Is It Just Dumb Luck? The Challenge of Getting Access to Public Records Related to Smart City Technology

By Amy Kristin Sanders, Daxton 'Chip' Stewart and Steven Molchanov

In October 2021, investigative journalists from *The Lens* reported on the City of New Orleans' recent deployment of police surveillance cameras throughout the city.[1] The story revealed shocking details of the city's $40 million public safety plan that included cameras, license plate readers and a "Real Time Crime Center" to serve as a hub for law enforcement's surveillance activity. Perhaps less shocking is the challenge the reporters faced in accessing information about the system, which includes tools maintained by the city, state and federal law enforcement, and even private organizations working as government contractors.

New Orleans' installation of a mass surveillance apparatus mirrors purchases being made nationwide, as the rise of 'Smart City' technologies (acoustic listening devices, street-light cameras, license plate readers, surveillance drones, etc.) finds major cities throughout the United States racing to purchase state-of-the-art products they promise will improve municipal services. A June 2018 report by consulting behemoth McKinsey & Company touted the benefits of Smart City technology: "As cities get smart, they are becoming more livable and more responsive—and today we are seeing only a preview of what technology could eventually do in the urban environment."[2] From New York to San Francisco and Austin to Chicago, cities are investing millions of dollars of taxpayer money into an array of devices that monitor everything from public transit and traffic patterns to water systems and electric grids.[3]

---

[1] https://surveillance.thelensnola.org/

[2] https://www.mckinsey.com/business-functions/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

[3] https://www.digi.com/solutions/by-industry/smart-cities

Yet the McKinsey report glosses over the potential dangers associated with increased monitoring—including the lack of public oversight taking place. As *The Lens* story noted:

> There is no consolidated 'department of surveillance' in New Orleans, no single venue where residents … can go to learn more. Nor is there a formal regulatory structure for internal tracking, public disclosure or approval for surveillance or data collection technology. The city makes it even harder to navigate the labyrinth by consistently refusing or failing to give accurate information to the public…"[4]

As journalists quickly learned, public records laws can be woefully inadequate with regard to Smart City technology. Many of these "records" consist of digital audio and video files rather than traditional paper records. But even the contracts for technology purchases are often withheld, as was the case in New Orleans: "[T]he city also provided incomplete and inaccurate records in response to some of The Lens' public records requests."

This paper analyzes public records laws and relevant case law from all 50 states to examine whether the laws are drafted in ways that cover access to records about, and produced by, Smart City technologies. Even in states like Louisiana, where the term "public record" is broadly defined,[5] government officials regularly rely on exemptions—often citing either law enforcement or privacy concerns—to deny access to these records. Although many Smart City technologies have not been addressed by the legislatures and courts to date, legislation and

[4] https://surveillance.thelensnola.org/

[5] In Louisiana, the state public records law relies on the following definition: "All books, records, writings, accounts, letters and letter books, maps, drawings, photographs, cards, tapes, recordings, memoranda, and papers, and all copies, duplicates, photographs, including microfilm, or other reproductions thereof, or any other documentary materials, regardless of physical form or characteristics, including information contained in electronic data processing equipment, having been used, being in use, or prepared, possessed, or retained for use in the conduct, transaction, or performance of any business, transaction, work, duty, or function which was conducted, transacted, or performed by or under the authority of the constitution or laws of this state, or by or under the authority of any ordinance, regulation, mandate, or order of any public body or concerning the receipt or payment of any money received or paid by or under the authority of the constitution or the laws of this state." *See* https://www.legis.la.gov/legis/Law.aspx?d=99632

litigation involving two technologies (police body-worn cameras and police dash cameras)[6] have advanced—offering some reason for optimism.

In this paper, we attempt to catalog the landscape of state public records laws with regard to how likely they are to provide the public with access to records about, and produced by, Smart City technology. We start with an overview of the nascent Smart City concept, offering examples of the types of technology that are included and the purported benefits, along with the real-world consequences, of the technology. Then we offer a brief review of the relevant scholarly literature, noting both the purpose of public records laws and contemporary discussions of access to government information. Our analysis then focuses on the state of the law throughout the United States, examining the text of state public records laws to determine the likelihood they would be interpreted to cover access to records about, and produced by, Smart City technology. Finally, we conclude with a discussion of the benefits and perils of providing access to these records, noting key areas of concern that lawmakers must address if our public records laws are to continue to fulfill their stated purpose.

Smart City Technology – The Latest Threat to Civil Rights

Smart City technology, including high-speed communication infrastructure, lights, cameras, sensors, microphones, meters and mobile phone apps, has become increasingly popular on the state and local level. In part, this popularity can be attributed to the promise of greater efficiency and higher quality of life. "Smart cities … collect and analyze data. The cities use this data to improve infrastructure, public utilities and services, and more."[7] Not surprisingly, many

---

6 https://www.americanbar.org/groups/communications_law/publications/communications_lawyer/fall2020/public-access-police-bodyworn-camera-recordings-status-report-2020/

7 Smart cities use 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, and more.

consumers are also intrigued by "smart" technology for their bodies and homes. From the Apple Watch to the Nest Smart Thermostat or Amazon Alexa, Americans have increasingly automated their lives. One study suggested the number of devices connected to the Internet—known in the tech world as the Internet of Things—will more than double between 2020 and 2025, rising to 3.74 billion devices in the next three years.[8]

