Journal of Law and Mobility

Volume 2022

2022

Privacy Frameworks for Smart Cities

Lindsey Tonsager

Jayne Ponder

PRIVACY FRAMEWORKS FOR SMART CITIES

LINDSEY TONSAGER & JAYNE PONDER

Cite as: Lindsey Tonsager & Jayne Ponder, *Privacy Frameworks for Smart Cities*, J. L. & Mob. 6.

I. INTRODUCTION

Smart infrastructure and transportation for city operations ("smart cities") have the potential to enhance the delivery of government services and tackle a range of societal problems, including managing traffic congestion,[1] reducing carbon emissions,[2] facilitating efficient waste management,[3] improving public health outcomes, constructing affordable housing, and enabling residents to efficiently access government services.[4] The COVID-19 pandemic also underscored the opportunity for smart cities to improve public health outcomes. For example, New York City launched an app for residents to more easily store and present their vaccine record and COVID-19 testing information.[5] Additionally, Kansas City, Missouri installed air quality sensors in areas of high COVID-19 transmission to help reduce infection rates and improve air quality as part of a grant program with the National Science Foundation, a project that was later expanded to Cleveland, Ohio and Chattanooga, Tennessee.[6] There are smart cities projects around the globe, with 379 fully

---

[1] *See* Press Release, N.Y.C. Dep't of Transp., *NYC DOT Announces Expansion of Midtown Congestion Management System, Receives National Transportation Award* (June 5, 2012), https://www1.nyc.gov/html/dot/html/pr2012/pr12_25.shtml.
[2] *Copenhagen*, World Smart Cities Forum (Oct. 14, 2019), https://worldsmartcities.org/copenhagen/?msclkid=c1451bbbd15911eca302d0f6add159e9.
[3] *See* Levi Sumagaysay, *San Francisco's Trash Bins Get Smart*, THE MERCURY NEWS (Feb. 27, 2019), https://www.mercurynews.com/2019/02/27/san-franciscos-trash-bins-get-smart/ (explaining San Francisco's waste bin smart sensors that can detect how full they are to reduce trash pickup time).
[4] *LifeSG*, Smart Nation Singapore, https://www.smartnation.gov.sg/initiatives/strategic-national-projects/lifesg (last visited Oct. 24, 2022).
[5] *See NYC Covid Safe*, App Store Preview, Apple, Mobile App, https://apps.apple.com/us/app/nyc-covid-safe/id1565213506 (last visited Oct. 19, 2022).
[6] *See* Josh Schacht, *Air Quality Sensors Track COVID-19 Activity in Kansas City*, GOV'T TECH. (Aug. 30, 2021), https://www.govtech.com/analytics/air-quality-sensors-track-covid-19-activity-in-kansas-city.

developed smart cities in 61 countries in 2019.[7] Analysts predict that the smart cities market will top $7 billion by 2023.[8]

A typical smart city initiative might involve internet-connected sensors, mobile apps, public WiFi offerings, high-speed communications networks, utility meters, and cameras. With these operations, smart cities could collect and use a large quantity of data, some of which could be sensitive in nature. Additionally, smart cities technologies might involve processing data with assistance from analytics tools and algorithms. Consequently, commentators have raised privacy concerns that smart cities' potential collection of significant amounts of information about residents, as well as new uses and methods of processing this information could contribute to government surveillance and cybersecurity risks, among other privacy concerns.

Privacy questions have had an influential role in the development and outcome of prior proposed smart cities initiatives. For example, Alphabet's subsidiary Sidewalk Labs announced plans to build a high-tech neighborhood on 12 acres of Toronto's waterfront in 2017, estimated to reflect at least a $1 billion investment, often called the Toronto Quayside project for the name of the neighborhood.[9] Citizens and privacy advocates raised concerns that the proposed plans could compromise residents' privacy interests.[10]

---

[7] *See* Sommer Mathis & Alexandra Kanik, *Why You'll be Hearing a lot Less About 'Smart Cities,'* CITY MONITOR, (Feb. 18, 2021), https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities.

[8] *See* Precedence Research, *Smart Cities Market Size to Surpass US$7,162.5 BN by 2030*, GLOBAL NEWSWIRE (May 10, 2022), https://www.globenewswire.com/en/news-release/2022/05/10/2439944/0/en/Smart-Cities-Market-Size-to-Surpass-US-7-162-5-BN-by-2030.html.

