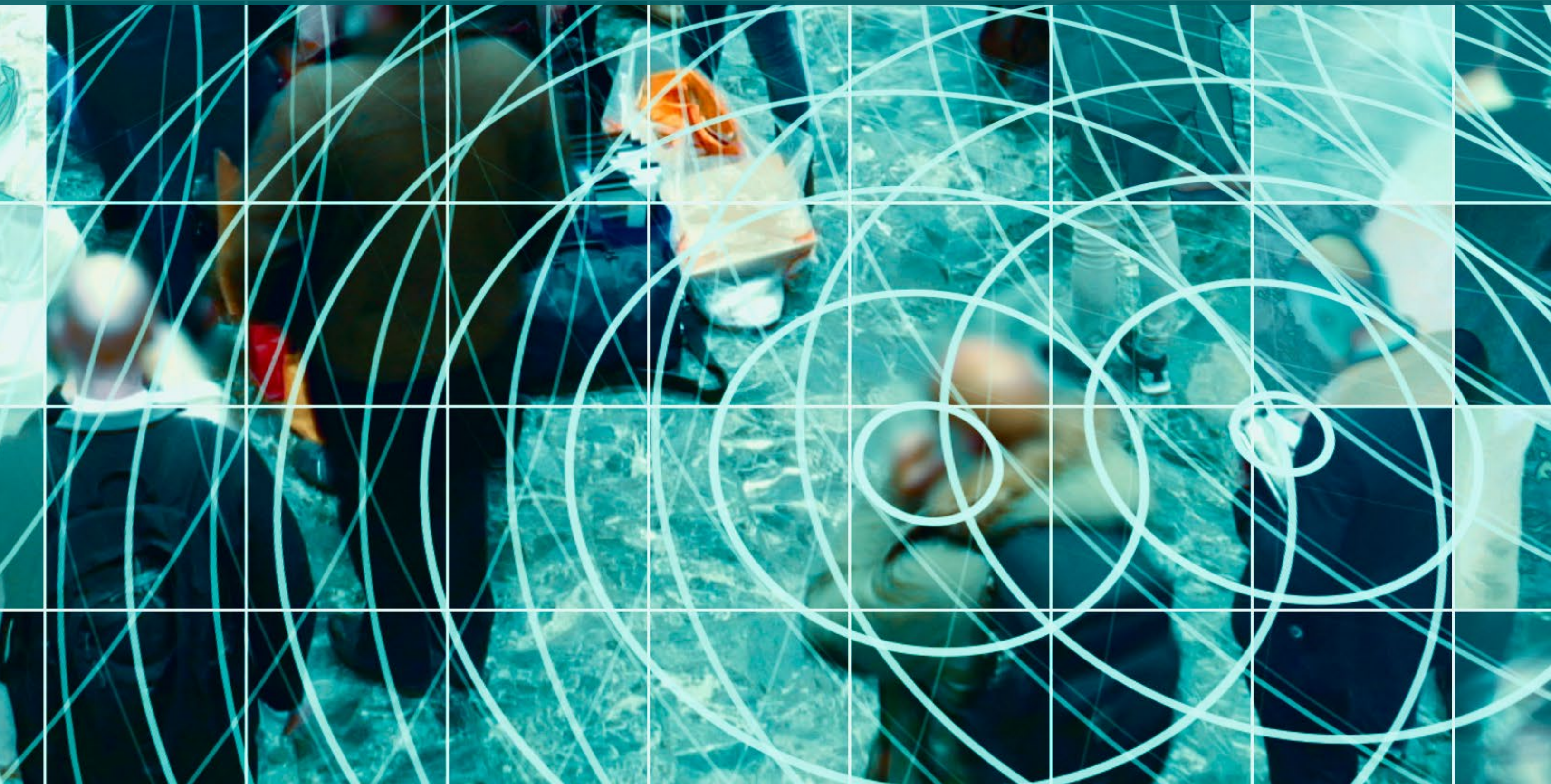
Booz | Allen | Hamilton®

PRIVACY CONCERNS IN SMART CITIES

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

While smart city technologies offer great potential for doing good, cities should ensure that foundational policies and safeguards are in place to provide individuals adequate privacy guardrails.