In many instances, IoT and other 'Smart' devices add convenience—allowing you to remotely control the lights or temperature in your home, for example—but privacy experts warn that they come at cost. In August 2021, Security Scorecard outlined seven distinct threats posed by IoT devices, including insecure data storage and transfer.[9] Consulting firm Deloitte noted that many sectors—from municipal infrastructure to urban transportation to the health sciences—have begun to rely on "Smart" technology, greatly increasing the cyber threat landscape.[10] As long ago as 2016, professors Woodrow Hartzog and Evan Sellinger were warning about the potential dangers of IoT devices:

> While IoT might be incredibly useful, we should proceed carefully. … Each new camera, microphone, and sensor adds another vector for attach 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]

Yet little oversight in either the public sector or the private sector has occurred to ensure users are protected.

---

[8] https://www.insiderintelligence.com/insights/iot-smart-city-technology/

[9] *7 Internet of Things Threats and Risks to Be Aware of,* Security Scorecard, August 4, 2021, https://securityscorecard.com/blog/internet-of-things-threats-and-risks

[10] *Cyber risk in an Internet of Things world,* Deloitte, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html

[11] Woodrow Hartzog & Evan Sellinger, *The Internet of Heirlooms and Disposable Things,* 17 N.C. J. Law & Tech. 581 (2016).

Given these issues, many citizens have grown particularly wary of governments who purchasing and using these 'Smart' technologies. Eugenie Birch, who directs the Penn Institute for Urban Research, pointed to the lack of transparency as one of the causes for citizen fear and concern:

> I also think there is a lack of rules around the use of technology, so that 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]

Amnesty International[13] and the American Civil Liberties Union[14] have both taken a public stance against facial recognition technology, noting concerns for how it impacts citizens constitutional rights. Community organizations in Chicago called on city officials to cancel its contract with ShotSpotter, whose controversial technology detects gunshots and reports them to police.[15] In May 2021, Northwestern University's MacArthur Justice Center questioned the value of the technology, noting that police were needlessly deployed more than 40,000 times in 21 months.[16]

---

[12] *Why Is There a Backlash to Smart Cities,* Brink News, Dec. 11, 2019, https://www.brinknews.com/why-is-there-a-backlash-to-smart-cities/

[13] *Ban dangerous facial recognition technology that amplifies racist policing,* Amnesty International, Jan. 26, 2021, https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

[14] *The Fight to Stop Face Recognition Technology,* American Civil Liberties Union, July 15, 2021, https://www.aclu.org/news/topic/stopping-face-recognition-surveillance

[15] Matt Masterson, *Activists Call on Chicago Officials to Dump ShotSpotter Contract,* WTTW, Aug. 19, 2021, https://news.wttw.com/2021/08/19/activists-call-chicago-officials-dump-shotspotter-contract

[16] *ShotSpotter creates thousands of dead-end police deployments that find no evidence of actual gunfire,* MacArthur Center for Justice, https://endpolicesurveillance.com/

Citizen Oversight in a Democracy

Numerous scholars have studied and theorized the ways in which citizens in a democratic society should be involved in the planning, implementation and upkeep of a "Smart" City. Many have noted that even when governments intend citizen involvement, it rarely moves beyond mere participation. Leclercq and Rijshouwer argued instead that cities should view citizens as "valued and trustworthy collaborators in the develop and the governance of public space."[17] They note, however, that most efforts to include citizens in these processes amount to very little:

> [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 surveilling nature of their projects, or that this contributed to more equal and just cities. [18]

Much of this modern work traces its roots back to Henri Lefebrve's research on urbanization after World War II. In his first major book on the city, *Le droit a la ville*, Lefebrve outlines the role of citizens in urban planning and policy as a function of democratic participation. According to Lebefvre, citizens do more than simply reside in their cities and public spaces. Because of this, they should have a role in shaping the role of those cities and the uses of those public spaces. Engin Isin has described this right as "the right to wrest the use of the city from the privileged new masters and democratize its space."[19] Fernandes takes this further, 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

[17] Els M. Leclercq & Emiel A. Rijshouwer, *Enabling Citizens' Right to the Smart City Through the Co-Creation of Digital Platforms,* 4 Urban Transformations 1 (2022), https://urbantransformations.biomedcentral.com/track/pdf/10.1186/s42854-022-00030-y.pdf

[18] Id. at 2.

[19] Democracy, Citizenship and the Global City 14 (1 st ed., ed. Engin F. Isin, 2001).

and non-public services."[20] Yet, as we will show, public oversight and the ability to access information about the growing implementation of Smart City technology remain woefully inadequate.

A Brave New World: Today's 'Smart City'

"Smart City" technology has come to encompass a wide array of devices and systems engaging in any number of monitoring functions—some of which may lead to involuntary engagement with law enforcement or other regulatory entities. Each of these new technologies carries with it the propensity to disadvantage certain groups of people—consequences rarely debated before governments acquire the technology. Two examples, one involving wastewater monitoring and the other involving ShotSpotter, prove illustrative in highlighting the disparate ways in which these technologies can be employed and the ways in which they raise concerns about privacy, discrimination and due process.