[9] *See* David George-Cosh & Eliot Brown, *Google Parent Nears Deal to Build Its Vision of a City in Toronto*, WALL ST. J. (Oct. 4, 2017), https://www.wsj.com/articles/alphabets-city-building-unit-nears-development-deal-in-toronto-1507142561.

[10] *See* Reuters, *Alphabet's Smart City Unit Just Released its Master Pplan for a Toronto Waterside District, Promising Not to Sell the Personal Data it Collects on Residents*, BUSINESS INSIDER (Jun. 24, 2019), https://www.businessinsider.com/alphabet-commits-to-data-privacy-in-toronto-smart-city-master-plan-2019-

(continued…)

Cities play an important role in the responsible integration of smart cities technologies to address these privacy concerns and safeguard public trust. This paper identifies some of the core privacy considerations raised by smart cities – government surveillance and data security in Part I. Then, Part II proposes a set of core principles for smart cities to consider in the development and deployment of smart cities to address privacy concerns. These principles include: (A) human-centric approaches to smart cities design and implementation, (B) transparency for city residents, (C) privacy by design, (D) anonymization and deidentification, (E) data minimization and purpose specification, (F) trusted data sharing, and (G) cybersecurity resilience.

II. PRIVACY CONSIDERATIONS FOR SMART CITIES

Privacy considerations in smart cities development and adoption are raised across academic commentary, public reporting, and past smart cities pilots, and generally focus on concerns over government surveillance and data security.

With respect to government surveillance, some commentators have voiced concerns that the implementation of smart cities technologies runs the risk of chilling First Amendment expression, as residents might be less willing to participate in free speech and public assembly if they perceive they are being recorded by the city.[11] For example, the White House's recent Blueprint for an Artificial Intelligence ("AI") Bill of Rights, the Office of Science and Technology Policy found that individuals and communities "should be free from unchecked surveillance" and technologies like AI should not limit the exercise of civil rights and civil liberties, such

---

6#:~:text=A%20high%2Dtech%20smart%20city,master%20plan%20released%20on%20Monday.

[11] *See, e.g.*, Tarun Wadhwa, *Smart Cities: Toward the Surveillance Society?*, *in* SMART CITIES AS DEMOCRATIC ECOLOGIES 125–141 (Daniel Araya, ed., 2015), https://link.springer.com/content/pdf/10.1057/9781137377203_9.pdf; Robert Muggah & Greg Walton, *'Smart' Cities Are Surveilled Cities,* FOREIGN POLICY (Apr. 17, 2021, 6:00 AM), https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/; *see also* Tara Morgan, *New Report Calls Out City of Cleveland for Lack of Transparency in Police Surveillance Technology*, NEWS 5 CLEVELAND (May 10, 2022, 6:16 PM), https://www.news5cleveland.com/news/local-news/new-report-calls-out-city-of-cleveland-for-lack-of-transparency-in-police-surveillance-technology.

as with respect to voting, peaceful assembly, speech, or association.[12] At the same time, however, state and local governments have used technology to facilitate citizens' First Amendment right to vote through the creation of mobile apps that help citizens connect with information about how, where, and when to vote.[13]

Regarding data security risks, privacy advocates and commentators have raised concerns that because smart cities might collect a large quantity of information, some of which may be sensitive in nature, smart cities provide an attractive target for bad actors. For example, city governments have already grappled with the threat of cybersecurity incidents, even outside the smart cities context. In September 2022, a ransomware attacker gained access to the Los Angeles, California Unified School District, and with it, access to student and teacher data, which led the school district to shut down its computer systems.[14] City governments at large have also been affected, as a ransomware attack on the city of Atlanta caused the city government to shut down its systems in 2018,[15] and a bad actor accessed all of the 156 emergency sirens in Dallas, Texas in 2017.[16]

Nevertheless, there are bright spots suggesting cities can do data security well using smart technologies. Members of Congress have introduced several bills that would, among other things, create literacy for small businesses on cybersecurity best practices and establish voluntary cybersecurity certification programs for IoT

---

[12] Office of Science and Technology Policy, The White House, *Blueprint for an AI Bill of Rights*, Privacy 6, 30, 34 (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[13] *See* Go Vote TN App; Ohio Voter Info App; Hudson County Votes (Hudson County, NJ) App.

