including 23 percent who are “extremely concerned.” These fears are especially pronounced when data is being collected by private companies, the survey said, with 91 percent of Canadians opposing the sale of their personal information. “You can’t underestimate the privacy concerns,” said Angela Orasch, a researcher who worked on the survey.<sup>35</sup>

33 Anna Nicolaou, “Future Shock: Inside Google’s Smart City,” Financial Times (March 2019) – <https://www.ft.com/content/3f8a87ba-3ff1-11e9-b896-fe36ec32aee>.

34 Chris Arsenault, “Green Paradise or Data-Stealing Dystopia? Toronto Smart City Sparks Debate,” Reuters (March 2019) – <https://www.reuters.com/article/us-canada-cities-privacy-feature/green-paradise-or-data-stealing-dystopia-toronto-smart-city-sparks-debate-idUSKBN1QS25E>.

35 Ibid.

## Privacy management for smart cities

Transparency, early resident involvement, data storytelling, and privacy by design are critical to smart city privacy management. Privacy International’s guidance for smart cities includes the following:

Citizen consultation needs to be at the heart of city planning. While deals between companies and cities have too often been signed behind closed doors, it is important to bring citizens who truly reflect the diversity of society to the discussion table to insure we create cities that are smart for everyone and that take into account people’s priorities.

Collection of data does not systematically improve cities. It is time for city planners to think of ways to improve our cities that do not impact our right to privacy. When data collection is deemed mandatory, only the data that is strictly necessary should be collected. Data should not be sold for advertisement purposes, nor should it be given to companies as part of government and private sector partnership.

Citizens should be made aware of the data that is collected about them and how it will be used. They should be entitled to have it corrected and deleted.

Surrendering one’s data should never be the condition to have access to services.<sup>36</sup>

36 “Smart Cities,” Privacy International – <https://www.privacyinternational.org/topics/smart-cities>.

# A LEAP AHEAD OR A STEP BEHIND?



CyberRisk Alliance PRESENTS

## InfoSecWorld

Conference & Expo 2020

MARCH 30 – APRIL 1, 2020 | DISNEY’S CONTEMPORARY RESORT | LAKE BUENA VISTA, FL



**2020 KEYNOTE  
SPEAKERS INCLUDE:**

**Jimmy Sanders**  
*Netflix DVD*



**Jamil Farschi**  
*Equifax*



**Parham Eftehari**  
*ICIT*

ISSA members save **15% off the InfoSec World** Main Conference or World Pass with discount code **ISW20-ISSA** at checkout.

[www.infosecworldusa.com](http://www.infosecworldusa.com)



## Barcelona

Barcelona, Spain, is already building privacy and transparency into its smart city planning:

Efforts have centered on two things. The first is opening up governance through participatory processes and greater transparency. The second is redefining the smart city to ensure that it serves its citizens, rather than the other way around.

The group started by creating a digital participatory platform, Decidim (“We Decide,” in Catalan). Now the public can participate directly in government as they would on social media by suggesting ideas, debating them, and voting with their thumbs. Decidim taps into the potential of social networks: the information spreading on Twitter, or the relationships on Facebook. All of these apply to politics—and Decidim seeks to channel them, while guaranteeing personal privacy and public transparency in a way these platforms don’t.

“We are experimenting with a hybrid of online and offline participatory democracy,” says Francesca Bria, Barcelona’s chief technology and digital innovation officer. “We used Decidim to create the government agenda—over 70 per cent of the proposals come directly from citizens. Over 40,000 citizens proposed these policies. And many more citizens were engaged in offline collective assemblies and consultations.”<sup>37</sup>

This approach “reverses” the existing smart city paradigm in which large volumes of data are collected and then city government tries to ascertain problems and solutions. In a pilot program Barcelona citizens drive the process of choosing which problems to solve; each resident has his own dashboard through which he can view and control access to his data; and residents place IoT sensors throughout their own neighborhoods.<sup>38</sup>

A core tenet of the Decode project, which runs the Barcelona pilot and a similar pilot in Amsterdam, is that data collection, handling, and usage be transparent and privacy-friendly.<sup>39</sup>

A recent Georgia Tech Center for the Development and Application of Internet of Things Technologies white paper declares that privacy is “the cornerstone of citizen interaction” for smart cities. The paper encourages the use of privacy by design (“PbD”) in smart city project planning. It explains PbD generally:

The general seven PbD foundational principles included in an October 2010 Resolution passed unanimously by the regulators at the International Conference of Data Protection Authorities and Privacy Commissioners, which recognized Privacy by Design as an essential component of

fundamental privacy, are listed below:

1. Proactive not reactive; preventative, not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality: positive-sum, not zero-sum
5. End-to-end security; full life cycle protection
6. Visibility and transparency; keep it open
7. Respect for user privacy; keep it user-centric

These seven principles are effectively complemented by eight privacy design strategies proposed by the European Union Agency for Network and Information Security (ENISA):

1. Minimize – personal data processing restricted to the minimal amount possible
2. Hide – concealed from plain view to achieve unlinkability and unobservability
3. Separate – distributed personal data in separate compartments whenever possible
4. Aggregate – at the highest level with the least possible detail while still remaining useful
5. Inform – refers to transparency and openness
6. Control – gives users the tools to exert their data protection rights (e.g., view, update, and delete)
7. Enforce – in place through established governance structures
8. Demonstrate – show compliance with policy and legal requirements

The paper explains the application of PbD to smart cities:

PbD’s framework embeds privacy into the design and architecture of IT systems and business practices. Applications for PbD include but are not limited to:

- Closed caption TV/surveillance cameras in mass transit systems
- Biometrics used in casinos and gaming facilities
- Smart meters and the smart grid
- Mobile devices and communications
- Near field communications (NFC)
- RFIDs and sensor technologies
- Redesigning IP geolocation data
- Remote home health care
- Big data and data analytics<sup>40</sup>

Adherence to privacy by design maximizes the citizen trust and engagement necessary for successful smart city efforts, anticipates and prevents privacy failure risk, and increases resiliency in the event of a privacy failure. In the US, gov-

37 Thomas Graham, “Barcelona is Leading the Fightback against Smart City Surveillance,” *Wired* (May 2018) – <https://www.wired.co.uk/article/barcelona-decidim-ada-colau-francesca-bria-decode>.

