Let's Not Be Dumb: Government Transparency, Public Records Laws, and "Smart City" Technologies

Amy Kristin Sanders  
*University of Texas at Austin*

Daxton R. Stewart  
*Texas Christian University*

Follow this and additional works at: [https://scholarship.law.ufl.edu/jlpp](https://scholarship.law.ufl.edu/jlpp)

**Recommended Citation**  
Available at: [https://scholarship.law.ufl.edu/jlpp/vol33/iss2/1](https://scholarship.law.ufl.edu/jlpp/vol33/iss2/1)

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in University of Florida Journal of Law & Public Policy by an authorized editor of UF Law Scholarship Repository. For more information, please contact rachel@law.ufl.edu.
LET’S NOT BE DUMB: GOVERNMENT TRANSPARENCY, PUBLIC RECORDS LAWS, AND “SMART CITY” TECHNOLOGIES

Amy Kristin Sanders* & Daxton R. Stewart**

Abstract

As the tools to automate our lives become more commonplace, so do the concerns about their use and the data they collect. State and local governments in the United States are increasingly turning to smart city technologies for everything from law enforcement and traffic management to public health monitoring and wastewater testing. Yet often, citizens are left in the dark about the ways in which their elected officials are researching, purchasing, and implementing these technologies. Public records laws represent one mechanism to help improve the public’s understanding of smart city technology and its uses in their communities. But not all public records laws are created equal. We argue that public records laws must be updated to ensure the definition of the term “public records” includes the types of records created by these technologies, including audio, video, and large datasets. Additionally, exemptions to public records laws that were designed to prevent invasions of privacy or ensure law enforcement could investigate crime must be narrowly tailored so they cannot be used as an excuse to withhold information that citizens have a right to access. Strong public oversight is crucial to guarantee these technologies are not abused, and most state public records laws are inadequate when it comes to ensuring access to records about, and created by, smart city technology.

INTRODUCTION ................................................................. 168

I. THE BENEFITS AND CONSEQUENCES OF SMART CITY TECHNOLOGY ........................................... 171

II. CITIZENS’ RIGHTS IN A SMART CITY ........................................ 173
   A. Using Public Records Laws to Advance Citizens’ Rights .................................................. 174
   B. Public Records Laws Must Broadly Define Records ......................................................... 178
   C. Public Records Laws Must Narrowly Define Privacy Exemptions .................................... 179
D. Public Records Laws Must Narrow the Law Enforcement Exemption ................................................. 180

CONCLUSION: THE ESSENTIAL ROLE OF PUBLIC RECORDS LAW IN UPHOLDING CITIZENS’ RIGHTS ................................................................. 181

INTRODUCTION

Americans heading out to protest the U.S. Supreme Court’s summer 2022 decision to overturn Roe v. Wade had more to think about than their 1970s predecessors.1 The rise in smart city technologies means it is more likely that local, state, and federal government agencies can identify them and track their movements. It came to light that Baltimore, Maryland, used facial recognition technology as individuals gathered in protest of the 2015 police killing of Freddie Gray, identifying members of the crowd who had outstanding warrants and arresting them at the protest.2 Since then, facial recognition has been used by police during protests in other major cities, including New York, Miami, and Washington, D.C.3 But it is not just facial recognition technology that should concern protestors—the rise of smart city technologies increase the reach of near-constant surveillance.

From cameras to sensors and microphones to mobile phone apps, smart city technologies have become mainstream. State and local governments have become particularly interested in these technologies because of their promises to increase the efficiency of delivering services and to improve the quality of life for residents.4 “Smart cities . . . collect and analyze data. The cities use this data to improve infrastructure, public

1. See Roe v. Wade, 410 U.S. 113, 164 (1973) (holding that the state may not regulate the termination of pregnancy in the first trimester), overruled by Dobbs v. Jackson Women’s Health Org., 142 S. Ct. 2228 (2022). On June 24, 2022, the Supreme Court, in a 6-1 decision, upheld the constitutionality of Mississippi’s Gestational Age Act, which prohibited nearly all abortions after 15 weeks. The majority held there was no constitutional right to an abortion, overruling two previous decisions upholding abortion rights as part of the implied right to privacy. See Dobbs v. Jackson Women’s Health Org., 142 S. Ct. 2228, 2242 (2022).
utilities and services, and more." The technologies have also piqued the interest of consumers, who are purchasing Internet-connected devices in the form of wearables and smart home devices, including Apple’s smart watch and Nest’s smart thermostat. Research suggests exponential growth in the sales of these devices, with the total number of smart devices connected to the Internet rising to 3.75 billion by 2025.