Wastewater monitoring efforts, tracking everything from polio to salmonella, went largely unnoticed by the public until the COVID-19 pandemic. Scientists analyzed water collected a various points in the sewer system to get a readout on the concentration of bacteria and viruses present in the water.[21] In September 2020, the Centers for Disease Control and Prevention established the National Wastewater Surveillance System to monitor the presence of SARS-CoV2, the virus that causes COVID-19.[22] The technology can be employed to monitor everything from bacteria and viruses to opioids, allowing researchers to "track infections at a

---

[20] Edesio Fernandes, *Constructing the 'Right to the City' in Brazil,* 16 Social & Legal Studies 201, 208 (2007).

[21] *How COVID-19 Created a Watershed Moment for Wastewater Surveillance,* Johns Hopkins Bloomberg School of Public Health, May 13, 2022, https://publichealth.jhu.edu/2022/how-covid-19-created-a-watershed-moment-for-wastewater-surveillance.

[22] *National Wastewater Surveillance System,* CDC, https://www.cdc.gov/healthywater/surveillance/wastewater-surveillance/wastewater-surveillance.html

community level in a population-based way."[23] Although this technology has the potential to speed community response to public health crises, privacy experts warn that it comes with concerns. An April 2022 report by the Government Accountability Office summarizes key ethical concerns:

> [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.[24]

Despite the seemingly innocuous nature of wastewater surveillance, the GAO report suggests a very real need for oversight to ensure privacy concerns are addressed.

Other "Smart City" technologies present more easily identifiable concerns with regard to constitutional rights. ShotSpotter technology relies on publicly erected microphones to pick up the sound of gunfire and automatically alert law enforcement. In theory, early detection systems like ShotSpotter would speed response, potentially saving lives and increasing arrests in gun-related crime. But research has found the technology, "which has been installed in about 110 American cities … in neighborhoods deemed to be the highest risk, which are often disproportionately Black and Latino communities,"[25] does not make communities safer. [26] "[T]he technology does not reduce firearm violence in the long-term, and the implementation of the

---

[23] *How COVID-19 Created a Watershed Moment for Wastewater Surveillance,* Johns Hopkins Bloomberg School of Public Health, May 13, 2022, https://publichealth.jhu.edu/2022/how-covid-19-created-a-watershed-moment-for-wastewater-surveillance.

[24] Science & Tech Spotlight: Wastewater Surveillance, Government Accountability Office, April 2022, https://www.gao.gov/assets/gao-22-105841.pdf

[25] https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

[26] Mitchell L. Doucette, Christa Green, Jennifer Necci Dineen, David Shapiro & Kerr M. Raissian, *Impact of ShotSpotter Technology of Firearm Homicides and Arrests Among Large Metropolitan Counties: A Longitudinal Analysis, 1999-2016,* 98 J. Urban Health 609 (2021).

technology does not lead to increased murder or weapons related arrests."[27] In more and more instances, ShotSpotter recordings are being introduced into evidence in criminal trials,[28] despite clear concerns about their veracity. Because of the seriousness of these concerns, citizens have a fundamental right to know which technologies their governments are employed. Yet many law enforcement entities are reluctant to be transparent with the public.

The Purpose of Public Records Laws

At both the state and federal level, open records laws are in place to guarantee a public right of access to government documents and data. There are many justifications for these kinds of laws. Founding Father James Madison implied the importance of a right to know to help provide the citizenry information so they can make voting decisions: "Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[29] The people have a right to know what their government is up to, in part to help to uncover waste and fraud in government spending, or as renowned jurist and eventual Supreme Court Justice Louis Brandeis put it in 1913, "Sunlight is said to be the best of disinfectants."[30] And transparency laws center taxpayers as the proper owners and managers of a democratic government as a core component of democratic self-governance, as the opening to the Texas Public Information Act declares, recognizing that "government is the servant and not the master of the people" and that while the people delegate authority to government, they

[27] https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

[28] Harm Venhuizen, *Court backs arrest by officers responding to ShotSpotter,* Associated Press, June 30, 2022, https://apnews.com/article/wisconsin-arrests-milwaukee-supreme-court-d1fd9cba23f757f34d72f794cc30b151

[29] James Madison, Letter to W.T. Barry, Aug. 4, 1822, available at https://www.loc.gov/resource/mjm.20_0155_0159/?sp=1&st=text.

[30] Louis D. Brandeis, What Publicity Can Do, Harper's Weekly, Dec. 20, 1913, at 10.

"insist on remaining informed so they may retain control over the instruments they have created."[31]

But the justification for government transparency most relevant to this inquiry about smart city technologies is oversight of government functions. "Democracies die behind closed doors," as Judge Damon Keith wrote in 2003.[32] As technology has advanced, so has the ability of the government to gather and store records using that technology. City, county, state and federal government agencies have become data warehouses in the past few decades, collecting "an extensive range of personal and sensitive data… with relatively few encumbrances from superior levels of government," often in conjunction with private third-party vendors.[33] As public agencies have become watchmen, freedom of information laws provide tools to help citizens watch those watchmen.

Finch and Tene identified several of the technologies that are implicated by smart city design, including digital maps, public and private transit options ranging from buses and trains to Lyft and Uber, and smart grids for power and water, all of which may be connected to the Internet of Things and enabled for tracking and monitoring.[34] Similarly, closed circuit television (CCTV) cameras are omnipresent on street corners in metropolises such as London, Dubai, and Chongqing, presenting further surveillance options for government as well as privacy challenges for citizens.[35] "Smart city technologies thrive on constant, omnipresent data flows captured by

---

[31] Texas Gov't Code Sec. 552.001(a) (2022).