[14] *See* Associated Press, *A Cyberattack Hits the Los Angeles School District, Raising Alarm Across the Country*, NPR (Sept. 7, 2022), https://www.npr.org/2022/09/07/1121422336/a-cyberattack-hits-the-los-angeles-school-district-raising-alarm-across-the-coun#:~:text=The%20attack%20on%20the%20Los,students%20and%2070%2C000%20district%20employees.

[15] *See* Alan Blinder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder*, N.Y. TIMES (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

[16] *See* Samira Said, *Hacker Sets Off Emergency Alarms, Frightening Dallas Residents*, CNN (Apr. 9, 2017, 9:40 AM), https://www.cnn.com/2017/04/08/us/dallas-alarm-hack.

devices.[17] Likewise, the National Institute of Standards and Technology ("NIST") has issued reports and best practices recommendations related to cybersecurity and IoT devices, including some specific to government operations such as the NIST Security Guidance for First Responder Mobile and Wearable Devices, which helps secure devices worn in emergency response operations.[18] Additionally, partnerships with private actors can help smart cities strengthen cybersecurity resilience.

Accordingly, any smart cities framework should be calibrated to consider how to minimize privacy risks while maximizing benefits to citizens and government efficiency.

III. SAFEGUARDING PRIVACY IN SMART CITIES

Cities play a critical role in ensuring public trust with the deployment of technologies for city government. This Section explains each of the key privacy principles in turn, and discuss how these principles can help address privacy concerns raised with smart cities. These principles include: (A) human-centric approaches to smart cities design and implementation, (B) transparency for city residents, (C) privacy by design, (D) anonymization and deidentification, (E) data minimization and purpose specification, (F) trusted data sharing, and (G) cybersecurity resilience. These principles are informed by numerous privacy frameworks, such as those proposed by the Organization for Economic Co-operation and Development ("OECD"), NIST, and the Asian-Pacific Economic Corporation ("APEC"), as well as existing laws in the European Union and the United States.

A. Human Centered Smart Cities

Because smart cities rely on the trust and confidence of its residents, smart cities should prioritize a human-centered approach to designing and operating smart cities to help allay privacy concerns

---

[17] *See, e.g.*, American Cybersecurity Literacy Act, H.R. 4055, 117th Cong. (2021); Cyber Shield Act of 2021, S. 965, 117th Cong. (2021) (creating a voluntary cybersecurity certification program).

[18] *See* NIST Security Guidance for First Responder Mobile and Wearable Devices (Jul. 2022), https://csrc.nist.gov/publications/detail/nistir/8235/final; *see also* NIST Seeks Comment on the Initial Public Draft of its Profile of the IoT Core Baseline for Consumer IoT Products (Sept. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf (requesting comments on cybersecurity labeling criteria for IoT devices).

like government surveillance and data security. Some critics of smart cities have reflected that smart cities advocates overlook the importance of individuals in the pursuit of deploying smart cities technologies.[19] Thus, in order to be successful and address privacy concerns, smart cities must therefore routinely engage with its residents to understand the benefits smart cities might bring to bear for residents, analyze how smart cities can be designed to benefit all residents equitably, appreciate the unique norms and culture of a city that will determine what smart cities implementations are appropriate, attend to concerns about resident privacy, and promote trust and accountability.

The Toronto Quayside project provides an example of the importance of incorporating residents in the process of designing and deploying smart cities. The Toronto Quayside project involved a partnership with Sidewalk Labs to build a smart city "from the internet up."[20] Not long after the project was announced, the Toronto Quayside project drew criticism for dismissing privacy concerns, which led four members of the project's advisory board to quit the project "over concerns about privacy and lack of public input."[21] As this example underscores, involving residents in the process of designing and building smart cities is critical to help ensure that the smart cities project reflects the norms and culture of the city and has the support of city residents.

B. Transparency

Transparency allows residents to shape the development of smart technologies in their city and understand the nature and extent of processing of their personal information to make informed choices about their information. In this way, transparency can help address

---

[19] *See* Karrie Jacobs, *Toronto Wants to Kill the Smart City Forever,* MIT TECH. REV. (Jun. 29, 2022), https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city/; *see also* Riad Medded & Calum Handforth, *We Need Smarter Cities, Not "Smart Cities,"* MIT TECH. REV. (Jun. 27, 2022), https://www.technologyreview.com/2022/06/27/1053896/we-need-smarter-cities/ (reflecting that a focus on smart cities "talk[s] about 'users' rather than people" and "[m]onthly and 'daily active' numbers instead of residents").