But the technology is not without danger. Smart devices and other Internet-connected devices, commonly dubbed the Internet of Things, may offer conveniences, but privacy experts are troubled by the amount of data they collect. Need to turn down the temperature at your home from your office? Your Nest smart thermostat is collecting this information, documenting the patterns of your energy usage. Security Scorecard detailed the threats these smart devices pose in an August 2021 report. Insecure storage and transfer of data were highest among those concerns.

As more and more consumers, businesses, and governments rely on these technologies, they pose more and more potential dangers. In a recent report, Deloitte pointed to concerns about cybersecurity in municipal infrastructure, public transportation, and healthcare services. These concerns are not new. Professors Woodrow Hartzog and Evan Sellinger offered cautionary words about smart technologies as far back as 2016:

---

5. Fariza Sabrina & Julian Jang-Jaccard, Entitlement-Based Access Control for Smart Cities Using Blockchain, 21 SENSORS 1, 1 (2021) (“Smart cities use the Internet of Things (IoT) devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities, and services.”).


9. Id.

While the IoT might be incredibly useful, we should proceed carefully . . . . Each new camera, microphone, and sensor adds another vector for attack and another point of surveillance in our everyday lives . . . . [T]he nature of the “thing” in the IoT should play a more prominent role in privacy and data security law. The decision to wire up an object should be coupled with responsibilities to make sure its users are protected.11

Despite this warning, very little has been done to regulate these devices to safeguard users’ data. Not all citizens have embraced a reliance on these technologies. Government use of IoT devices and smart city technologies raises significant concerns given the lack of transparency in how they are adopted and implemented. Eugenie Birch, who directs the Penn Institute for Urban Research, voiced those concerns:

I also think there is a lack of rules around the use of technology, so that also makes people quite uncomfortable. Some of these complaints are justified because, in the face of an absence of control around the use of the collected data, it can be like the Wild West out there. Even the providers would welcome more transparency and accountability in this area.12

Ms. Birch is not alone. Numerous advocacy groups, including the American Civil Liberties Union13 and Amnesty International,14 have publicized their concerns about facial recognition technology, noting its impact on citizens’ constitutional rights. Another controversial technology known as ShotSpotter purports to detect gunshots.15 Based on concerns about effectiveness, community organizations have demanded Chicago officials stop using the “smart” microphones, which report

directly to the police. Even researchers at Northwestern University’s MacArthur Justice Center doubt the value of the technology, documenting more than 40,000 errant reports in twenty-one months.

Public records laws represent one legal tool to improve transparency and accountability for governments implementing smart technologies. In the first part of this Article, we outline the potential benefits and drawbacks of these technologies. Then we argue that citizens have certain rights in a smart city. To advance those rights, we examine the role that public records laws play in providing stronger oversight. We argue that three key aspects of public records laws must be evaluated to ensure they adequately address smart city technologies: the definition of record as well as the scope of the privacy and law enforcement exemptions. We conclude that there is a need for stronger public records laws to ensure stronger oversight as more and more governments adopt smart city technology.