[32] Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).

[33] Ira S. Rubenstein & Bilyana Petkova, Governing Privacy in the Datafied City, 47 Fordham Urb. L. J. 755, 791 (2020);

[34] Kelsey Finch & Omar Tene, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town, 41 Fordham Urb. L.J. 1581, 1583-90 (2014).

[35] Id. at 1598.

cameras and sensors placed throughout the urban landscape," Fince and Tene noted. "These devices pick up all sorts of behaviors, which can now be cheaply aggregated, stored, and analyzed to draw personal conclusions about city dwellers."[36]

Like Finch and Tene, legal scholars examining the challenges of smart city technologies have largely focused on the privacy implications of this constant monitoring and surveillance. However, portions of those works have begun to unpack the challenges for government transparency laws in these technologies. Rubenstein and Petkova envisioned smart cities in part as "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" through data-sharing arrangements with third-party vendors in public-private arrangements.[37] The data stewardship examples they examined, however, did not always play nicely with public records laws, as they noted efforts to exempt from public records laws both data gathered through Seattle's dockless bike program and Boston's deal with Uber for ride-share data.[38] They argued that New York City's Taxi and Limousine Commission showed a "near perfect disregard for data stewardship" in its regulation of Uber, specifically noting the lack of any provisions on data privacy, including "to whom it would disclose (ride share data) such as in response to public records act requests."[39] Waterfront Toronto (WT), a smart city effort headed by Google's Sidewalk Labs, was exempt from freedom of information requests under a "quirk of WT's constitution" despite being a public project, meaning information about the project was not accessible to the public unless it

[36] Id. at 1582.

[37] Id. at 773.

[38] Id. at 809, 812.

[39] Id. at 805-6.

was voluntarily released.[40] The Toronto experience also informed a proposal by Austin and Lie for a "safe sharing site" for data gathered by smart city technology and stored by the government, with a strategy of making smart city data open by default but de-identified as a way to balance individual citizen privacy concerns with public oversight goals.[41] Even de-identification presents challenges, as noted by Hartzog and Selinger in the context of facial recognition technology (FRT). They argue that it is inadequate to protect individual privacy interests and urge a ban on use of FRT, as some cities including San Francisco and Oakland have enacted in recent years.[42]

Beyond the surveillance and monitoring tools employed by smart cities, the algorithms used to make sense of the data gathered also present transparency challenges.[43] Private ownership of algorithmic records by third-party vendors can frustrate public records laws. A 2018 study of algorithmic transparency by smart cities using public records laws found "wide variation" in the responses from 42 agencies across 23 states, with several requests not receiving responses and many others citing exemptions or limited information in response. "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," Brauneis and Goodman concluded.[44]

---

[40] Ellen P. Goodman & Julia Powles, Urbanism Under Google: Lessons from Sidewalk Toronto, 88 Fordham L. Rev. 457, 464 (2019).

[41] Lisa M. Austin & David Lie, Safe Sharing Sites, 94 N.Y.U. L. Rev. 581, 583-4 (2019).

[42] Woodrow Hartzog & Evan Selinger, Privacy's Constitutional Moment and the Limits of Data Protection, 61 B.C. L. Rev. 1687, 1754 (2020).

[43] *See* Katherine Fink, Opening the Government's Black Boxes: Freedom of Information and Algorithmic Accountability, 21 Info. Comm. & Soc'y 1453 (2017).

[44] Robert Brauneis & Ellen P. Goodman, Algorithmic Transparency for the Smart City, 20 Yale J. L. & Tech. 103, 136 (2018).

Specific technologies that may be employed by smart cities have also received some attention from scholars, again largely focusing on privacy risks but occasionally delving into the implications for transparency and public records. Data gathered from automated license plate readers, for example, are subject to "broad public records exemptions" that make it unavailable for citizens to access in many U.S. states, according to Wesner and Blevins.[45] Tools like ALPRs and police body cameras, while they enhance government surveillance and monitoring, also offer potential for greater transparency and oversight of law enforcement conduct, according to Block-Wehba. "Visibility is a critical element of democratic oversight by elected officials, legislative bodies, and communities affected by surveillance," she concluded. "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."[46] She urged more affirmative and regular disclosures of such information under public records laws, rather than "the reactive model embraced by FOIA" that only requires disclosure in response to a citizen's request.[47]

Freedom of information laws have the potential to provide oversight to the gathering and use of data by smart cities, as the aforementioned scholars have noted, though the privacy risks of the release of that data will remain a challenge. This is not a new challenge, of course. Public records laws have long balanced transparency goals with privacy interests. As digital record-keeping and data have increased over the decades, privacy interests have had the upper hand. Cramer noted the duality of government protection of personal privacy, as it is "used

[45] The authors note some exceptions, including Montana and Arkansas. Kearston Wesner & Katie Blevins, Restraining the Surveillance Society: Comparing Privacy Policies for Automated License Plate Readers in the United States and the United Kingdom, 18 ISJLP 99, 138 (2021).