38 *Ibid.*

39 Francesca Bria, “DEcentralised Citizens Owned Data Ecosystem,” DECODE (May 2017) – <https://decodeproject.eu/sites/default/files/uploads/decodemydata-170903124926%20%281%28%29.pdf>.

40 White paper, “Driving New Modes of IoT-Facilitated Citizen/User Engagement,” Georgia Tech Center for the Development and Application of Internet of Things Technologies (July 2018) – [https://cdait.gatech.edu/sites/default/files/georgia\\_tech\\_cdait\\_thought\\_leadership\\_working\\_group\\_white\\_paper\\_july\\_9\\_2018\\_final.pdf](https://cdait.gatech.edu/sites/default/files/georgia_tech_cdait_thought_leadership_working_group_white_paper_july_9_2018_final.pdf).

ernment officials are joining the newly-formed Civic Data Privacy Leaders Network, whose goal is to advance civic data privacy by:

- Creating a comprehensive privacy risk assessment for smart and connected community projects, providing guidance to local governments and technology providers, and ensuring projects serve the common good.
- Expanding the network of privacy leaders for smart cities and creating peer networks, best practices, and practical tools for responsible data use.
- Hosting workshops in conjunction with MetroLab Network, the South Big Data Hub, and others in order to share best practices and identify areas for further research and collaboration.

These efforts will equip local officials with the tools they need to collect and use civic data responsibly, engage with the public about data and technology, and unleash the power of data to improve our communities.<sup>41</sup>

## Conclusion

Privacy is critical to successful smart cities. An early and consistent commitment to citizen privacy increases the civic engagement necessary to implement smart city strategies and allows for PbD resolution of potential privacy concerns before they arise.

The following principles should be considered at the start and during the course of any smart city project to address privacy concerns and promote buy-in:

- Conduct a privacy impact assessment
- Engage citizens early in the process and involve them in decision-making
- Incorporate privacy by design into all stages of the project and develop metrics that align with privacy goals
- Implement transparency and openness at each stage
- Limit data collection to that which is necessary to achieve project goals and ensure that the least invasive methods of collection are employed
- Limit private sector involvement in collection
- Implement ongoing purpose specification and use limitations regarding data (including third-party access)
- Strictly limit private sector rights of use of data
- Prohibit use of data for marketing purposes and sale of data in secondary data market
- Encrypt, anonymize, or de-identify data as much as possible
- Ensure the security of data and access vectors and the integrity and relevance of data
- Provide for citizen access to data and rights in data correction when possible

- Facilitate opt-outs as possible and prohibit the conditioning or pricing of city services on data collection
- Document the process and data decision-making to provide accountability of city government to citizens regarding data privacy
- Implement a mechanism to track and respond to citizen complaints

The purpose of any privacy impact assessment is to identify and address potential negative impacts on privacy posed by the introduction or change in any smart city technology, particularly technology involving the collection of individual data. Not all privacy concerns can be resolved in a connected environment. Engaging citizens early in the process helps government explain what the community and individual benefits are and how privacy risks may be addressed and involves them in prioritizing privacy risks and deciding which risks are acceptable given the beneficial impacts of the smart city proposal.

Certain types of technologies, like facial recognition or biometrics, spark greater resident alarm. In order to successfully implement them, government officials should be able to explain why less intrusive technologies would not be effective and what steps have been taken to alleviate the risks.

Data collection by vendors may also cause greater concern among residents. Citizen input on whether additional restrictions should be taken, even to the extent of limiting beneficial impacts, is important. Citizen participation in the development of proposals, rather than post-development reaction based solely on privacy concerns, can make the difference in the success of the project.

Ongoing monitoring and reassessment, including citizen feedback, lets citizens know that any new or heightened privacy concerns will be addressed. There will never be zero privacy risk in a connected environment. Different communities have different privacy and security concerns and differing levels of interest in and enthusiasm about smart city technologies. Inviting citizens to help prioritize and manage risk is a game changer in terms of ensuring citizen engagement and participation.

Cities that successfully implement privacy principles and treat them as ongoing and changing responsibilities will have greater leeway and success in smart city innovation and development.

## About the Author

Paige Boshell is a managing member of Privacy Counsel LLC, which offers cybersecurity and privacy legal advice and strategies. She is a privacy law specialist, Fellow of Information Privacy, and ANSI-certified CIPP/US (US law), CIPP/E (European law), and CIPM. She may be reached at [pboshell@privacycounselllc.com](mailto:pboshell@privacycounselllc.com).



<sup>41</sup> Editor, "Municipal Leaders Joining Network to Advance Civic Data Privacy," Future of Privacy Forum (March 2019) – <https://fpf.org/2019/03/28/municipal-leaders-joining-network-to-advance-civic-data-privacy/>.



Copyright of ISSA Journal is the property of Information Systems Security Association, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.