I. THE BENEFITS AND CONSEQUENCES OF SMART CITY TECHNOLOGY

Governments implement these smart technologies for their common core function: monitoring. This monitoring function brings with it both benefits and consequences. These technologies may offer government officials early notification that something is amiss. But these technologies may also increase the frequency of citizens’ interactions with government and law enforcement officials. Further, numerous scholars have identified the disparate impact of surveillance technologies, noting they often disadvantage already marginalized groups. Two increasingly popular technologies, both of which have made headlines recently, offer excellent examples of how these technologies raise civil rights concerns. Wastewater surveillance is not a new practice, but U.S. government agencies have increasingly relied on it since the coronavirus pandemic began in 2020. ShotSpotter is a gun-shot detection technology that law

16. Id.  
18. See, e.g., Barton Gellman & Sam Adler-Bell, Century Found., The Disparate Impact of Surveillance 2 (2017) (“Mass surveillance society subjects us all to its gaze, but not equally so. Its power touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status.”); Christopher Jones, Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation, 22 N.C. J.L. & TECH. 777, 786 (2021) (“Since human judgment is required for programming and training data, implicit biases present in humans may creep into the machine’s processes and produce biased results.”).  
19. Stephanie Desmon, How COVID-19 Created a Watershed Moment for Wastewater Surveillance, JOHNS HOPKINS BLOOMBERG SCH. PUB. HEALTH (May 13, 2022),
enforcement agencies have begun to deploy in cities around the United States.20 Both are discussed in detail below.

Governments have monitored wastewater outputs to track disease for many decades.21 By collecting water at select points in a municipality’s wastewater system, scientists can determine the concentration of bacteria and viruses present in the samples.22 But the public’s knowledge of this practice, which can detect everything from HIV to COVID-19, was limited prior to the coronavirus pandemic.23

Within months of the COVID-19 pandemic taking hold in the United States, the Centers for Disease Control and Prevention (CDC) established the National Wastewater Surveillance System as means of tracking SARS-CoV2, the virus that causes COVID-19.24 But this technology can be used to monitor far more than just infectious diseases. Some agencies have used it to measure opioid levels, allowing scientists to “track infections at a community level in a population-based way.”25 Taken in the best light, wastewater surveillance may be able to prevent the next public health crisis in the United States, but privacy experts have urged caution. After the CDC’s rollout of its national effort, the Government Accountability Office issued this warning in April 2022: “[W]astewater contains not only a pathogen’s genetic data that allow public health officials to identify the pathogen, but also human genetic data that could potentially be misused. Additionally, communities may be stigmatized if wastewater surveillance data indicate pathogen spread or illicit drug use.”26 Yet little has been done to address the privacy concerns associated with government surveillance of wastewater.


20. See Garance Burke et al., How AIPowered Tech Landed Man in Jail with Scant Evidence, AP NEWS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220 [https://perma.cc/MMS5-GG6S] (“Police chiefs call ShotSpotter a game-changer. The technology, which has been installed in about 110 American cities, large and small, can cost up to $95,000 per square mile per year.”).


22. See id. at 463–64 (discussing instances of scientists collecting and examining samples of wastewater for detection of viruses).

23. Desmon, supra note 19.


25. Desmon, supra note 19.

Like wastewater surveillance, ShotSpotter technology seems promising on its face. It relies on the installation of microphones in public spaces to detect the sound of gunfire. Proponents argue the technology increases police responsiveness, shaving critical minutes off response times. In theory, cities using ShotSpotter should be able to reduce the number of gun deaths and potentially catch more suspects. In practice, researchers have found the technology, “which has been installed in about 110 American cities . . . in neighborhoods deemed to be the highest risk for gun violence, which are often disproportionately Black and Latino communities,” does not live up to its promises. “[T]he technology does not reduce firearm violence in the long-term, and the implementation of the technology does not lead to increased murder or weapons related arrests.” Regardless of the technology’s ineffectiveness in aggregate, ShotSpotter recordings—like those of other smart technologies, including Alexa and Echo—are increasingly being used in criminal trials.