[46] Hannah Block-Wehba, Visible Policing, Technology, Transparency, and Democratic Control, 109 Calif. L. Rev. 917, 978 (2021).

[47] Id. at 965.

increasingly as the justification for withholding government-held documents under FOIA…thus preventing public knowledge of governmental operations discussed in those documents" while the same privacy justifications remain "powerless in reducing the secrecy of the surveillance state."[48]

In the present study, the authors seek to examine this balance between protecting privacy interests while also allowing the public robust oversight of smart city technologies, examining state and federal transparency laws and how they may or may not allow access for such oversight.

Analysis of State Public Records Laws

As the journalists at *The Lens* learned, even in states with well-written public records laws, there is no guarantee that government officials will turn over records related to Smart City technology. But having an adequate definition of what constitutes a record, along with narrowly tailored exemptions, can go a long way in strengthening the argument for access to information.

In this section, we outline the current state of the law throughout the United States. To undertake our analysis, we gathered the most-recent published versions of each state's public records law. After assembling our database of laws, we scoured each to determine whether and how the word 'record' was defined. Then we analyzed each state's exemptions—with particular emphasis on privacy and law enforcement exemptions—to determine whether they would plainly exclude access to records about, and created by, Smart City technology.

Defining 'a Record'

[48] Benjamin W. Cramer, Privacy Exceptionalism Unless it's Unexceptional: How the American Government Misuses the Spirit of Privacy in Two Different Ways to Justify Both Nondisclosure and Surveillance, 16 ISJLP 306, 348 (2020).

Even in 1966 when the federal Freedom of Information Act took effect, government officials should have anticipated that 'records' would quickly come to mean more than just printed paper documents. By the 1980s, the federal government recognized large-scale shifts to electronic record-keeping, and state and federal laws needed to adapt to cover these new formats. In 1996, Congress passed E-FOIA to extend FOIA to make it clear that electronic records were covered by the act, to require digital reading rooms for records requested by anyone, and to provide records in digital formats when requested if possible.[49] Yet, several state public records laws continue to define 'record' narrowly, even in 2022.

At the outset, it might be useful to take a brief look at how the definition of 'record' has been construed at the federal level. Interestingly, FOIA itself contains no definition of the word record.[50] However, federal case law makes clear that records are not confined to written documents. In *Save the Dolphins v. U.S. Department of Commerce,* the Northern District of California ruled that a movie about tuna fishing was an agency record.[51] Previously a federal district court in Kansas had ruled that rifle and bullet remains from the Kennedy assassination were not records.[52] There, the Court noted the need for "information in language or other symbols." The D.C. Circuit, in its *decision in American Immigration Lawyers Association v. EOIR,* once wrote that agencies "in effect define a 'records' when they undertake the process of identifying records that are responsive to a request."[53] It continued its tautological reasoning by

[49] See Daxton R. "Chip" Stewart & Charles N. Davis, Bringing Back Full Disclosure: A Call for Dismantling FOIA, 21 Comm. L. & Pol'y 515, 523 (2016).

[50] https://www.justice.gov/oip/oip-guidance/defining_a_record_under_the_foia

[51] 404 F. Supp. 407 (N.D. Cal. 1975).

[52] *Nichols v. United States,* 325 F. Supp. 130 (D. Kan. 1971).

[53] 830 F.3d 667, 678 (D.C. Circuit 2016).

noting the "range of possible ways in which an agency might conceive of a 'record'."[54] In July 2021, the Department of Justice issued guidance to the federal agencies that referenced the Privacy Act's definition of a record, which includes each "item, collection or grouping of information."[55] Under 45 CFR 5.3, which implements FOIA for the Department of Health and Human Services, "[r]*ecord* means any information that would be an agency record when maintained by an agency in any format, including an electronic format; and any information that is maintained for an agency by an entity under Government contract, for the purposes of records management."[56]

Definitions in State Public Records Laws

Although the federal landscape provides little to no clarity on the definition of what constitutes a record, most state records laws clearly define the word within the statute's language. The breadth of that language, not surprisingly, varies quite dramatically. A majority of states[57] take a relatively modern and wide-reaching approach to defining a record by employing this language found in the Florida Sunshine Law, or language that is virtually identical:

> '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.[58]

Variations on this definition include South Carolina's quite similar rendition defining public records to include "all books, papers, maps, photographs, cards, tapes, recordings, or other

---

[54] *Id.*

[55] https://www.justice.gov/oip/oip-guidance/defining_a_record_under_the_foia

[56] https://www.law.cornell.edu/cfr/text/45/5.3#:~:text=FOIA%20request%20means%20a%20written,552(a)(2).

[57]

[58] Fla. Stat. 119.011 (2022).

documentary materials regardless of their physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body."[59] This approach, which clearly recognizes that government information can be stored in myriad ways besides mere paper records, provides access advocates with significant runway to argue for access to everything from still photographs from license plate readers, video footage from aerial drones, sound recordings from gunfire detection microphones and tables containing levels of bacteria in wastewater. It also provides solid grounding for citizens and others to request the documentation behind the research, purchase, installation and operation of Smart City technology, which is what journalists from *The Lens* were most interested in.