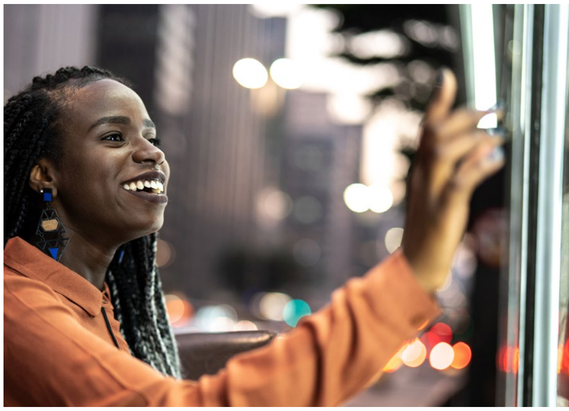


PRIVACY CONCERNS IN SMART CITIES

Cities Seek Smart Efficiency

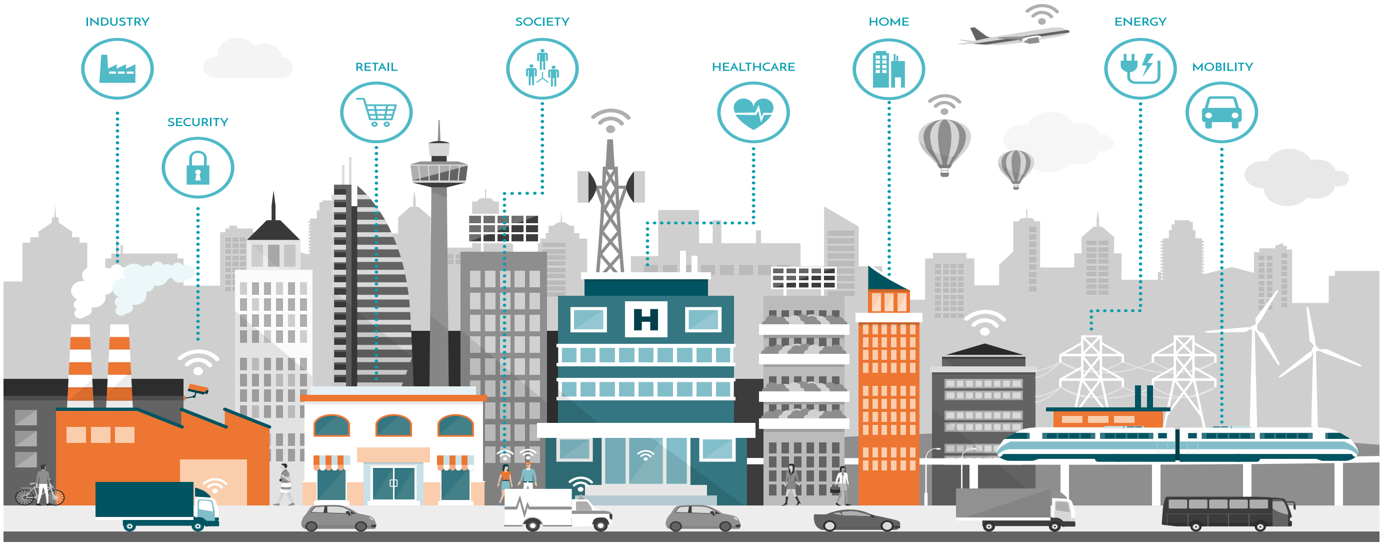
It is commonly said that "states are the laboratories of democracy" because of their ability to experiment with implementing novel policy ideas. While many states, including California and Washington, have borne this out through their approaches to privacy, interesting experimentation is also happening at a more granular level: in cities and municipalities. Often branded as smart or connected in keeping with the moniker given to enhanced devices and other electronics such as mobile phones, watches, or vehicles, these communities serve a variety of functions. More specifically, a smart city is defined as an urban area which "use[s] new technologies to gather comprehensive data and algorithms to achieve increased efficiency, sustainability, and safety."[1]

Communities have experimented with a variety of approaches to implementing smart technology to enhance the lives of their citizens. Jacksonville, Florida, for example, has created an entire innovation corridor that relies on data from hundreds of remote sensors to facilitate improved transportation and commuting experiences.[2] Other cities, such as St. Louis and Detroit, have installed kiosks that provide a variety of public services, serving as free Wi-Fi hotspots that allow browsing nearby "social and civic resources."[3,4] Smart solutions even extend to waste management, with cities like San Francisco distributing trash bins equipped with sensors that provide live feedback to the city and sanitation crews, communicating which bins are full and where, thus optimizing collection frequency and routes while reducing unnecessary road congestion.[5]



Some cities, such as St. Louis and Detroit, have installed kiosks that provide a variety of public services

While the desired outcomes from the smart city movement, such as reducing waste, increasing efficiency, and anticipating and supporting the needs of a populace, are common to many urban improvement efforts, the privacy impacts may be unique. In the era of the Internet of Things (IoT), cities are leveraging technology and increased data access to construct communities that are more efficient, safer, and smarter than ever. While these outcomes offer great potential for doing good, cities should ensure that foundational policies and safeguards are in place to provide individuals adequate privacy guardrails.



Privacy Concerns for Citizens

One important takeaway from the smart city examples is that the term smart city is not rigidly defined; instead, it is an umbrella term enveloping a plethora of network- or data-based activities. Norman Speicher, a program manager working on smart cities for the U.S. Department of Homeland Security's Science and Technology Directorate, notes that many municipalities "are being pressured and that there's this expectation that they know what 'smart cities' means—and it really means many things to many people."[5] In other words, the novelty and variety of application contribute to a sense of abstractness. This in conjunction with the pressure to adopt exciting, smart solutions to community issues creates fertile grounds for a range of privacy issues, including those of transparency, consent, and the risk of over-surveillance.

Considerations for Smart City Leaders

Leaders of aspiring smart cities should strive for transparency by providing notice of what data is being collected, how it is used, and with whom it is shared. Such notice is necessary to ensure citizens retain control over their information. In the case of urban districts equipped with Wi-Fi connected kiosks, transparency may be achieved via privacy notices similar to those we are accustomed to seeing when engaging with personal smart devices. Indeed, in many cases, the data that smart cities are collecting is anonymized or aggregated so that data about individuals is neither collected nor stored.[7]

However, cities may also choose to collect real-time data about individuals in order to provide more personalized services. Individuals benefit from sharing their personalized data all the time, whether it's for a new book suggestion, real-time GPS navigation to that new taco place, or buyer loyalty programs. However, attitudes toward privacy and comfort with the data sharing required for some of these tools may differ from city to city and person to person. Accordingly, smart cities should be clear about what data they collect and how it is used. They should be transparent about what their data processing intentions are—and those of the companies that lease or provide the equipment and services to the cities.

Another important tenet of privacy is the ability to maintain personal control of one's data. The growing market[8] for smart cities suggests that the number of communities incorporating smart city solutions is on the rise. However, despite this trend, it's still not particularly clear where or when you are present in a smart community.[9] If an individual is not aware that they are passing through the bounds of a smart city, they cannot actively and meaningfully engage in a decision to share their personal data.

While providing adequate notice and opportunities for consent seems like a straightforward solution, examples of smart city applications paint a more complex picture. Consider a community that installs sensors that collect traffic data on public roads: If the proposition is for citizens to either use public roads and consent to data collection or not use the roads at all, can meaningful consent be obtained? Solutions requiring citizens to move to a new community without sensor-equipped roads or perhaps to pay a toll for roads that are sensor-free are impractical and create new equity issues where privacy is only available to those with the means to secure it.

A city could anticipate that taxpayers and regular commuters might use the road and may therefore be able to provide notice to and obtain consent from those individuals. However, this may not be the case with tourists or other infrequent users. If a smart city cannot accurately predict who it is collecting data about until (presumably in such cases) after it has collected that data, then consent is impossible.

Cities and municipalities implementing smart technologies should also minimize information collected to only that which is necessary. For example, cities implementing smart trashcans likely don't need to collect any personal information to function as intended. Where personally identifiable information (PII) is necessary for the technology to function optimally, city leaders should balance the utility of that information with privacy concerns. In order to properly weigh those equities, those implementing smart city technology should have a clear idea of the desired outcome of that technology. Without adequate data minimization practices, smart cities and municipalities may not have a clear idea of what data they possess and how to properly protect it. Additionally, collecting more PII than necessary may put the city or municipality at increased risk during a data breach.

According to a study by the Pew Research Center, more than 80% of Americans believe the potential risks of data collection by companies outweigh the benefits.[12] The same study found that 79% of Americans are "very or somewhat concerned" about how companies are using the data collected about them, while more than six out of 10 Americans feel the same about data collected by the government.

With Americans lacking confidence that their data will be treated and handled appropriately, civic leaders must be sensitive to how local perspectives might hinder the efficiency, sustainability, and particularly the safety-related goals of smart city projects. Mass implementation absent public buy-in could prove to be a poor investment, particularly with increasing societal awareness and public attention growing the conversation around data privacy norms.[13]

Smart City Surveillance

Smart kiosks in Detroit, Michigan, serve a variety of purposes, including providing job listings, maps and navigation assistance, and access to municipal services such as city council agendas and emergency alerts.[10] They provide details on nearby attractions, retail, food, arts, and culture. These kiosks are also notable for what features they lack, such as high definition security cameras, opinion polls and games, and a photo booth that can integrate with social media.[11]

The absence of a camera is notable, not just because it is perhaps the only such instance of a city using these kiosks with the camera disabled, but also because it could enhance functions such as the emergency notification feature. In Detroit, at least, community concerns of police surveillance have far outweighed the public safety benefits. Other communities, particularly those with widespread usage of cameras, should balance increased data collection and the public's privacy concerns. While the norms and expectations of privacy are clearly different in public spaces than private, cities should be wary of a one-size-fits-all approach.

According to a study by the Pew Research Center, more than 80% of Americans believe the potential risks of data collection by companies outweigh the benefits.

Solutions for Smart Cities

Having identified just a few of the important considerations smart city leaders should take into account prior to implementing these technologies, there are several potential solutions for city and municipal governments. The first is to create a dedicated privacy office to ensure that privacy controls are built into these technologies and address any of the public's privacy concerns. For example, the city of Oakland, California, has created a Privacy Advisory Commission to keep the city informed of "best practices to protect Oaklanders' privacy rights in connection with the city's purchase and use of surveillance equipment and other technology that collects or stores"[14] personal data.

Among other roles, the Oakland commission submits yearly reports and recommendations to the city council regarding the city's use of surveillance equipment and whether new privacy and data retention policies should be developed or amended. Along with Oakland, cities including Seattle[15] and New York City[16] have also devoted specific resources to oversee and address community privacy issues, creating Chief Privacy Officer roles in their city governments. While resources will vary across the board, it's important to remember that communities can enlist outside privacy experts to assess and address privacy issues.

An Educated Citizenry

Cities and municipalities should seek to educate their citizens on the smart technology they deploy and any potential privacy concerns. Education is critical to both consent and transparency. The education effort should start with identifying the data processing activity and any legal basis for the activity, if applicable. The next step should be creating a mechanism for individual consent. The most effective way to achieve this will vary depending on the scenario at hand, but the request should be made in plain language and be easily accessible. Finally, individuals should be provided with a clear way to withdraw consent, if desired, ideally without losing access to the service in question. Consent and notice should be paired so that the person has a clear understanding of their choice and how to manage that choice moving forward.

Providing notice and obtaining consent should be closely tied to understanding and accounting for local attitudes on surveillance and the data processing that may accompany smart city activities. Just as attitudes held by citizens and individuals toward privacy and smart city technologies may evolve over time, the smart city tools could transform as well. For this reason, it is necessary to develop and adopt a framework for considering data privacy issues. This framework should be based on established best practices, but more critically, it should be developed with local perspectives, customs, and values at the forefront. Cities and municipalities are best equipped for determining how to effectively survey the citizens and individuals impacted by their decisions, whether through townhalls, relying on elected representatives, or other methods. However, there are many examples today of such frameworks which might be leveraged or serve as a starting point.[17]

In addition to adopting data privacy ethics frameworks, cities should consider standardizing their approach to privacy issues writ large. For example, the National Institute of Standards and Technology (NIST) has established a set of privacy controls used to enforce privacy requirements and best practices, which cities can leverage to ensure that privacy is built into their organization, systems, and programs and that assess their privacy posture on a continuing basis.[18] In 2020, NIST updated their security and privacy controls to specifically account for IoT devices.[19] While a consensus on the long-term impact of the control revisions remains to be seen, it is one that appears particularly relevant for smart cities.

Similarly, cities may consider conducting privacy impact assessments (PIAs) on their smart city technology to determine, document, and communicate how data is collected, stored, used, and shared. PIAs can provide insight into potential gaps in the privacy safeguards that support smart city initiatives. In addition, conducting a privacy risk analysis can lead to increased transparency, not only in terms of what risks are posed (if made available publicly), but also in terms of transparency of the process and what risks are being considered or omitted. PIAs should tell the story of the data through its lifecycle from a technical perspective, but more importantly, illuminating the effect of technology on social, economic, and community considerations as well.

Next Steps for Smart Cities

While a national consensus on the privacy governance of smart cities is still evolving, it is clear that states and their cities and municipalities are well positioned to fill the void. They can come to their own consensus on defining the limits of smart cities and instituting meaningful privacy frameworks. Because communities' needs can differ drastically, smart solutions to community problems and inefficiencies may well differ, too. However, this should not deter policymakers from seeking custom solutions within the broader frameworks.

In addition, cities and municipalities should strongly consider enlisting the help of experienced privacy professionals to assess and address their transparency and compliance efforts and establish best practices. With the IoT and the smart city era still in its infancy, it is time to lay a proper foundation for the profound data privacy considerations and opportunities on the horizon.

Footnotes

[1] Chad Marlow and Maryiam Saifuddin. September 17, 2018. “How to Stop ‘Smart Cities’ from Becoming ‘Surveillance Cities.’” American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-stop-smart-cities-becoming-surveillance-cities.

[2] Carole Hawkins. December 19, 2019. “Florida Cities Get Smart With ‘The Internet of Things.’” The News-Journal. https://www.governing.com/news/headlines/Florida-Cities-Get-Smart-With-The-Internet-of-Things.html.

[3] The City of St. Louis, Press Release Desk, News Partner. January 24, 2020. “Smart City Digital Kiosks New to St. Louis.” St. Louis Development Corporation. https://patch.com/missouri/stlouis/smart-city-digital-kiosks-new-st-louis.

[4] Christine Ferretti. October 9, 2019. “New Kiosks in Downtown Detroit Will Search but Not Surveil.” The Detroit News. https://www.governing.com/news/headlines/New-Kiosks-in-Downtown-Detroit-Will-Search-but-Not-Surveil.html.

[5] Rebecca Heilweil. July 5, 2019. “Smart City Trash Cans Are Already Here. And They Do Things You’d Never Imagine.” https://cheddar.com/media/smart-city-trash-cans-are-already-here-and-they-do-things-youd-never-imagine.

[6] Brandi Vincent. August 28, 2019. “DHS Launches Smart City Sensor Pilot in St. Louis.” Nextgov. https://www.nextgov.com/emerging-tech/2019/08/dhs-launches-smart-city-sensor-pilot-st-louis/159517/.

[7] Claudia Geib. November 7, 2017. “Smart Cities May Be The Death of Privacy As We Know It.” https://futurism.com/privacy-smart-cities.

[8] https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html (forecasting a compound annual growth rate [CAGR] of 18.4% from 2018–2023).

[9] Emilie Scott. February 28, 2019. “The Trouble with Informed Consent in Smart Cities.” The International Association of Privacy Professionals. https://iapp.org/news/a/the-trouble-with-informed-consent-in-smart-cities/ (arguing that the typical person has no way of recognizing a smart city or providing informed consent when engaging with smart city technologies).

[10] Christine Ferretti. October 9, 2019. “New Kiosks in Downtown Detroit Will Search but Not Surveil.” The Detroit News. https://www.governing.com/news/headlines/New-Kiosks-in-Downtown-Detroit-Will-Search-but-Not-Surveil.html.

[11] Ibid.

[12] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. November 15, 2019. “Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information.”
Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[13] Ibid.

[14] Privacy Advisory Commission. https://www.oaklandca.gov/boards-commissions/privacy-advisory-board.

[15] Rosalind Brazel. July 11, 2017. “City of Seattle Hires Ginger Armbruster as Chief Privacy Officer.” Tech Talk Blog. https://techtalk.seattle.gov/2017/07/11/city-of-seattle-hires-ginger-armbruster-as-chief-privacy-officer/.

[16] Official Website of the City of New York, Press Release. April 3, 2018. “Mayor de Blasio Appoints Laura Negrón As Chief Privacy Officer.” NYC.gov. https://www1.nyc.gov/office-of-the-mayor/news/167-18/mayor-de-blasio-appoints-laura-negr-n-chief-privacy-officer.

[17] UN Global Pulse. Building Ethics Into Privacy Frameworks for Big Data and AI. IAPP. https://iapp.org/media/pdf/resource_center/BUILDING-ETHICS-INTO-PRIVACY-FRAMEWORKS-FOR-BIG-DATA-AND-AI-UN-Global-Pulse-IAPP.pdf.

[18] National Institute of Standards and Technology (NIST). April 2013. Special Publication (SP) 800-53, Rev. 4, Appendix J. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[19] NIST. September 2020. SP 800-53, Rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia, and offices worldwide, our firm employs nearly 27,200 people and had revenue of $7.5 billion for the 12 months ending March 31, 2020. To learn more, visit BoozAllen.com. (NYSE: BAH)