[20] Sidney Fussell, *The City of the Future Is a Data-Collection Machine*, THE ATLANTIC (Nov. 21, 2018), https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/.

[21] *Id.*

concerns about government overreach because residents and civil society stakeholders can monitor and take action in potential instances of government overreach. Transparency – in particular, the principle that people should be informed over how their information is collected and used – is foundational across global data protection frameworks.[22]

Transparency has long been a central aspect of the U.S. privacy framework. The Fair Information Practices, a 1970s government report identified principles for fair government processing of information that provide the foundation for modern U.S. privacy requirements, one of which is the principle of transparency.[23] With respect to presentation of notices, the Federal Trade Commission ("FTC") has recommended that entities make disclosures to consumers "at a relevant time and in a prominent manner" (and provide choice) to individuals, in instances where personal information collection is inconsistent with what consumers might expect.[24] The California Privacy Rights Act, which enters into effect January 1, 2023, requires that a business provide notice "at or before the point of collection" to consumers.[25]

While global frameworks are not uniform with respect to the content required in such notices, many privacy frameworks call for notice that includes the purposes for which personal information is being collected, used, and shared; recipients of the data (including third parties); and information about any applicable choices with respect to that data.[26]

Although transparency has been a longstanding principle in privacy frameworks, the nature of smart cities technologies and their integration with city government raises novel challenges for

[22] The GDPR, U.S. state privacy laws, and other global frameworks likewise contemplate some form of transparency with respect to how individuals' information is collected, used, and shared. *See, e.g.*, GDPR, Articles 13 & 14.
[23] *See* Federal Privacy Council, *Fair Information Practice Principles* (last visited Oct. 24, 2022), https://www.fpc.gov/resources/fipps/.
[24] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change* 27 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[25] Cal. Civ. Code § 1798.100(a) (effective Jan. 1, 2023).
[26] *See, e.g.*, Asia-Pacific Economic Cooperation, APEC PRIVACY FRAMEWORK (2005); U.S. Dep't of Health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens* (1973); FTC, *supra* note 34.

transparency. First, the reality of developing technologies means that the way in which residents interact with the tool may not be through a traditional account signup process or on a screen. This presentation likely requires that smart cities think creatively about how to provide notice to residents. For example, where smart cities use sensors to collect data automatically, providing notice may include using QR codes that link to a city's privacy disclosures or providing public signage about when sensors or in use. Cities could also use standardized images in these signs where appropriate to signal to residents when sensors or cameras are in use. As another example, cities can develop privacy portals or hubs where citizens can go to access comprehensive information about how technologies deployed throughout the city might process personal information.

C. Privacy by Design

Privacy by design can help allay privacy concerns related to smart cities, including those related to government surveillance and data security, as privacy by design requires a proactive consideration of privacy risks and available safeguards. Privacy by design has been recognized in global privacy frameworks, including in the Global Data Protection Regulation ("GDPR"), in FTC guidance, and most recently, in the proposed legislative text for the American Data Privacy and Protection Act, the leading bipartisan U.S. federal legislative framework for privacy.[27]

Privacy by design is not a new concept for smart cities. Seattle implemented a programmatic privacy review process that assists city government officials in collecting and using data.[28] Designed to provide "structure and guidance" for city agencies to build confidence in how residents' personal information is used, the privacy program asks Seattle officials to complete a privacy impact assessments to review how data is collected and managed by a project or proposal through a series of questions.[29]

---

[27] *See* FTC, *supra* note 34, at vii, 22; *See* GDPR, Art. 25; *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).
[28] *See* City of Seattle, *About the Privacy Program*, https://www.seattle.gov/tech/initiatives/privacy/privacy-program (last visited Oct. 20, 2022).
[29] *See id.; see also* City of Seattle, *Privacy Reviews of City Technology*, https://www.seattle.gov/tech/initiatives/privacy/privacy-reviews (last visited Oct. 24, 2022).