Not all states have such wide-ranging definitions in their statutes. Alabama, for example, defines public record by listing an assortment of items—all of which are print:

> "[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 records authorized by law or any paper, pleading, exhibit or other writing filed with, in, or by any such court, office or officer.[60]

This approach is not uncommon. Ideally, the statutory language would make reference to the many electronic and/or digital means in which today's records may be kept, including but not limited to photos, video, audio recordings and others mediums listed in the Florida statute.

In states like Alabama, where the statutory definition is lacking, requestors are at the mercy of case law. Fortunately for Alabama residents, a key state Supreme Court decision supports an argument in favor of access. In Chambers v. Birmingham News Co., the court made

---

[59] S.C. Code Ann. 30-4-20(c) (2022). https://www.scstatehouse.gov/code/t30c004.php

[60] Ala. Code 41-13-1 (2019). https://codes.findlaw.com/al/title-41-state-government/al-code-sect-41-13-1.html

several helpful pronouncements about the Public Records Law.[61] The first noted that the legislature intended a liberal construction of the law.[62] The second affirmed a presumption in favor of disclosure, and the third clearly shifted the burden of proof to the nondisclosing party.[63]

Other states, like Arizona, do not specifically define the term record in their statutes. Instead, the statute defines "officer" and "public body."[64] In a 1984 case,[65] the Arizona Supreme Court attempted ot provide some clarification of the public records law. There, it ruled:

> Section 39-121.01(B) creates a statutory mandate which, in effect, requires all officers to make and maintain records reasonably necessary to provide knowledge of all activities they undertake in the furtherance of their duties. We think that the objective implicitly expressed in § 39-121.01 is to broadly define those records which are open to the public for inspection under § 39-121, thus obviating the need for any technical distinction between "public records" or "other matters," insofar as the right to inspection by the public is concerned.[66]

Although statutes that are silent on the definition of a record clearly provide "wiggle room" for a crafty argument in a court of law, they also provide no real guarantee of access to records about, or created by, 'Smart City' technology.

Exempting 'Smart City' Technology

Even when a state's public records statute or case law clearly support the release of records held in electronic or digital mediums, requestors must still overcome the statute's stated exemptions. With regard to 'Smart City' technologies, three popular exemptions are likely to cause requestors serious consternation: 1) proprietary software and trade secrets, 2) law enforcement and 3) unwarranted invasions of privacy. We will discuss each in turn.

---

[61] 552 So. 2d 854, 856 (Ala. 1989).

[62] *Id.*

[63] *Id.* At 856-857

[64] A.R.S. §§ 39-121

[65] *See* Carlson v. Pima County, 141 Ariz. 487, 687 P.2d 1242 (Ariz. 1984).

[66] *Id.* at 490.

Proprietary Software and Trade Secrets

One possible roadblock to the public's ability to access records about, and produced by, 'Smart City' technology has to do with public records laws that address "proprietary software." In Alaska, for example, the definition of a public record specifically excludes proprietary software programs.[67] Because many 'Smart City' technologies rely on various types of artificial intelligence, including algorithms and machine learning, government entities may try to use exemptions for proprietary software to exclude access to these records. This issue has already come to light in criminal trials, including one that resulted in the pre-trial detention of Michael Williams.[68] As the Associated Press reported, "Prosecutors said technology powered by a secret algorithm that analyzed noises detected by the sensors indicated Williams shot and killed the man."[69] Eventually, after Williams had spent more than a year in jail, prosecutors asked the judge to dismiss the case.[70]

In other states, the public records law includes an exemption addressing proprietary software. New Jersey outlines the exclusion of proprietary software in its trade secrets exemption, which exempts:

> Trade secrets and proprietary commercial or financial information obtained from any source. For the purpose of this paragraph, trade secrets shall include data processing

---

[67] AS 40-25-220. "'[P]ublic records' means books, papers, files, accounts, writings, including drafts and memorializations of conversations, and other items, regardless of format or physical characteristics, that are developed or received by a public agency, or by a private contractor for a public agency, and that are preserved for their informational value or as evidence of the organization or operation of the public agency; 'public records' does not include proprietary software programs;"

[68] https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

[69] https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

[70] https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

> software obtained by a public body under a licensing agreement which prohibits its disclosure.[71]

Under this kind of provision, government entities would be incentivized to insist that 'Smart City' technology vendors include provisions in their contracts that prohibit disclosure. Such a loophole basically permits the government entity to coopt its business partner for the sake of limiting public access to records.

Many states have similar exemptions that address trade secrets, confidential business information or other proprietary information. In Kentucky, for example, the language reads:

> Records confidentially disclosed to an agency or required by an agency to be disclosed to it, generally recognized as confidential or proprietary, which if openly disclosed would permit an unfair commercial advantage to competitors of the entity that disclosed the records;[72]

As we have noted in our other research, the burgeoning interpretation of exemptions related to confidential business information after the U.S. Supreme Court's 2019 decision in *Food Marketing Institute v. Argus Leader Media*[73] represent a real threat to government transparency.[74] This is particularly true in the area of 'Smart City' technology, where many government entities that lack deep technical capability will undoubtedly contract out significant portions of the operation, including the installation of technology as well as the analysis and retention of data.

Law Enforcement Exemptions

---

[71] NJSA 47:1A-1.1.

[72] KSA 61.878(1)(c)(1).

[73] 588 U.S. ___ (2019).

[74] *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).