II. Citizens’ Rights in a Smart City

Citizens in a democratic society have a right to participate in the structuring and maintenance of their communities. Not surprisingly, many scholars have recently turned their focus to the role of citizens in the rise of the smart city. Although governments may envision greater interactions, most projects involve only de minimis citizen participation. A deeper relationship might develop if citizens were “valued and trustworthy collaborators in the develop and the governance of public space.” However, Els Leclercq and Emiel Rijshouwer’s research suggests this is not the case:

[D]espite the fact that smart city governments and corporations increasingly use a participatory and citizen-centric rhetoric, researchers and activists do not necessarily find that they fundamentally changed the neoliberal and

28. Id.
29. Burke et al., supra note 20.
30. See Doucette et al., supra note 27 (describing the results of various studies on the effectiveness of gunshot detection technology (GDT) and ShotSpotter, including that GDT does not “impact the level of reported gun crimes” and that ShotSpotter does not “improve case closures”).
31. Burke et al., supra note 20 (internal quotations omitted).
32. See Doucette et al., supra note 27, at 609 (examining the evidence suggesting that ShotSpotter implementation does not lead to a reduction in firearm related homicides and suggesting policy solutions as more cost-effective measures).
33. Burke et al., supra note 20.
surveilling nature of their projects, or that this contributed to more equal and just cities."34

After World War II, Henri Lefebvre argued that democratic participation includes citizen involvement in urban planning and policy in *Le Droit à la Ville*.35 Lefebvre posited that citizens have a right to shape public spaces in their communities and to help determine their use.36 Engin Isin colorfully characterized this as “the right to wrest the use of the city from the privileged new masters and democratize its space.”37 Edésio Fernandes advanced Isin’s work, noting the importance of “the right to information; the right of expression; . . . the right to self-management, that is, the democratic control of the economy and politics; the right to public and non-public services.”38

Drawing upon Fernandes’ work, we argue that citizens in a smart city have specific rights to information that they should be able to exercise through the use of public records laws:

1. Citizens have a right to know which technologies are being employed.
2. Citizens have a right to know how money is being spent.
3. Citizens have a right to know what data is being collected.
4. Citizens have a right to know how data is being used.
5. Citizens have a right to independent oversight.

A. Using Public Records Laws to Advance Citizens’ Rights

Open records laws provide the public with the right to access federal and state government records and meetings—including those related to the use of smart city technologies.39 Access to government information is

---

35. HENRI LEFEBVRE, *LE DROIT À LA VILLE* passim (1968).
36. See Nayeli Riano, *Henri Lefebvre and the Urban Revolution*, IMAGINATIVE CONSERVATIVE (Feb. 21, 2020), https://theimaginativeconservative.org/2020/02/henri-lefebvre-urban-revolution-nayeli-riano.html [https://perma.cc/28YJ-2K9F] (explaining that *Le Droit à la Ville* “argued for a human ‘right to the city’ where local authorities reclaim the city as a co-created space that is detached from the growing effects that commodification and capitalism have had over social interaction” and “aimed to rectify, through urban planning, the spatial inequalities in cities”).
38. Edésio Fernandes, *Constructing the ‘Right to the City’ in Brazil*, 16 SOC. & LEGAL STUD. 201, 208 (2007).
39. See, e.g., 5 U.S.C. § 552(b) (1976) (“[E]very portion of every meeting of an agency shall be open to public observation.”); FLA. STAT. § 286.011(1) (2022) (“All meetings of any board or commission of any state agency or authority or of any agency or authority of any county, municipal corporation, or political subdivision . . . are declared to be public meetings open to the
a fundamental democratic value. U.S. President James Madison once said, “[k]nowledge will for ever [sic] govern ignorance: and a people who mean to be their own Governours, must arm themselves with the power which knowledge gives.”\textsuperscript{40} By providing the public with access to these documents and proceedings, open records laws help voters hold their governments accountable. Shortly before joining the U.S. Supreme Court, civil rights defender Louis Brandeis noted, “[s]unlight is said to be the best of disinfectants.”\textsuperscript{41}

The idea behind open records and meetings laws is to provide additional transparency to the carrying out of government duties. As the Texas Public Information Act points out in its opening, “government is the servant and not the master of the people,” and that while the people delegate authority to government, they “insist on remaining informed so that they may retain control over the instruments they have created.”\textsuperscript{42} In no small part, this is because government officials are spending taxpayer money as they govern. Because of the costs and intrusiveness associated with smart city technology, oversight is essential for the protection of our fundamental rights. Often, however, residents know little to nothing about these technologies before they are implemented. Lack of transparency and oversight run counter to our democratic heritage; Judge Damon Keith once wrote that “[d]emocracies die behind closed doors.”\textsuperscript{43}

The more technologies government agencies employ, the more these agencies become warehouses of public data—and targets for malicious actors. Given the decreasing cost of gathering and storing information, it is not unusual for even municipal governments to possess “an extensive range of personal and sensitive data . . . with relatively few encumbrances from superior levels of government.”\textsuperscript{44} Much of this data is collected by, stored by, or shared with third-party vendors,\textsuperscript{45} raising serious concerns about privacy and security given the weak data protection laws in the United States.

\textsuperscript{40}. Letter from James Madison, President of the United States, to William T. Barry, Lieutenant Governor of Kentucky (Aug. 4, 1822), https://founders.archives.gov/documents/Madison/04-02-02-0480 [https://perma.cc/F292-WWDH].
\textsuperscript{42}. TEX. GOV’T CODE ANN. § 552.001(a) (2021).
\textsuperscript{43}. Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).
\textsuperscript{45}. See id. at 792 (explaining that data stewardship includes managing third-party vendors “because so many smart city developments depend on public-private partnerships”).
Smart city technologies are permeating municipal governance. From smart transportation systems that monitor public and private transit, to smart infrastructure, including water systems and power grids, these Internet-connected technologies allow for ever-increasing amounts of surveillance.\(^{46}\) The growing use of CCTV in major cities from London to New York also raises issues related to the tracking and monitoring of private individuals.\(^{47}\)

Smart city technologies thrive on constant, omnipresent data flows captured by cameras and sensors placed throughout the urban landscape. These devices pick up all sorts of behaviors, which can now be cheaply aggregated, stored, and analyzed to draw personal conclusions about city dwellers.\(^{48}\)

Legal scholarship on smart city technology primarily addresses privacy concerns. But some scholars have raised the issue of government transparency in the use of these technologies. Ira Rubinstein and Bilyana Petkova describe the possibility of “data stewards,” functioning as a “hybrid between a public institution seeking to act in the public interest and as a business corporation seeking to maximize profits,” noting the opportunity for public-private partnerships engaged in contractual data-sharing arrangements.\(^{49}\) These partnerships, like all public-private partnerships, often land in the gray area of open records and meetings laws, leaving the public without meaningful oversight.\(^{50}\) One example: efforts were undertaken to exempt Seattle’s dockless bike program from public records laws.\(^{51}\) Another: despite being a public project, Waterfront Toronto, Google’s Sidewalk Labs’ attempt to create a smart city, was

---

47. Id. at 1598.
48. Id. at 1582.
49. Rubinstein & Petkova, supra note 44, at 773.
50. See Amy Kristin Sanders & Daxton “Chip” Stewart, Secrecy, Inc.: How Governments Use Trade Secrets, Purported Competitive Harm and Third-Party Interventions to Privatize Public Records, 1 J. CIVIC INFO. 1 (2019) (“As governments engage in public-private partnerships, they have devised ways to shield the public’s business from the traditional level scrutiny offered by citizens and journalists, watchdogs of the public trust.”).
51. See Amy Kristin Sanders et al., Is It Just Dumb Luck? The Challenge of Getting Access to Public Records Related to Smart City Technology, J. CIVIC INFO. (forthcoming 2023) (manuscript at 11), https://www.nfoic.org/wp-content/uploads/2022/10/SmartCities.pdf [https://perma.cc/5Z5R-2UY8] (“The data stewardship examples they [Rubinstein and Petkova] examined, however, did not always play nicely with public records laws, as . . . [there were] efforts to exempt from public records laws . . . data gathered through Seattle’s dockless bike program.”). See generally Rubinstein & Petkova, supra note 44, at 811 (discussing how Seattle piloted a program for dockless bikes in 2017).
exempt from public records requests, locking off the public’s ability to ensure accountability.52

Some have proposed using de-identification to ensure that data in a smart city can be shared with the public while protecting individuals’ privacy.53 But de-identification is not perfect. In critiquing the use of facial recognition technology, Woodrow Hartzog and Evan Selinger argue that it is inadequate to protect individual privacy interests.54

Even when information about smart city technologies is available, the algorithms that power their data analyses are often not open source.55 Such is the case with ShotSpotter, a private company that refuses to release information about its algorithm for gunshot detection.56 Seemingly a public records gray area, private ownership of algorithmic records of technology used by government entities often allows that information to remain secret.57 Even the government agencies themselves are unsure whether to release the information. A 2018 study that requested public records related to smart city technology’s algorithms from forty-two agencies in twenty-three states received responses across the spectrum: “The barriers we encountered amount to substantial limitations on public access to information about algorithms, even if some of them could be overcome with more time and money.”58

Given these challenges, it is clear that state public records laws must be amended to ensure better access to information about smart city technology. For the public to engage in appropriate oversight and ensure individuals’ rights are being protected anytime government entities purchase and employ these tools, changes must occur. Three key issues must be addressed: (1) defining the term “public records” broadly; (2) defining privacy exemptions narrowly; and (3) narrowing law enforcement exemptions.

55. See Katherine Fink, Opening the Government’s Black Boxes: Freedom of Information and Algorithmic Accountability, 21 INFO., COMM’N & SOC’TY 1453, 1453 (2017) (“[G]overnment operations increasingly involve algorithms. While algorithms can make agency activities and decisions more efficient, they also hide information inside ‘black boxes’, away from public view. Whether freedom of information laws allow, or should allow, the public to see inside those black boxes is not clear.”).
58. Id. at 136.
B. Public Records Laws Must Broadly Define Records

Most state public records laws include a definition for what constitutes a record within a definitions section in the statute, but those definitions are far from uniform. As we previously found, a majority of states define the term “public records” broadly in a way that encompasses modern recordkeeping.  FLA. STAT. § 119.011(12) (2022). Florida’s public records law provides an example of this approach:

“Public records” means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

South Carolina’s law represents a similar take on the broad definition, defining “public record” as including “all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of their physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body.” S.C. CODE ANN. § 30-4-20(c) (2022). For individuals requesting records related to, or produced by, smart city technology, broadly-worded open records laws that demonstrate an understanding of modern recordkeeping technology provide the most support in favor of transparency.

Some states take a much narrower approach that could give requestors headaches. Alabama’s public records law includes a lengthy list of records—except they are all paper documents:

“[P]ublic records” shall include all written, typed or printed book, papers, letters, documents and maps made or received in pursuance of law by the public officers of the state, counties, municipalities and other subdivisions of government in the transactions of public business and shall also include any records authorized to be made by any law of this state belonging or pertaining to any court of record or any other public record authorized by law or any paper, pleading, exhibit or other writing filed with, in or by any such court, office or officer.

59. See Sanders et al., supra note 51, manuscript at 16 (“A majority of states take a relatively modern and wide-reaching approach to defining a record.”).

60. FLA. STAT. § 119.011(12) (2022).

61. S.C. CODE ANN. § 30-4-20(c) (2022).

Obviously, this language is less than ideal for those seeking information about smart city technology. Modern open records laws must embrace modern recordkeeping practices, including electronic and digital storage of information and data. In 2022, it is hard to argue that government information does not include photographs, video recordings, and audio records. Unless these states have useful case law, individuals requesting access to government records and data in these states may find themselves out of luck. Requestors whose state statutes do not include a definition of “public records” at all, however, may benefit from the lack of specificity, depending on the government entity they encounter.

C. Public Records Laws Must Narrowly Define Privacy Exemptions

Given the privacy concerns raised about the amount of data collected and stored when governments use smart technology, balancing individual privacy and government transparency proves challenging. But this is not a new challenge. Governments have regularly used privacy exemptions in public records laws to obfuscate the public’s access to information. Even with the proliferation of digital records, governments routinely give privacy the upper hand. Professor Benjamin Cramer noted the irony of governments claiming personal privacy, as it is “used increasingly as the justification for withholding government-held documents under FOIA [Freedom of Information Act] . . . thus preventing public knowledge of governmental operations discussed in those documents,” yet the public remains “powerless in reducing the secrecy of the surveillance state.”

Video records, which could be used for facial recognition, and audio records, possibly used for voice identification, are particularly likely to be withheld under a claim of personal privacy. Vaguely written exemptions allow for broad interpretation by records custodians. In Maryland, for example, any record that would cause “an unwarranted invasion of personal privacy” can be withheld. But statutory language is not the only issue that transparency advocates have to overcome. Not all state public records laws include a personal privacy exemption, but that does not mean adverse case law does not exist. To determine whether records should be released, Iowa courts employ a multi-part balancing test that examines: “(1) the public purpose of the party requesting the information; (2) whether the purpose could be accomplished without the disclosure of personal information; (3) the scope of the request; (4) whether alternative sources for obtaining the information exist; and (5)

64. Id. at 348.
65. MD. CODE ANN., GENERAL PROVISIONS § 4-351(b)(3) (LexisNexis 2022).
the gravity of the invasion of personal privacy.” As a result, many records related to, and produced by, smart city technologies are likely to be withheld based on privacy concerns, even when redaction may offer a path forward.

D. Public Records Laws Must Narrow the Law Enforcement Exemption

Many of the smart city technologies governments have adopted serve a surveillance function. As a result, it is no surprise that the law enforcement exemption found in many states’ open records laws could prove problematic. Overly broad statutory exemptions inhibit transparency. Colorado’s law enforcement exemption has this effect: “Any records of the investigations conducted by any sheriff, prosecuting attorney, or police department, any records of the intelligence information or security procedures of any sheriff, prosecuting attorney, or police department, or any investigatory files compiled for any other law enforcement purpose.” Colorado is not alone in drafting overly broad exemptions. Nebraska’s language is particularly troubling:

(5) Records developed or received by law enforcement agencies and other public bodies charged with duties of investigation or examination of persons, institutions, or businesses, when the records constitute part of the examination, investigation, intelligence information, citizen complaints or inquiries, informant identification, or strategic or tactical information used in law enforcement training, except that this subdivision shall not apply to records so developed or received:

(a) Relating to the presence of . . . alcohol or drugs in any body fluid of any person; or [a family member’s request for investigation into an employee death in the line of duty].

As government entities begin to amass and share information, broad language like this serves as a serious impediment to requestors. Fire departments, for example, make use of thermal imaging cameras when fighting fires. Would sharing that video with law enforcement then permit an agency to withhold it under the law enforcement exemption? What about when the municipal traffic department shares traffic camera data with police? In many states, the answer may be “yes.”

Scholars have already noted instances where requests for information from automated license plate readers have been denied based on the law

68. NEB. REV. STAT. § 84-712.05(5) (2012).
enforcement exemption. Similarly, police body cameras and dash cameras offer the promise of government transparency, but only if that footage is made publicly available.

Visibility is a critical element of democratic oversight by elected officials, legislative bodies, and communities affected by surveillance. The proliferation of new technologies should prompt us to ask not just what rules ought to constrain the police, but what we need to know in order to decide what the rules ought to be.71

Although some agencies are engaging in affirmative disclosures, more often than not, government entities are employing “the reactive model embraced by FOIA.”72 As a result, if citizens do not request the video, it may never see the light of day.

As law enforcement officers increasingly rely on drones, facial recognition, and other smart technology to engage in surveillance of protestors and others engaged in lawful activity, it is likely we will see an increase in requests for these records. As they currently stand, many states’ public records laws do not provide adequate transparency with regard to these types of records.

CONCLUSION: THE ESSENTIAL ROLE OF PUBLIC RECORDS LAW IN UPHOLDING CITIZENS’ RIGHTS

Public records laws will undoubtedly play a central role in protecting citizens’ rights in a smart city. Given the massive amounts of data collected by smart city technologies, public oversight is necessary to ensure governments are not infringing on individual rights. But public records laws may come up short in supporting that oversight. In spirit, these laws are designed to ensure the public can hold government officials and entities accountable. But in practice, they are riddled with outdated language and vague exemptions that could limit access to records related to, and produced by, smart city technologies. As our reliance on artificial intelligence, facial recognition, and other forms of surveillance and monitoring technologies in the provision of government services evolves, so too must our public records laws.


72. Id. at 965.