Privacy assessments can serve as a component of a privacy by design program, like the one deployed in Seattle.[30] Recently, the Dutch Data Protection Authority issued recommendations for smart city applications that include a recommended data protection impact assessments before the integration of smart cities technologies to assess privacy risks and potential safeguards available.[31] Additionally, the White House Blueprint for an AI Bill of Rights recognized that pre-deployment assessments and ongoing assessments of privacy and surveillance considerations would be appropriate for some applications of technology that could be used for surveillance purposes "to protect privacy and civil liberties."[32] Impact assessments also help address privacy concerns of government surveillance and data security, as the impact assessment would require the city to examine who would be allowed to have access to the data, what safeguards and policies should be in place, and how the data should be protected. Likewise, impact assessments promote public trust through transparency with citizens about how their data is used and managed.

D. Anonymization and Deidentification

Importantly, not all data collection necessarily raises the same types and degrees of privacy concerns. Privacy interests are arguably substantially lessened where information cannot be associated with a particular individual – for example, data in aggregated or deidentified forms. Many data privacy frameworks explicitly exclude aggregate and deidentified information from its scope.[33]

---

[30] Privacy impact assessments are required by some U.S. state privacy statutes, depending on the nature of the processing. *See, e.g.*, Colo. Rev. Stat. § 6-1-1309 (requiring assessments for processing that presents a heightened risk of harm for consumers, such as profiling, the processing of sensitive data, and targeted advertising) (effective July 1, 2023).

[31] *See* Press Release, Autoriteit Persoonsgegevens, *The Dutch DPA Issues Recommendations for Smart Cities*, (Jul. 30, 2021), https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-issues-recommendations-smart-cities.

[32] Office of Science and Technology Policy, *supra* note 15, at 6, 30.

[33] *See, e.g.*, Cal. Civ. Code § 1798.140(v)(3) (excluding deidentified and aggregate information from the scope of personal information). *See, e.g.*, Cal. Civ. Code § 1798.140(b) (defining aggregate consumer information) (effective Jan. 1, 2023); Cal. Civ. Code § 1798.140(m) (defining deidentified consumer information) (effective Jan. 1, 2023).

Relying on aggregate and deidentified information wherever possible, instead of personal information, could help city governments unlock the potential benefits of smart cities, while also managing privacy concerns. For example, environmental sensors that measure temperature, air quality, and humidity would address privacy concerns, as would sensors that measure the amount of trash in a bin. Additionally, collection of information about the number of cars that travel through an intersection at a given time – not the type, make, model, or license plate of the vehicle – could help a city reduce congestion without implicating serious privacy concerns. Consequently, cities could consider as a principle prioritizing the collection and use of aggregated and deidentified data whenever feasible to address privacy concerns with smart cities development and implementation.

Nevertheless, absent processes and controls to prevent reidentification, deidentification and anonymization alone might not address privacy concerns due to the ability to reidentify datasets and should be coupled with policies and procedures to prohibit reidentification.[34] Even where data has been pseudonymized or deidentified, academics have raised concerns about the use of big data or other data sets to reveal previously anonymous portions of the data or enable complete reidentification.[35] Thus, smart cities should consider policies, procedures, and safeguards to prohibit reidentification and refrain from storing data longer than required. As at least one academic commentator noted, deidentification may not be the only solution, but it has a role to play.[36]

E. Data Minimization & Purpose Specification

Smart cities could adopt the "less is more" principle of data minimization to help respond to concerns about government over-collection of personal information and surveillance. Data minimization describes collecting and maintaining the minimum amount of data required for a particular purpose.[37] Like transparency, data minimization is a principle grounded in the Fair Information

[34] *See* Woo, *supra* note 20, at 961.
[35] *Id.* (citing example where researchers re-identified medical records using sex, date of birth, and zip code of patients).
[36] *See id.* at 967.
[37] *See, e.g.*, Information Commissioner's Office, *Data Minimisation Principle*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#data_minimisation (last visited Oct. 20, 2022).

Practice Principles[38] and is a common theme across global privacy frameworks.[39]

Data minimization helps address some of the privacy concerns raised in the context of smart cities.[40] A frequently cited concern with smart cities is that the over collection of personal information that could be used for government surveillance or that, when data collected by the smart city is stored together, attracts bad actors seeking to obtain unauthorized access. However, if smart cities limit the volume and types of data collected, this helps address concerns that government agencies can use and analyze information for purposes of government surveillance.