Because many 'Smart City' technologies have surveillance capabilities—from facial recognition to location tracking and gun-shot detection—that are of interest to law enforcement, we would we be remiss not to address the challenges posed by these exemptions. In fact, a law enforcement exemption can be found in X state public records laws. Often these exemptions are either written broadly or have been interpreted in that manner. Given the jurisprudence on Exemption 7 to the federal Freedom of Information Act, this is unsurprising.[75]

But in some instances, government officials need not even rely on a court's interpretation of the public records law. In some states, including Colorado, the statutory language itself is quite far-reaching, exempting:

> 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;[76]

Given police use of drone technology, combined with facial recognition, to surveil crowds at protests, one can imagine how law enforcement might use exemptions such as these to protect that footage, claiming the surveillance was related to protecting law enforcement personnel on the ground at the protest. Similar claims could be made about exempting the location of, and footage from, license plate readers if police could argue that information was part of an investigatory file used in drug trafficking or other criminal monitoring.

---

[75] In *Department of Justice v. Reporters Committee for Freedom of the Press,* the Supreme Court rule unanimously that Exemption 7 was intended to protect the kind of personal privacy that would be violated were the FBI to release a person's criminal file when requested under the open records law. *See* 489 U.S. 749 (1989).

[76] CRSA 27-72-204(2)(a)(I).

Other states' law enforcement exemptions are even more far-reaching than Colorado. Its neighbor to the northeast, Nebraska, likely takes the prize for the most overbroad law enforcement exemption. Exemption 5 reads:

> 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 [related to the presence of alcohol or drugs in a person's bodily fluids or a family member's request for investigation into an employee death in the line of duty][77]

This broad language clearly protects information shared with law enforcement by other governmental entities. Consider a fire department's use of thermal-imaging drones at fires that happen to pick up a neighboring house's excessive thermal output. If the fire department shares these images with the police department who uses them to seek a search warrant, are they exempt from release under the public records law? In Nebraska, it would seem so. Yet determining whether agencies are sharing data obtained from 'Smart City' technologies with law enforcement as a means of skirting the Fourth Amendment seems like the exact type of oversight public records laws were intended to foster.

Unwarranted Invasion of Privacy

Another dangerous catch-all exemption lurking in many state public records laws has the potential to thwart access to records produced by 'Smart City' technologies: the personal privacy exemption. Particularly with video records that could be subject to facial recognition or audio records that could be subject to voice-printing, the personal privacy exemption is likely to come into play. Some states, like Maryland, have quite vague statutory language that exempts any

[77] NRSA 84-712.05(5)

record that would "cause an unwarranted invasion of privacy."[78] Even in states with no statutory exemption for personal privacy—including Iowa—case law can prove challenging. There, courts are expected to employ a four-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) the gravity of the invasion of personal privacy."[79]

Conclusion

As written, most state open meetings and records laws could further citizens' rights with regard to 'Smart City' technologies, if they were interpreted to advance the spirit of government transparency. But research has also shown us that government officials do not always follow these laws—particularly when they are eager to keep information from the public.[80] As work moved online during the COVID-19 pandemic, we introduced more communication technologies into our everyday routines, replacing face-to-face interactions and email with Zoom meetings and direct messaging apps—nearly all of which have output that should qualify as government records.[81] Instead, Iowa Freedom of Information Council director Randy Evans noted "The

[78] Md. Code Ann. 4-351(b)(3).

[79] *See DeLaMater v. Marion Civil Serv. Comm'n*, 554 N.W.2d 875, 879 (Iowa 1996).

[80] *See, e.g.,* Amy Kristin Sanders & Daxton "Chip" Stewart, Ghosted by the Government: Why Government Entities Should Be Required to Respond to Public Records Requests, 3 J. Civic Info. 1-13 (2021); A.Jay Wagner, *Piercing the Veil: Examining the Demographic and Political Variables in State FOI Law Administration,* 38 Gov. Info. Q. (2021); Daxton "Chip" Stewart & Amy Kristin Sanders, Secrecy, Inc.: How Governments Use Trade Secrets, Purported Competitive Har and Third-Party Intervention to Privatize Public Records, 1 J. Civic Info. 1-29 (2019); David Cuillier, *The People's Right to Know: Comparing Harold L. Cross' Pre-FOIA World to Post-FOIA Today,* 21 Comm. L. & Pol'y 433 (2016); David Cuillier, *Honey v. Vinegar: Testing Compliance-Gaining Theories in the Context of Freedom of Information Laws,* 15 Comm. L. & Pol'y 203 (2010).

[81] For a more detailed discussion of how COVID impacted access to information, *see* Amy Kristin Sanders, *COVID-19, Death Records and the Public Interest: Why Now is the Time to Push for Transparency,* 2 J. Civic Info. 1 (2020).

technology has opened up a whole new avenue for people who want to circumvent the spirit of open meetings law by communicating away from the public during the meeting. That's very worrisome because if the meeting were open to the public in the traditional sense you would know if they were whispering to each other or if one were passing a note to each other."[82]

Investigative journalists have also uncovered officials' attempts to circumvent freedom of information laws through the use of various communication technologies. Multiple sources told Axios reporter Cuneyt Dil that members of D.C. Mayor Muriel Bowser's staff were using WhatsApp for government communication despite Bowser's pledge to increase government transparency.[83] A few months earlier in December 2021, the *Washington Post* reported that Maryland Gov. Larry Hogan was found using Wickr, a messaging app that deletes message after 24 hours.[84] These reports raised serious concerns among open government advocates. D.C. Open Government Coalition president Tom Sussman said, "Use of a messaging app that does not provide for collection, archiving, search or generally, availability to the public of that information is a clear violation of the law and circumvention of open government principles."[85] As a result, the Washington, D.C., Council voted in March 2022 to limit officials' of direct-messaging apps like WhatsApp for government work, requiring the retention of all messages and prohibiting the use of "auto-delete" functions.[86]

Even more recently, the Secret Service was unable to produce text messages in response to a request from Congress. The DHS inspector general told Congress the messages had been

---

[82] http://www.timescitizen.com/kifg/county-disables-zoom-private-chats-amid-open-meeting-concerns/article_ac4cf0c4-fbc3-11ea-b813-239203eb9a01.html

[83] https://www.axios.com/local/washington-dc/2022/02/15/dc-mayor-whatsapp-records-concerns

[84] https://www.washingtonpost.com/dc-md-va/2021/12/30/hogan-wickr-messages-disappear/

[85] https://www.axios.com/local/washington-dc/2022/02/15/dc-mayor-whatsapp-records-concerns

[86] https://dcist.com/story/22/03/01/dc-council-limits-whatsapp-government/

deleted during a "system migration."[87] After only a single message was released from the 24 agents whom Congress had subpoenaed, a criminal investigation was launched. Thereafter, the *Washington Post* reported that neither Chad Wolf nor Ken Cuccinelli—the top two officials at DHS—could produce text messages from January 6.[88]

The lack of a transparency culture not only presents an issue at the federal level. As journalists from *The Lens* in New Orleans learned, even when public records laws are on your side, it can be a battle to get access to information. For its "Neighborhoods Watched" investigative report, *The Lens* spent more than a year "obtaining and reviewing thousands of city documents" to shed light on New Orleans' use of "Smart City" technologies for surveillance, uncovering what they call "rapid, largely unchecked" proliferation.[89] Interviews with privacy experts revealed little oversight had been occurring:

> The status quo is that the government is really free to acquire, deploy and expand existing surveillance technology outside of public view, without public input and without oversight. Often, as a result, we really don't know what is out there.[90]

To get access to the locations of surveillance cameras, the Orleans Public Defenders Office had to file a lawsuit. In 2020, the Louisiana Supreme Court declined to overrule a state appellate court ruling[91] requiring the city turn over the map of camera locations.[92] Further, New Orleans officials failed to provide complete and accurate responses to public records requests about the

---

[87] https://www.vox.com/23274533/secret-service-text-messages-january-6

[88] https://www.washingtonpost.com/national-security/2022/07/29/homeland-inspector-general-texts/

[89] Michael Isaac Stein, Caroline Sinders & Winnie Yoe, *Neighborhoods Watched: The Rise of Urban Mass Surveillance,* The Lens, Oct. 21, 2021, https://surveillance.thelensnola.org/

[90] *Id.*

[91] Bixby v. Arnold, 287 So. 3d 43 (La. Ct. App. 2019).

[92] *Louisiana Supreme Court Upholds Lower Court Ruling Requiring New Orleans to Turn Over Surveillance Camera Locations,* ACLU, April 9, 2020, https://www.aclu.org/press-releases/louisiana-supreme-court-upholds-lower-court-ruling-requiring-new-orleans-turn-over-0

city's surveillance apparatus, including a request for the location of 40 fixed license plate readers that the New Orleans Police Department deployed in early 2021.[93] Similar challenges occurred years earlier in Oakland, where Brian Hofer and the Oakland Privacy Advisory Commission sought access to records on the city's surveillance network:

> What we were doing in Oakland… submitting a lot of public records requests and poring through agendas and contracts, matching up model numbers and serial numbers and trying to see what was being used. And that takes a lot of effort.[94]

But it should not be like that. Public records laws are intended to increase transparency and access to information. Yet anyone who uses them regularly knows their limitations. Referring to her efforts to obtain information as "public records odysseys," Tracy Rosenberg of Oakland Privacy noted, "For everything we asked, we probably got answers on 20 to 30 percent of it. We still have public records requests that go back to 2014 and 2015 that haven't been answered."[95] Despite these challenges, residents in Oakland and a handful of other U.S. cities, working with advocacy groups like the Surveillance Technology Oversight Project, have been able to implement some oversight into their cities' use of "Smart City" technologies.[96]

As the IoT and other technologies continue to advance, it is important to ensure that our public records laws keep pace—both by ensuring a broad definition of record and a narrow construction of privacy and law enforcement exemptions. Often these records provide the public with its first opportunity to learn about government activity, and no single actor bears the full responsibility of lobbying lawmakers on issues of transparency and accountability. Access advocates and the press play a key role in pressing legislatures to amend these laws to ensure

---

[93] Stein, Sinders & Yoe, *supra* note X.

[94] *Id.*

[95] *Id.*

[96] *Id.*

they continue to hold governments accountable. The judiciary has a responsibility to interpret public records laws in light of the spirit of government transparency they seek to promote rather than assisting government officials in their quest to obfuscate. But most importantly, the voting public needs to make regular use of these laws as a means of providing the oversight critical to a functioning democratic society.