F. Trusted Data Sharing

Smart cities will need to work with partners and vendors to source and facilitate the technology used for smart cities, a process that will necessitate sharing some personal information collected by smart cities with partners. Absent some data sharing, cities may not be able to provide smart solutions if they lack the necessary technical infrastructure, robust security measures, or to share data with researchers (e.g., to validate their efficacy of their solutions, promote transparency, or enable additional technological developments). Moreover, data sharing helps ensure that smart city technologies are designed, trained, and tested with datasets that represent the diversity of the city's population and avoids unintended biases.

Such sharing can be accomplished in a way that fosters trust and confidence with the individuals about whom the data relates. For instance, contractual terms that delegate the roles, responsibilities, and rights of the city and the relevant data recipient with respect to personal information can provide assurances to the city and to residents that the recipient must use their data responsibly and in line with any specific provisions of the contract.[41] In coordination with the University of Washington, the City of Seattle undertook a review of vendor contracts to understand whether vendors with access to

[38] *See supra* note 33.
[39] *See* GDPR, Art. 5. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); FTC, *Complying with COPPA: Frequently Asked Questions* (Jul. 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.
[40] *See* Woo, *supra* note 20, at 968.
[41] *See, e.g.* Colo. Rev. Stat. § 6-1-1305(2) (requiring that processors adhere to the instructions of the controller) (effective Jul. 1, 2023).

city data were contractually obligated to adopt best practices for privacy and cybersecurity, and the findings of this study led to the city renegotiating contracts with a vendor so that these protections were in place.[42]

Additionally, certification programs for vendors or other third parties that are in line with privacy principles can also provide an easy mechanism for cities and residents to identify whether the recipient of smart city data has undergone vetting of their privacy and security programs. Certification programs have had some success in other privacy contexts. For example, the Children's Online Privacy Protection Act ("COPPA") allows the FTC to approve self-regulatory guidelines that implement the protections of the COPPA Rule.[43] The creation and adoption of certification programs could serve as a valuable mechanism to innovate on privacy best practices for smart cities and provide a means for residents to easily understand how smart cities partners are processing their personal information.

G. Cybersecurity Resilience

Data security is critical to both addressing smart cities privacy concerns and fostering public trust. Smart cities can adopt a cybersecurity program similar to that included in global privacy frameworks. For example, many privacy frameworks include a security principle to ensure that personal information is only used by those authorized to do so and safeguarded in a reasonable manner, taking into account the nature of the underlying data and the purposes for processing.[44] In the smart cities context, this could mean implementing access controls to limit who and what types of personnel can access certain types of resident data collected by the smart city. For example, data from a traffic light sensor collecting aggregated data about congestion (i.e., 100 cars passed through an

---

[42] *See* Woo, *supra* note 20, at 969.

[43] *See* 15 U.S.C. § 6503 (providing a safe harbor for companies that comply with FTC approved self-regulatory guidelines).

[44] *See* FTC, *Start with Security: A Guide For Businesses* 1 (June 2015) (noting that companies should make "reasonable choices based on the nature of their business and the sensitivity of the information involved" regarding cybersecurity), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *See also* 201 Mass. Code Regs. 17.00, https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf (requiring entities to implement a cybersecurity program that takes into account factors such as their size, scope, resources, and the nature of the data collected).

intersection during rush hour) might be limited to those who service and operate the traffic light and may not be available to, for example, law enforcement or government personnel determining benefits entitlement. Smart cities can also put in place procedures like multi-factor authentication to verify the identity of the individual seeking to access the data. In considering cybersecurity safeguards, smart cities can learn from other government entities, such as those at the federal and state level, and might identify support and resources from grant programs, such as the $1 billion cybersecurity grant program for state and governments allocated in the Bipartisan Infrastructure Law.[45]

Not only does cybersecurity resilience protect residents against harm from malicious actors, but robust cybersecurity also furthers public confidence and trust in the smart city project.

IV. CONCLUSION

Smart cities offer tremendous opportunity to improve how citizens experience and benefit from their city governments. Cities have an important role to play in adopting a privacy framework – such as through the adoption of principles like those described in this paper – to address privacy concerns and foster public trust and confidence in smart cities projects. Privacy in smart cities can be a feature, not a bug, and the principles outlined in this paper can help provide a framework for the responsible adoption of smart cities projects.

[45] Bipartisan infrastructure bill and references to (1) electric vehicle charging section and (2) state and local government cyber fund. *See* Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 70612(a), 135 Stat. 429, 1272, 1285) (2021), https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf.